INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PICOS

ANALISE E DESENVOLVIMENTO DE SISTEMAS

JOSÉ COÊLHO VIANA JÚNIOR

ESTEGANOGRAFIA: A ARTE DE ESCONDER INFORMAÇÕES

PICOS
2018

José Coelho Viana Júnior

ESTEGANOGRAFIA: A ARTE DE ESCONDER INFORMAÇÕES

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do diploma do Curso de Analise e Desenvolvimento de Sistema do Instituto Federal de Educação, Ciência e Tecnologia. Campus Picos.

Professor Orientador: Mestre João Paulo Lima do Nascimento

Picos

2018

FICHA CATALOGRÁFICA
Sistema de Bibliotecas
Gerada automaticamente com dados fornecidos pelo(a) autor(a)

Viana, Jose Coelho Viana Junior
VV61 Esteganografia: A Arte de Esconder Infomações / Jose Coelho Viana Junior Viana -
4e 2018.
76 p. : il. color.

Trabalho de conclusão de curso (Tecnologia) - Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Picos, Tecnologia em Análise e Desenvolvimento de Sistemas, 2018.

Orientador : Prof Me. João Paulo Lima do Nascimento.

1. Ocultação da Informação. 2. Esteganografia. 3. LSB. 4. Segurança da Informação. I.Título.

CDD 004

José Coêlho Viana Júnior

ESTEGANOGRAFIA: A ARTE DE ESCONDER INFORMAÇÕES

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do diploma do Curso de Analise e Desenvolvimento de Sistema do Instituto Federal de Educação, Ciência e Tecnologia. Campus Picos.

Aprovado em: 02/05/2018.

BANCA EXAMINADORA:

João Paulo Lima do Nascimento

Prof. Mestre João Paulo do Nascimento (Orientador)
Instituto Federal do Piauí (IFPI)

Manoel Messias Pereira Medeiros

Prof. Especialista Manoel Messias Pereira Medeiros
Instituto Federal do Piauí (IFPI)

Daniel de Sousa Luz

Prof. Especialista Daniel de Sousa Luz
Instituto Federal do Piauí (IFPI)

DEDICATÓRIA

A minha esposa Maria de Fatima e minhas filhas Loysla e Lorena
pelo apoio, compreensão, amor e incentivo incondicional,
Aos meus pais, pelas orações e eterna dedicação.
Dedico

AGRADECIMENTOS

Primeiramente a Deus, a todos os professores do curso de Analise e Desenvolvimento de Sistema, que foram tão importantes na minha vida acadêmica e no desenvolvimento deste TCC e em especial aos Professores Juciê, Messias, Gilberto, Rogerio, James, Ayslan, Jader e João Paulo com os quais tive a honra de conviver e aprender nas disciplinas do curso de ADS.

RESUMO

Este trabalho faz uma abordagem sobre Segurança da Informação e descreve a Esteganografia como mecanismos utilizado na proteção da informação e seus mecanismos. O trabalho tem como foco trazer uma abordagem sobre a proteção da informação utilizando como mecanismo de proteção a Esteganografia, no qual foi implementado uma ferramenta para demonstração que faz a inserção de mensagens curtas em arquivos de imagens. O objetivo dessa ferramenta é demostrar a ocultação de uma informação em imagens digitais, utilizando a Esteganografia. Utilizou-se o método de Esteganografia *Last Significant Bit* (LSB), para a ocultação da informação em uma imagem definida pelo usuário do sistema. Essa ferramenta demostrar a introdução de forma imperceptível ao ser humano (visão), de tal maneira que é a detecção por terceiros seja pouco provável, como também a garantia de recuperação praticamente inalterável da mensagem. Baseadas em esquemas da Esteganografia e de acordo com os resultados obtidos de outros trabalhos analisados neste trabalho, avalia-se a viabilidade do desenvolvimento de aplicações para garantir a autenticidade, o sigilo e a proteção de informações transmitidas pela web.

Palavras-chave: Ocultação da Informação. Esteganografia.

ABSTRACT

This work takes an approach on Information Security and describes the Steganography as mechanisms used in the protection of information and its mechanisms. The work focuses on an information protection approach using a Steganography protection mechanism, in which a demonstration tool has been implemented that inserts short messages into image files. The purpose of this tool is to demonstrate the concealment of information in digital images, using Steganography. The Last Significant Bit Steganography (LSB) method was used to conceal the information in a user-defined image of the system. This tool demonstrates the introduction of an imperceptible form to the human being (vision), in such a way that the detection by third parties is unlikely, as well as the guarantee of almost unalterable recovery of the message. Based on Steganography schemes and according to the results obtained from other works analyzed in this work, the feasibility of the development of applications to guarantee the authenticity, the confidentiality and the protection of information transmitted by the web is evaluated.
Palavras-chave: Information Concealment. Steganography.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Segundo Coutinho (2008), desde o princípio os seres humanos compartilham informações utilizando-se de variados meios e com técnicas diferentes, pois o homem sempre buscou simbolizar seus hábitos e costumes, no intuito de serem utilizados posteriormente por ele ou por outras pessoas do grupo. As informações relevantes eram gravadas em objetos, que geralmente estavam abrigados em locais de difícil acesso. A tais objetos só tinha acesso aqueles que teriam autorização para ver, interpreta-lo ou decifra-lo**.**

Acrescenta-se também que no século XXI, as informações se tornaram ainda mais preciosas principalmente para empresas ou pessoas em particular, pois planejar e implementar uma Política de Segurança da Informação (PSI) tornam-se indispensáveis, visto que a informação deve estar de forma confiável, segura, controlada e atualizada (OLIVEIRA, 2009). Com o avanço tecnológico da informática, com a popularização da internet e com a crescente utilização de aplicativos móveis para troca de informação, decerto haverá uma procura maior por meios de proteção da informação.

Em outras palavras as Informações de valor expressivos precisam ser guardadas e transmitidas com segurança, fora do alcance de terceiros não autorizados ou mal-intencionados, pois essa informação pode ser um diferencial competitivo. Por tanto, as Políticas de Segurança da Informação (PSI) têm como finalidade garantir que as informações adquiridas, desenvolvidas ou aperfeiçoadas, estejam seguras através de seus mecanismos. (CARVALHO, 2003).

Certamente um dos mecanismos mais conhecidos e utilizados para a transferência de informações, sem que haja a possibilidade de perda do sigilo, mediante a codificação ou cifragem das informações, tornando-as incompreensíveis, é conhecido como Criptografia (KOBUSZEWSK, 2004)

Segundo Kobuszewsk (2004), a Criptografia é a ciência que estuda os princípios e métodos para proteger a violabilidade das informações por meio da cifragem e que permite a recuperação da informação original por meio do processo de decifração. Amplamente aplicada na transmissão de dados, esta ciência utiliza-se de algoritmos matemáticos e da criptoanálise para inferir maior ou menor proteção de acordo com sua complexidade e estrutura de desenvolvimento.

Do mesmo modo outro método utilizado é a Esteganografia, que é uma antiga arte utilizada para esconder mensagens secretas em objetos aparentemente sem qualquer outra informação tais como: imagens, textos, áudio e vídeos, de forma que previna sua detecção por parte de terceiros. Ao contrário da Criptografia, no qual tem como finalidade tornar a mensagem incompreensível, o propósito da Esteganografia é tornar imperceptível a existência da mensagem, sendo assim possível a utilização das duas técnicas em conjunto, aumentando ainda mais a segurança e dificultando uma possível violação (KOBUSZEWSK, 2004).

Acrescenta-se que a Esteganografia permite uma comunicação mediante o anonimato, ocultando o envio e a presença de alguma informação durante a comunicação. Técnicas e métodos desenvolvidos na atualidade como a *Last Significant Bit* (LSB), ocultam mensagens em arquivos digitais, na internet ou em outros tipos de objetos, com a finalidade de transmitir ou assegurar que as informações se mantenham sigilosas. Os procedimentos de ocultação variam desde técnicas rudimentares e manuais a técnicas digitais bastante avançadas.

É provável que a Esteganografia vem se popularizando devido as suas várias aplicações em torno de seu princípio que é tornar imperceptível a informação. Bem como, ela compõe-se de numerosas técnicas para embutir mensagens em uma variedade de meios. E entre esses métodos estão tintas invisíveis, micropontos, assinaturas digitais, canais escondidos e comunicação de espectro espalhado. Atualmente, com o avanço da tecnologia, a Esteganografia pode ser utilizada em mídias digitais.

Sem dúvida, as definições de Carvalho (2003, p.10) e Kobuszewsk (2004, p.14), reforçam a importancia da Segurança da Informação e principalmente o controle de seu acesso, descrevendo alguns meios para tal restrição.

Inclusive há inúmeros motivos nos quais entidades ou pessoas tenham o desejo de manter suas informações em segredo, seja para obter privacidade em suas conversações, seja para manter em sigilo e em segurança o conteúdo da informação que está sendo transmitida.

Logo, é possível afirmar que a Esteganografia e a Criptografia têm sua importância como meio de controle da Segurança da Informação, em especial como elementos centrais no controle ao acesso a informações, nesse novo cenário tecnológico.

.

1.1 Motivações

A partir dos avanços tecnológicos, principalmente com o surgimento da internet houve um expressivo crescimento em relação a troca de informações como mostra pesquisa: “dos 116 milhões de pessoas que acessaram a internet no Brasil em 2016, 94,2% enviaram ou receberam mensagens de textos, voz ou imagens por aplicativos[...]. ” (IBGE, 2018).

Nesse sentido, a Segurança da Informação torna-se indispensável para assegurar a transmissão dessa informações trocadas, portanto através de seus mecanismos como é o caso da Esteganografia, que entre diversas vantagens, possibilita o envio de informações sigilosas de forma segura, dessa forma aumentando o grau de privacidade e da confidencialidade dos dados privados que são transmitidos na internet, destacando-se assim sua importância significativa como meio de controle para acesso as informações sigilosas.

Portanto a motivação para utilização da Esteganografia é o mascaramento digital de dados, principalmente na proteção do envio de mensagens digitais. Como conceitua (ROCHA, 2003, p. 2), dentre as várias utilidades, pode-se destacar:

> “Técnicas de espalhamento de espectro e modulação, para agencias militares e de inteligência que necessitam de comunicação segura;
> Interesse por parte da justiça em dominar esta tecnologia e conhecer suas fraquezas;
> Busca de meios singulares por uma comunicação anônima, após tentativas recentes de alguns governos de proibir outros meios de controle de acesso a informação;
> Utilização de meios para transmissão anônima em sistemas de urnas eletrônicas e dinheiro eletrônico.”

1.2 Objetivos

1.2.1 Geral

O objetivo geral desse trabalho e fazer uma abordagem sobre a Segurança da Informação e seus mecanismos de controle, como é o caso da Esteganografia digital.

Assim, o desenvolvimento deste trabalho propõe um estudo sobre a Esteganografia e algumas tecnicas existentes.

1.2.2 Especificos

1) Comparação dos métodos LSB aplicados em imagens, vídeos e áudios.
2) Aplicação do método LSB de Esteganografia em imagens;
3) Desenvolvimento de uma ferramenta de software desktop a fim de demonstração, onde o usuário digitará uma mensagem curta que será escondida em uma imagem, ou irá extrair uma mensagem de uma imagem;

1.3 Estrutura do Trabalho

Este trabalho está dividido em 6 capítulos que serão explicitados a seguir:

O primeiro capítulo apresentou a contextualização e justificativas para o desenvolvimento do trabalho.

No segundo capitulo é feita uma singela abordagem sobre a Segurança da Informação, explicando alguns conceitos importantes sobre: mecanismo de segurança ataques, políticas de segurança, vulnerabilidade e etc.

O terceiro capítulo aborda a Esteganografia desde a sua história até a aplicação na atualidade. Faz a abordagem sobre a utilização da Esteganografia, em especial sobre a Esteganografia digital, que servirá de base para o desenvolvimento da ferramenta.

O quarto capitulo traz trabalhos relacionados, a metodologia e faz uma análise da técnica LSB e suas variações.

O quinto capítulo trata do desenvolvimento da ferramenta, mostrando os diagramas de classe, caso de uso. Este capítulo explica a implementação da ferramenta.

O sexto capítulo apresenta as considerações finais, contendo a conclusão do desenvolvimento deste trabalho, as dificuldades encontradas e as sugestões para trabalhos futuros.

2 SEGURANÇA DA INFORMAÇÃO

2.1 Contexto

É evidente que a informação nos dias atuais está em sua maioria em arquivos digitais, nesse novo cenário tecnológico, por isso é importante que os arquivos tenham algum meio de proteção e não esteja perceptível a pessoas mal-intencionadas. Tendo em vista que a Segurança da Informação tem como princípio assegurar que a informação esteja protegida de situações adversas que possam oferecer algum tipo de acesso não autorizado.

Ainda por cima a informação é um ativo precioso para uma empresa ou indivíduo. Logo, deve-se garantir a segurança na armazenagem e transmissão. Atualmente com o avanço dos computadores e da internet o detentor da informação vem se utilizando cada vez mais de meios digitais para armazenamento ou transferência de dados. De fato, a proteção é um dos princípios da Segurança da Informação e através desta podemos controlar o acesso a informação, esta pode está para uso restrito ou exposta ao público, uma vez que só pessoas devidamente autorizados poderiam usufruir ou modica – lá, como destaca Tanenbaum:

> “A segurança é um assunto que inclui inúmeros problema, ela se preocupa em garantir que pessoas mal-intencionadas não leiam, ou modifiquem secretamente mensagens enviados a outros destinatários, ou tenham acesso a serviços remotos que não estão autorizados a usar. Ela também lida com meios para saber se uma mensagem supostamente verdadeira é um trote. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que tentam negar o fato de terem enviado determinadas mensagens. A Segurança da Informação trata da proteção de determinados dados, com o objetivo de preservar os valores que determinada informação possa ter para uma empresa ou um indivíduo, de modo que eles não possam ser acessados, copiada ou codificada por pessoas não autorizadas. ” (TANENBAUM, 1996, p. 543)

Inclusive a Segurança da Informação está apoiada em cinco atributos fundamentais, que são definidos a seguir.

Confidencialidade: “A transmissão das informações deve estar protegida e assegurada de que ela realmente chegue ao destino sem que se torne disponível pelo caminho, portanto só deve estar disponível a ela pessoas autorizadas a manuseá-las, ” (PEIXOTO, 2006, p. 38), já segundo, Teotônio (2013), “Se uma informação for

privada, ela será disponível e deverá ser armazenada com segurança, e indisponível para pessoas não-autorizadas". A Criptografia e a Esteganografia têm meios de assegurar a confidencialidade de uma informação.

Integridade: "É a propriedade que assegura que as informações não tenham sofrido nenhum tipo de remodelação, comprometendo sua real genuinidade, levando à perda da integridade que possuía quando partira da origem. " (PEIXOTO, 2006, p. 39).

Disponibilidade: é a capacidade de que a informação sempre esteja acessível para os usuários autorizados.

> Disponibilidade: "De nada adiantaria termos a confidencialidade e a integridade das informações se tais informações não estiverem disponíveis para serem acessadas. Talvez um dos grandes desafios seja justamente conseguir manter toda a estrutura de passagem das informações de forma confiável e íntegra [...]" (PEIXOTO, 2006, p. 39).

Autenticidade: é a segurança de que a informação é de fato procedente da origem alegada, portanto a informação é realmente nativa do emissor que alega ter enviado a mensagem (MARCIANO, 2006, p. 64).

Repúdio: é a capacidade de contradizer que algo tenha acontecido. Um exemplo é quando em um sistema determinado usuário realiza alguma operação indevida e nega que tenha realizado tal procedimento. Os algoritmos que realizam assinatura digital atestam essa qualidade para a mensagem, não podendo a sua autenticidade ser negada, já o não-repúdio segundo Marciano (2006), ele é a segurança de que não se pode negar a autoria da informação.

Todavia, a Segurança da Informação também pode ser comprometida por certas práticas de seus usuários pela estrutura que a cerca, ou por indivíduos mal-intencionados com a finalidade de desviar, destruir ou alterar alguma informação.

2.2 Ataques à Segurança da Informação

Certamente, os ataques se multiplicaram de forma descontrolada nessa última década a partir do uso de computadores e da internet como ferramenta para auxilio no desenvolvimento do conhecimento, troca de informações e várias outras finalidades, que passaram a ser essenciais no uso doméstico e vitais no mundo empresarial.

Alguns tipos de ataques, podem ser visualizadas tipos de ataques na Figura 1.

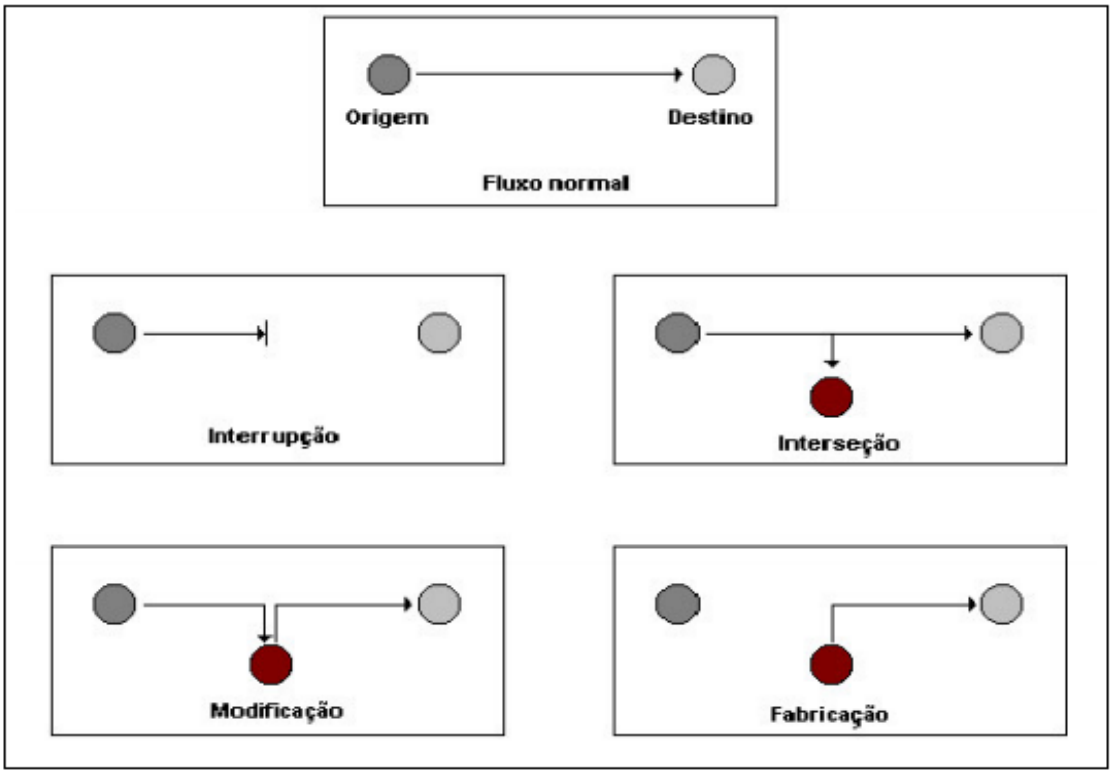

Figura 1- Posição do ataque em relação à origem e ao destino da informação
Fonte: (JASCONE, 2003).

Nesse sentido, Stallings (1995, p.9) descreve as quatro categorias para esses tipos de ataques a informação (Figura 1):

a) interrupção: é quando a informação sofre a interrupção, deixando o dispositivo de destino sem receber os dados;

b) interseção: é quando a informação é interceptada e se torna disponível ao intruso;

c) modificação: é quando a informação é interceptada e depois modificada pelo intruso, posteriormente enviado para o destino;

d) fabricação: é quando a informação é fabricada para ser enviada para o destino. O dispositivo receptor não tem como saber quem está enviando esses dados.

Além disso, os ataques podem também se distinguir em ameaças passivas e ativas, onde na primeira não ocorre alteração ou modificação nas informações

transmitidas por um intruso, no entanto as ativas provocam alterações nas informações, comportamento ou operações de um sistema, (STALLINGS, 1995).

Nessa perspectiva os ataques à segurança de informações estão cada vez mais modernos e sofisticados, e se baseiam no conhecimento de quem ataca o sistema, em ferramentas quem monitoram as redes, no descuido de usuários e no próprio conhecimento do sistema do qual se quer retirar alguma informação.

2.3 Segurança na Internet

A internet é uma grande rede de comunicação entre seus usuários e que proporciona diversos serviços como troca de mensagens, compras online pagamento de contas entre outros, ela já é usual entre a maioria das pessoas. Porém ela possui numerosos perigos e um dos principais são os ataques de *hackers*, por isso é necessário estabelecer medidas de segurança na internet.

De certo, a segurança da internet é composta por todos os cuidados que possamos tomar em favor de proteção dos elementos que compõe a internet enquanto infraestrutura e informação. Inclusive esse tipo de segurança deve contar com bases de dados, arquivos, aparelhos, métodos, procedimentos e normas que possam buscar, detectar e eliminar as vulnerabilidades das informações e equipamentos físicos, como os computadores, para que tais informações não se disseminem a pessoas não autorizadas.

2.4 Mecanismo de Segurança

Mecanismos de proteção se baseiam nas políticas de segurança que podem ser feitas através de vários mecanismos que limitam o acesso a informação, com a finalidade de prevenir possíveis ataques aos dados sigilosos, e que, de outro modo, ficariam expostos a interceptação não autorizada por intrusos. Como por exemplo, através de backups de segurança, ferramentas de detecção de intrusos no sistema entre outros que serão descritos a seguir.

2.4.1 Criptografia

A todo momento o homem percebe a importância de proteger as suas ideias ou as informações que compartilha. Por exemplo, em tempos de guerras, onde uma informação que ordene um ataque ou uma possível movimentação das tropas seja interceptada por terceiros, comprometendo toda a operação militar.

Por certo a Criptografia apareceu através das necessidades da troca de informação por meios de mensageiros, cartas e posteriormente a internet, meios esses em que ainda não eram possíveis a garantia de que uma informação seguirá o seu fluxo normal de origem e destino sem que sejam interceptadas pelo invasor que posteriormente poderá destruí-la ou até mesmo extraí-la.

Além disso, um dos registros mais antigos de um esquema criptográfico é o criptograma de César, por certo era como os documentos mais confidencias eram codificados, invertendo-se a posição das letras do alfabeto. Naquela época eram usados pelos monarcas romanos para transmitir mensagens a seus comandados. Cogita-se que esse criptograma era usado através de uma tabela com as letras do alfabeto que servia como referência, junto com seu significado correto das letras do alfabeto a partir da regra salte três: as letras eram permutadas pela terceira letra seguinte como mostra a Figura 2.

Figura 2- Criptograma de César
Fonte: Própria Autoria.

A Criptografia é uma ciência que reescreve textos de modo a ser incompreendido pelo intruso, ou seja, é o meio de proteção da informação que utiliza técnicas que transformam a informação em cifras ou códigos onde somente quem enviou e o seu respectivo destinatário decifre e compreenda a informação ali contida.

Com o objetivo de garantir o sigilo da informação de pessoas não autorizadas, mesmo que tais consigam visualizar os dados criptografados.

Segundo Tanenbaum (1996) há quatro grupos principais de pessoas que utilizaram a Criptografia e contribuíram para a Ciência da Criptografia: os militares, os diplomatas, as pessoas que gostam de armazenava memórias e os aventureiros. Dentre eles, os militares tiveram o papel fundamental no desenvolvimento desta tecnologia.

Até a invenção dos computadores, uma das restrições impostas à Criptografia era a habilidade do auxiliar de Criptografia em fazer a mudança essenciais, geralmente com poucos equipamentos e no ápice da guerra. Uma outra retenção era a dificuldade de revezamento de métodos criptográficos, pois isso exigia com frequência adestração de numerosas pessoas, (TANENBAUM, 1996).

2.4.2 Assinatura Digital

Assinatura digital é um composto de métodos matemáticos realizados com o emprego de procedimentos criptográficos assimétricos, que permite, de modo único e específico, a confirmação da autoria de uma determinada informação. Como se pode ver na autenticidade de muitos documentos legítimos, que é determinada pela presença de uma assinatura digital (TANENBAUM, 1996).

Dessa forma, um documento digital não pode ser assinado de modo usual, por onde o autor por meio de sua assinatura manuscrita confirma sua identidade. E é através da assinatura digital que é possível garantir a veracidade destes documentos, assegurando ao receptor de uma mensagem digital tanto a identidade do emissor quanto a integridade da mensagem.

De acordo com Tanenbaum (1996), para a geração de uma assinatura digital, necessita de um sistema computacional, através do qual o emissor enviar uma mensagem “assinada” para o receptor de forma que:

a) o receptor possa afirmar a identidade alegada pelo transmissor;

b) posteriormente, o transmissor não possa negar o conteúdo da mensagem;

c) o receptor não tenha a chance de modificar ele mesmo a mensagem.

Em outras palavras, a técnica de assinatura digital faz uso de algoritmos criptográficos para unir uma informação secreta a outra informação que necessita de alguma segurança que garanta a sua legalidade. Por tanto, a segurança é garantida, pois só quem conhece o segredo pode reproduzir o mesmo resultado. Logo o recurso de verificação da assinatura utiliza-se de uma informação pública acrescida da mensagem original para verificar se a referida pessoa efetivamente firmou a mensagem.

2.4.3 Integridade dos Dados

Integridade significa assegurar que a informação guardada ou enviada está correta e é mostrada corretamente para quem a examinar.

E com o avanço da internet e o crescente volume de aplicativos para troca de mensagens e dados, naturalmente a integridade da informação se torna indispensável e a falta dela gera ineficiência tornado a informação inconsistente, adulterada ou corrompida causando um desgaste ou perda de tempo na verificação, que se traduz em desperdício de dinheiro e privacidade para empresas ou pessoas.

Exemplificando, uma informação íntegra é aquela em que se tem certeza de sua origem e a segurança de que não sofreu modificação no meio por onde a mesma transitou quando ainda era um dado.

Partindo desse princípio, uma informação integra é muito importante do ponto de vista operacional, pois assegura e valida todo o processo de comunicação em uma empresa ou comunidade.

Tantas pessoas como empresas empresa comunicam-se o tempo todo, transmitindo procedimentos ou mensagens e a comunicação efetiva só acontece quando o emissor e o receptor da informação a interpretam da mesma maneira.

Interpretar não será uma tarefa fácil se informação não está íntegra. Torna-se então uma tarefa muito mais lenta e trabalhosa quando a informação é adulterada ou corrompida no meio do caminho entre emissor e receptor. Informação sem integridade demanda verificação, correção e retrabalho, portanto, causa conflito, que se traduz em desperdício de tempo.

2.4.4 Controle de Acesso

Controle de acesso é um mecanismo que tem como princípio buscar e verificar a autenticação de um usuário autorizado de um determinado sistema possibilitando a permissão a um recurso deste sistema seja limitado ou ilimitado.

Exemplificando, os Controles de Acesso fazem parte de um processo de dois passos a identificação e autenticação para se determinar quem pode ter acesso a determinado sistema. Durante a identificação digita-se em geral o nome do usuário. Durante a autenticação da identidade é verificada através de uma senha fornecida pelo usuário.

Já na atualidade esse método usuário e senha vem sendo substituídos por novas tecnologias, como por exemplo o reconhecimento por impressão digital ou *Radio-Frequency IDentification* (RFID). A identificação biométrica por impressão digital é a mais conhecida e utilizada atualmente, como exemplo na Justiça Eleitoral.

2.4.5 Esteganografia

A Esteganografia é um método utilizado para transmissão secreta de dados, ela esconde uma informação sigilosa dentro de outro objeto insignificante, de modo que seja impossível a detecção da informação oculta no objeto. Na computação, esse outro objeto pode ser um arquivo de som, imagem ou texto, onde em um dos métodos empregados, parte dos *bytes* destes objetos, os quais, não são significativos são aproveitados para a inclusão da informação, tornando-a a informação imperceptível dentro de um objeto. Este assunto é detalhado no capítulo 3 neste trabalho.

3 ESTEGANOGRAFIA

3.1 Referencial teórico

Com o avanço da tecnologia a internet passou a ser utilizada como meio de transações comerciais entre empresas e pessoas, despertando em pessoas mal-intencionadas o interesse em interceptar e roubar informações destas transações.

> "O uso da rede mundial de computadores deixou de ser apenas uma ferramenta de pesquisa e lazer para se tornar um dos mais promissores centros de negócio. Considerando que a História nos ensina que onde há riquezas e concentração de poder existe também a cobiça, esse sentimento é despertado em pessoas que se especializam em roubar e interceptar informações de outras pessoas e empresas. " (PASSOS, 2006, p. 1).

Passos (2006) e Colombo (2006) ressaltam que a internet vem ganhando grande volume e velocidade no que se diz a respeito ao trafego de informações. Com isso, a segurança torna-se essencial para uma comunicação segura.

Portanto, um dos meios principais no que se trata em garantir a Segurança da Informação é a Esteganografia. "A Esteganografia tem sua importância para a computação no que se refere a contribuir para a Segurança da Informação. " (HONDA, 2011, p. 34).

Jascone (2003) conceitua a Esteganografia como a arte de transmitir informações em segredo, escondendo a informação confidencial dentro de outra informação insignificante.

Em Moura (2006) e Mezzari (2012), eles explicam que a Esteganografia Moderna oculta informações dentro de arquivos de mídia digital, onde em geral a mensagem é escondida através da técnica do *bit* menos significativo e que a informação interceptada só poderá ser revelada por quem souber onde ela está e conhecer o código de extração da mensagem.

Do ponto de vista de Colombo (2006) e Honda (2011) a técnica de inserção de LSB (*Least Significant Bit*) é fácil de implementar, porque os dados podem ser escondidos no *bit* insignificativo, e trabalha na incapacidade do olho humano em detectar pequenas alterações da imagem portadora, ou seja, a mensagem pode passar despercebida. "Inserção no *bit* menos significativo consiste em utilizar o *bit*

menos significativo de cada *pixel* da imagem para ocultar a mensagem. ” (LUCAS, 2017, p. 34).

Como é explicada a seguir:

> “Ao aplicar técnicas de LSB (método do *bit* menos significativo) a cada *byte* de uma imagem 8-*bit* s, 1 *bit* pode ser codificado em cada *pixel*, como cada *pixel* é representado por um *byte,* todas as mudanças ocorridas no *pixel* serão imperceptíveis ao olho humano. ” (COLOMBO, 2006, p. 10).

Já as tecnicas de mascaramento e filtragem:

> “Ao contrário da inserção LSB, as técnicas de mascaramento e filtragem têm como alvo o bit se mais significativos da imagem e por isso são restritos às imagens em tons de cinza (*grayscale*), visto que em imagens coloridas essa mudança geraria uma alta quantidade de ruído, tornando as informações detectáveis. ” (LUCAS, 2017, p. 35).

Mezzari (2012) e Honda (2011) alegam que na técnica LSB existem desvantagens, pois ao desenvolver está técnica é necessário considerar o objeto portador mais apropriado, determinar como este objeto vai chegar ao receptor e a esteganálise.

> “O objetivo da esteganálise é determinar a existência de uma mensagem, e após esta determinação, decifrar mensagens a partir de cifras e chaves empregadas no processo de Criptografia. Ela atua de duas formas, a primeira tem como objetivo identificar o aspecto de mensagem ocultas na mídia e a segunda tem o objetivo de extrair do material a mensagem esteganografada. ” (MEZZARI, 2012, p. 36)

3.2 Contexto

Com os avanços tecnológicos ocorridos nas últimas décadas as pessoas vêm cada vez mais a utilizar os avanços tecnológicos, principalmente a internet, mas devido aos ataques aplicados por *hackers*, os usuários vêm buscando meios de se proteger, principalmente na segurança da transmissão de informações por meio da *web*, desta forma vem o desejo de se comunicar ou transmitir dados de forma secreta ou oculta. “A ciência de ocultar mensagens é chamada esteganografia” (TANENBAUM, 1996).

A Esteganografia é descrita na literatura como a arte de mascarar ou ocultar informações, com a finalidade de evitar a sua detecção. “ A palavra esteganografia é derivada do grego, no qual estegano = esconder, mascarar e grafia = escrita”

(PETITCOLAS,1999 apud SECUNDINO, 2013, p. 10). Ela possui um esquema básico na sua montagem, que é composto segundo Jascone, (2003), por um portador e o dado embutido resultando no objeto esteganográfico.

Partindo do princípio da Esteganografia que é ocultar dados, logo o objetivo é que os dados transmitidos não sejam percebidos por terceiros, onde a presença da informação oculta em um arquivo é simplesmente desconhecida e somente o receptor desta mensagem têm o conhecimento de sua existência e a maneira de extrair tal informação (MOURA, 2006).

Além disso há muitos meios para aplicação da Esteganografia. Informações podem ser escondidas em imagens utilizando técnicas especificas, como é o caso do *bit* menos significativo, que será explicado mais posteriormente. Além de imagens, arquivos de áudio também podem ser utilizados para esconder informações, de forma que estas sejam imperceptíveis por quem estiver captando o som. Outras técnicas usam também arquivos de texto, arquivos HTML (*HyperText Markup Language)* e pacotes TCP (*Transmission Control Protocol*) para mascarar informações entre outros. Portanto é necessário observar que os métodos também possuem algumas limitações. Por exemplo como o tamanho das informações a serem ocultas é restringido pelo tamanho do objeto que será utilizado como cobertura. Quanto menos essas informações modificarem a aparência dos arquivos, o potencial das técnicas esteganográficas será maior. Em geral, informações muito grandes acabam danificando o meio, o que facilita a detecção de uma possível mensagem escondida no arquivo (MEZZARI, 2012).

Constata-se que a Esteganografia tem sido bastante procurada, para ser utilizada em vários setores, principalmente na autenticação ou validação de documentos, comunicação anónima, comércio electrónico, sigilo dos sistemas de computação, detecção de informação oculta, urnas eleitorais digitais, privacidade e ocultação de informação, cifragem e decifragem.

Porém diferentemente da Criptografia, que codifica as mensagens de modo a torná-las indecifrável a Esteganografia esconde-as através de técnicas, por exemplo imagens ou um texto que não tenha sentido, mas que sirva apenas de suporte para a camuflagem da informação secreta (MOURA, 2006)

Mas as duas técnicas podem ser utilizadas em conjunto com isso à expectativa do aumento da Segurança da Informação. Por exemplo, pode-se utilizar a técnica de Criptografia em uma mensagem de texto e em seguida estenografar à mesma em uma

imagem qualquer e então enviar a imagem, se a imagem for interceptada, o invasor primeiramente terá que descobrir a mensagem camuflada entre os *bits* da imagem, e, a parti da descoberta da informação, poderá realizar tentativas de descriptografá-la, Moura (2006).

Nas Figuras 3 e 4, como exemplo podemos observar várias características que nos permitem identificar o uso da técnica da Esteganografia em validação ou autenticação de documentos como por exemplo carteira de habilitação ou cédulas de dinheiro.

Figura 3- documento
Fonte: (MEUCARRONOVO, 2018).

Figura 4- cédula de dinheiro
Fonte: (D.AAI, 2018).

Percebe-se que esta arte de esconder mensagens não é atual. Relata-se que no passado foram inventados vários meios para esconder informações, mascarando ou embutindo em outros objetos, na tentativa de assegurar a privacidade na transmissão de informações, onde conheceremos alguns a seguir.

3.3 Histórico

A Esteganografia, como já foi dito, não é uma área nova, pois o primeiro registro do uso da Esteganografia se dá a mais de 3000 anos do início da idade antiga segundo Jasper (2009), muitas técnicas desta área são conhecidas e descritas na literatura como por exemplo na Grécia Antiga onde os tabletes de madeira cobertos com cera eram utilizados para escrita e comunicação, as informações eram escritas na cera, e quando elas não eram mais necessárias, a cera era derretida e uma nova camada era colocada sobre a madeira. Para esconder mensagens, utilizava-se um método que consistia em escrever essas mensagens na madeira, uma vez que a madeira fosse coberta por uma camada de cera, não seria possível saber da existência de tais mensagens.

A seguir é descrita a técnica explicada por Heródoto:

> “O perigo de ser descoberto era grande; havia apenas um modo pela qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os outros gregos. ” (SINGH, 2008, apud JASPER, 2009, p. 28).

Outra técnica também é descrita nas Histórias de Heródoto como é descrito a seguir:

> “Um certo Histio, querendo fazer contato secreto com seu superior, o tirano Aristágoras de Mileto, escolheu um escravo fiel, raspou sua cabeça e escreveu na pele a mensagem que queria enviar. Esperou que os cabelos crescessem e mandou o escravo ao encontro de Aristágoras com a instrução de que deveriam raspar seus cabelos. ” (HETZL; MÜLLER; SELLARS, 2002 apud PETRI, 2004, p. 23).

A Esteganografia na idade moderna, segundo Coutinho (2008), tem início após diversas crises europeias (políticas, religiosas e econômicas). E é nesse período que diversos algoritmos esteganográficos foram criados por religiosos e cientistas, que se preocupavam em transmitir mensagens sem que fossem percebidas principalmente pelo tribunal da inquisição ou por entidades governamentais, que eram implacáveis contra qualquer sinal de heresia ou traição.

A palavra Esteganografia se tornou conhecido no século XV, quando um monge chamado Johannes Trithemius (Figura 5) publicou o livro *Steganographia* (figura 6), escrito em três volumes (GOIS,2003, apud PETRI, 2004, p.12). Naquela época em que foi publicado, acreditavam que esses livros tinham como tema principal rituais de magias. Porém, após a chave para a decodificação do livro foi descoberto, notou-se que o livro descrevia sobre Esteganografia e Criptografia, no qual tais livros continham várias técnicas destinadas a enviar mensagens sem que as mesmas pudessem ser entendidas, percebidas ou encontradas, (CASIERRA, 2009).

Figura 5 - Johannes Trithemius
Fonte: (TEIXEIRA, 2011).

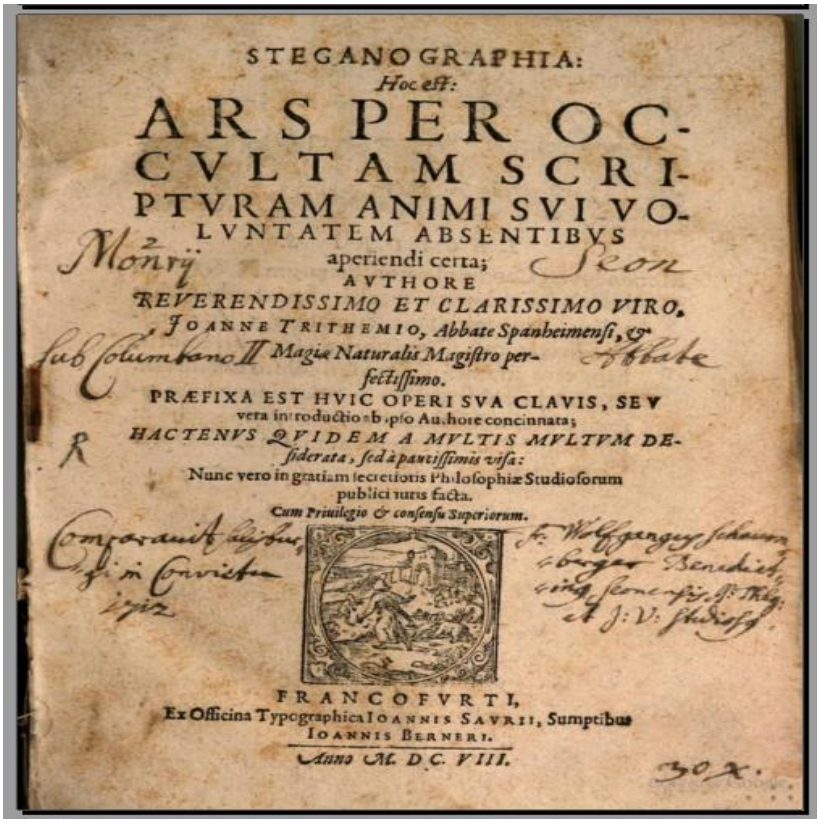
STEGANOGRAPHIA:
Hoc eſt:
ARS PER OC-
CVLTAM SCRI-
PTVRAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimenſi, &c.
ſub Columbano II Magiæ Naturalis Magiſtro per-
fectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Au. hoc concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
ſiderata, ſed à paucissimis viſa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
FRANCOFVRTI,
Ex Officina Typographica IOANNIS SAVRII, Sumptibus
IOANNIS BERNERI.
Anno M. D.C. VIII.

Figura 6 - Pagina do livro de Johannes Trithemius.
Fonte: (CASIERRA, 2009).

Durante a Segunda Guerra Mundial, houve a utilização das tintas invisíveis. As informações escritas por esse tipo de material só poderiam ser reveladas e posteriormente lidas se o papel fosse aquecido. Houve também a utilização da técnica dos micropontos, nesse mesmo período, com o surgimento da fotografia, surgiram os chamados micropontos, onde as mensagens eram fotografadas e posteriormente reduzidas ao tamanho de um ponto, para então serem enviada ao destinatário (PETRI, 2004). Os micropontos ficaram populares e foram muito utilizados nesse combate, onde eram colados em pontos finais das frases ou no pingo de alguma letra i da mensagem. Os micropontos são fotografias que foram reduzidas para imagens com cerca de 1 milímetro de diâmetro, se tornando microfotografias (JASPER, 2009).

Finalizando, no Brasil, principalmente após a década de 80, como afirma Cantanhede (2009), é comum que traficantes recrutem pessoas para esconder drogas no seu corpo, as drogas são ingeridas. Esse tipo de pratica, retorna ao princípio das técnicas de Esteganografia, que foram utilizadas nos séculos passados.

3.4 Esteganografia Digital

A Esteganografia atual evoluiu, acompanhando as evoluções tecnológicas. Neste novo cenário não faz mais sentido a utilização de tintas invisíveis ou escrever em tabletes de madeira. Na atualidade a informações sigilosa é oculta dentro de arquivos de mídia (áudio, vídeo e imagens).

Na visão de Rocha (2003), a Esteganografia digital tem ganhado espaço por causa dos estudos de *copyright*[1] *e watermarking*[2] de arquivos digitais, com a finalidade de evitar a pirataria (copias não-autorizadas), principalmente na internet.

Serão descritas na seção seguinte as várias áreas de aplicação e formas de Esteganografia digital moderna.

[1] ***Copyright*** é um direito autoral, a propriedade literária, que concede ao autor de trabalhos originais direitos exclusivos de exploração de uma obra artística, literária ou científica

[2] ***Watermarking*** é uma técnica esteganográfica de ocultação de informação. Seu objetivo principal é pôr de manifesto o uso ilícito de verdadeiro serviço digital por parte de um usuário não autorizado.

3.5 Áreas de aplicação

3.5.1 Privacidade

A Esteganografia assegura a privacidade provendo sigilo ao ocultar a existência de uma mensagem. No campo da espionagem, tanto militar quanto industrial, um exemplo é descrito por (CAHÚ, 2009), um usuário deseja transmitir uma informação sigilosa criptografada para outra pessoa, simplesmente este fato pode levantar suspeita e consequentemente sofrer um ataque, entretanto utilizando-se da Esteganografia a transmissão possivelmente não sofrerá um ataque.

3.5.2 Propriedade Intelectual

A Esteganografia pode ser usada para embutir *watermarking* ou *copyright* em uma mídia, para impedir, e até restringir cópias ou provar sua autoria se necessário.

3.5.3 Rastreabilidade e Autenticidade

Equipamentos como filmadoras e impressoras podem inserir, usando técnicas esteganográficas, números de série, datas e horários de criação nas mídias que produzem, com o fim de tornar fraudes rastreáveis. Por exemplo uma CNH, através dos dados embutidos pode-se verificar a sua autenticidade.

3.6 Técnicas de Esteganografia Digital

A Esteganografia vem evoluindo bastante nessas últimas décadas com o surgimento dos computadores. Essa tecnologia digital veio a facilitar as aplicações das técnicas esteganográficas.

Há várias técnicas que facilitam a utilização da Esteganografia em vários meios da tecnologia digital. Entre as técnicas mais conhecidas estão as que utilizam as imagens, áudio e vídeo são as técnicas de inserção no *bit* menos significativo - LSB, técnica de filtragem e mascaramento, algoritmos e transformações além do espalhamento por espectro, (RANGEL, 2005).

Nesse capítulo será abordado o funcionamento do método de Esteganografia em imagens.

3.6.1 Algoritmos e transformações

As técnicas de Esteganografia baseadas em algoritmos e transformações conseguem tirar proveito de um dos principais problemas da inserção no canal LSB que é a compressão.

Em outras palavras é uma variação das tecnicas de filtragem e mascaramento, e consiste no cálculo dos valores dos cossenos. Essa transformação baseia-se na alocação dos valores calculados de forma ordenada na imagem. Para isso, ele procura colocar os bits mais significativo no canto superior esquerdo, proporcionado a percepção de degradê. Essa transformação é denominada de transformação discreta do cosseno. (JULIO, 2007, apud REIS, 2011, p 07).

Diante disso são consideradas como técnicas mais elaboradas que o LSB, porém, mesmo assim podem sofrer os ataques de esteganálise. Esse método distribui melhor os *bits* do dado embutido em toda região da imagem. Dessa forma, as imagens ficam mais protegidas já que são mais difíceis de serem detectadas e compreendidas.

3.6.2 Filtragem e mascaramento

São procedimentos ou técnicas que só podem ser utilizadas em imagens de escala cinza, pois consiste em ocultar a mensagem através da marcação da imagem, parecido com o funcionamento das marcas d’água aplicadas em papeis. As principais vantagens dessa técnica é que pode ser aplicado em imagens que passam por métodos de compressão, levando em consideração que agora a marca d’água faz parte da imagem. A outra vantagem é que esse procedimento de Esteganografia passa despercebido pelo olho humano, que por sua vez não consegue distinguir a algumas mudanças na imagem.

Ao contrário da inserção no canal LSB, as técnicas de filtragem e mascaramento trabalham com modificações nos *bis* mais significativos das imagens. As imagens que serviram de objeto portador devem ser em tons de cinza porque estas técnicas não são eficazes em imagens coloridas. Isto deve-se ao fato de que

modificações em *bits* mais significativos de imagens em cores geram muitos artefatos tornando as informações mais propensas a detecção.

3.6.3 Técnicas de inserção no bit menos significativo (LSB)

> "O método *Least Significant Bit* (LSB) é o mais comum utilizado para armazenar informação em imagens digitais. Consiste em utilizar o *bit* menos significativo de cada *pixel* (ou de cada cor) da imagem, para ocultar a mensagem". (JASCONE, 2003, p. 38).

Explicando o funcionamento da técnica LSB:

> "As técnicas de LSB podem ser aplicadas a cada *byte* de uma imagem 32-*bit s*. Estas imagens possuem cada *pixel* codificado em quatro *byte* s. Um para o canal alfa (*alpha transparency*), outro para o canal vermelho (*red*), outro para o canal verde *(green*) e, finalmente, outro para o canal azul (*blue*). Seguramente, pode-se selecionar um *bit* (o menos significativo) em cada *byte* do *pixel* para representar o *bit* a ser escondido sem causar alterações perceptíveis na imagem. " (ROCHA, 2003, p. 19)

Exemplificando, a técnica LSB consiste na substituição do *bit* menos significativos de uma imagem digital ou de um áudio por uma informação. Podendo retirar ou alterar o ultimo *bit* menos significativo de um *byte* que não irá causar uma perda significativa da qualidade da imagem ou do áudio, o ser humano não será capaz de perceber se alguma informação foi alterada.

Como exemplo dessa técnica, pode-se supor que uma mensagem de texto seja inserida em uma imagem ou em um áudio tomando o último *bit* em cada bloco (que está em negrito) como a posição que será inserida o texto, (PETRI, 2004).

10111100**1** - 01110101**1** - 00011010 - 00110001 – 11010000

Agora o texto, cujo código binário e 10010 será inserido em uma determinada mídia.

10111100**1** - 01110101**0** - 00011010 - 00110001 – 11010000

Pode-se perceber que dos dados inseridos apenas foi modicado o segundo bloco binário, fazendo com que a alteração seja imperceptível ao olho humano.

Para que possa esconder uma mensagem de texto utilizando a técnica de inserção do último *bit* significativo em uma imagem de 24 *bit se* por exemplo, no qual cada *pixel* possui 3 *bytes s*, percebe-se que só pode armazenar 3 *bits se* em cada *pixel*, manipulando 1 *bit* de cada *byte* desse *pixel*, por tanto, cada *byte* da mensagem a ser ocultada devera ocupara 8 *bytes* da imagem.

Se por exemplo em uma imagem obtém-se os valores dos *pixel*s como mostra a figura 7:

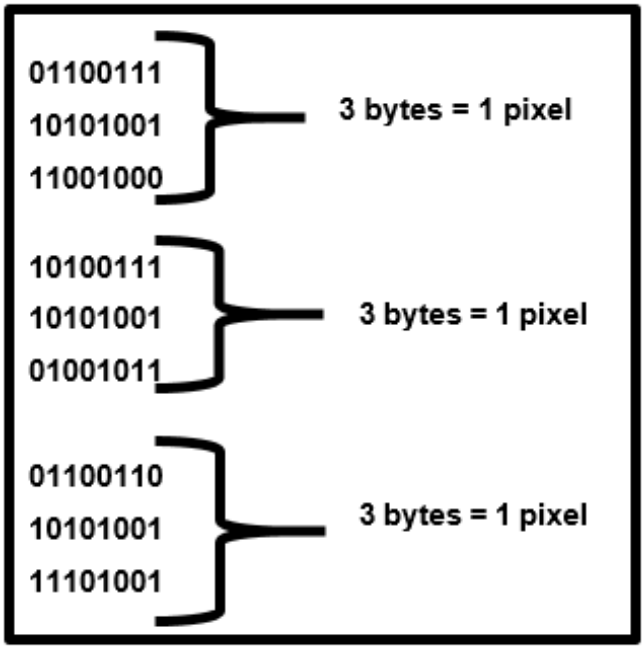

Figura 7- Exemplo de *pixel* de uma imagem
Fonte: (JASCONE 2003)

Se quisermos armazenar a letra ”A” esta suposta imagem, a letra “A” tem como código binário na tabela ASCII 0 1 0 0 0 0 0 1. Posicionado esse código binário, *bit* a *bit,* ao decorrer da imagem e utilizando a técnica LSB, a imagem será como mostra a Figura 8.

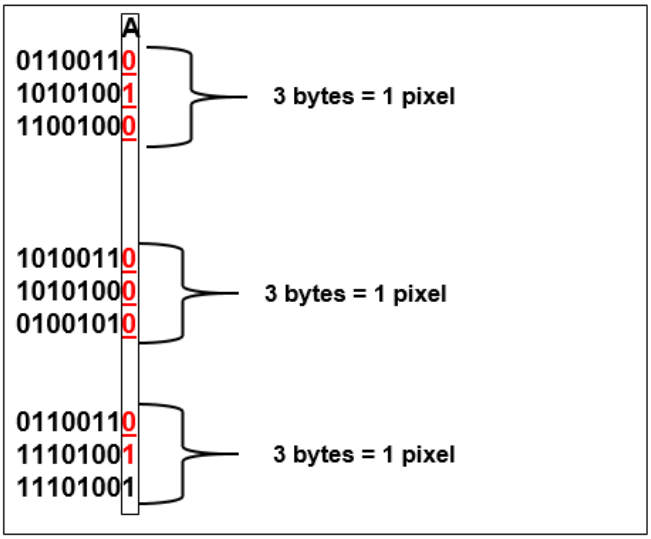

Figura 8- Exemplo do uso do modelo LSB
Fonte: (JASCONE 2003)

O bit s circulados e sublinhados são os que foram modificados, provocando uma imperceptível alteração na cor do *pixel*, que no caso é inviável distinguir está diferença a olho Humano. Esses valores inseridos foi o *byte* que representa a letra "A".

3.7 Esteganálise

> "O processo de esteganografia não é perfeito. Algumas falhas podem ser detectadas através de uma análise detalhada da imagem. Para descobrir se uma imagem é, na verdade, um estego-objeto as técnicas de esteganálise procuram por alteraçõoes nas características da imagem e na maioria das vezes somente a confirmação que existe uma mensagem escondida é suficiente, pois como as mensagens possivelmente são inseridas aleatoriamente e podem ter sido criptografadas torna-se mais difícil recuperar o seu conteúdo. " (PEREIRA et al, 2009 apud SECUNDINO, 2013, p.30).

Segundo Petri (2004), a esteganálise se assemelha com a criptoanálise, pois ambas estão relacionadas à quebra de códigos.

A esteganálise tem como finalidade identificar e extrair informações escondidas por técnicas esteganográficas. Esta baseia-se em uma análise estatística, procurando falhas no uso de técnicas de Esteganografia nas mídias digitais suspeitas. Cada método tem características próprias, modificando o objeto portadora de uma maneira peculiar e deixando uma espécie de assinatura. É fácil notar que técnicas que parecem imperceptíveis ao ser humano, como LSB ou inserção de eco, podem ser detectadas facilmente com o auxílio de computadores, (KOBUSZEWSK, 2004).

Há técnicas de esteganálise que visam apenas detectar a presença ou ausência de uma informação secreta no objeto analisado, mas sem se preocupar com seu conteúdo. Essas técnicas são classificadas como esteganálise passiva. As técnicas que se destinam a extrair uma cópia, às vezes aproximada, da mensagem secreta fazem parte da esteganálise ativa, (CHANDRAMOULI, 2002).

Os principais tipos de ataques realizados aos objetos esteganos descritos por (SECUNDINO, 2013) são:

a) Ataques Aurais: é feita uma análise a olho nu (olhar sem o uso de instrumentos ópticos) no objeto estegano a fim de detectar pequenas alterações, provocadas em geral pela substituição dos bits menos significativo da imagem;
b) Ataques Estruturais: é feita uma análise na estrutura do arquivo, pois assim que se aplica a esteganografia o arquivo algumas vezes muda sua estrutura. Por exemplo em imagens indexadas (baseadas em paletas de cores como RGB[3] e CMYK[4]) quando são utilizadas para ocultar informações muitas vezes são necessários usar diferentes paleta, portanto mudando as características estruturais da imagem esteganografada;
c) Ataques estatísticos: é feita uma análise nos padrões dos *pixels* e seus *bits* menos significativos da imagem. Por exemplo após aplicar a esteganografia LSB em uma imagem, o objeto estegano não possui o mesmo padrão esperado.

3.8 Esteganografia contra Criptografia

A Criptografia é mais utilizada quando tratamos de segurança de informação por ser mais conhecida que a Esteganografia. Porém quando uma informação é criptografada e transmitida pela web e é interceptada ela fica em destaque e possivelmente receberá ataques de criptoanálise afim de se extrair a informação cifrada. Já na Esteganografia há uma vantagem que é o desconhecimento da

[3] Abreviatura de um sistema de cores aditivas em que o Vermelho (**R**ed), o Verde (**G**reen) e o Azul (**B**lue) são combinados de várias formas de modo a reproduzir um largo espectro cromático.
[4] Abreviatura dos sistema de cores subtrativas formado por Ciano (**C**yan), Magneta (**M**agenta), Amarelo (**Y**ellow) e Preto (Black (**K**ey)).

mensagem camuflada em um outro arquivo, o que pode evitar um ataque como mostram as Figuras 9 e 10. Porém ambas têm o mesmo princípio que é o de impedir que pessoas não autorizadas tenham acesso a informação, mais com objetivos diferentes onde a Esteganografia tenta ocultar a informação de um possível intruso enquanto que Criptografia codifica a informação no intuito do intruso não compreenda a informação.

ESTEGANOGRAFIA	*CRIPTOGRAFIA*
Oculta a mensagem em outro objeto de aparência inocente, como imagens, vídeos, sons ou arquivos.	A mensagem é visível, mas cifrada torna-se uma mistura de caracteres sem qualquer significado.
Uma coleção de imagens, vídeos ou sons que não geram suspeitas.	Pelo fato da existência da mensagem estar em evidência, a coleção de caracteres aleatórios gera muita suspeita e curiosidade.
Requer cuidado quando reutilizar arquivos de som ou imagem.	Requer cuidado ao reutilizar chaves.
Não existem leis regulamentando ou proibindo o uso de Esteganografia.	Existem algumas leis que, inclusive, proíbem seu uso.

Figura 9 - Diferenças entre Esteganografia e Criptografia
Fonte: Própria autoria.

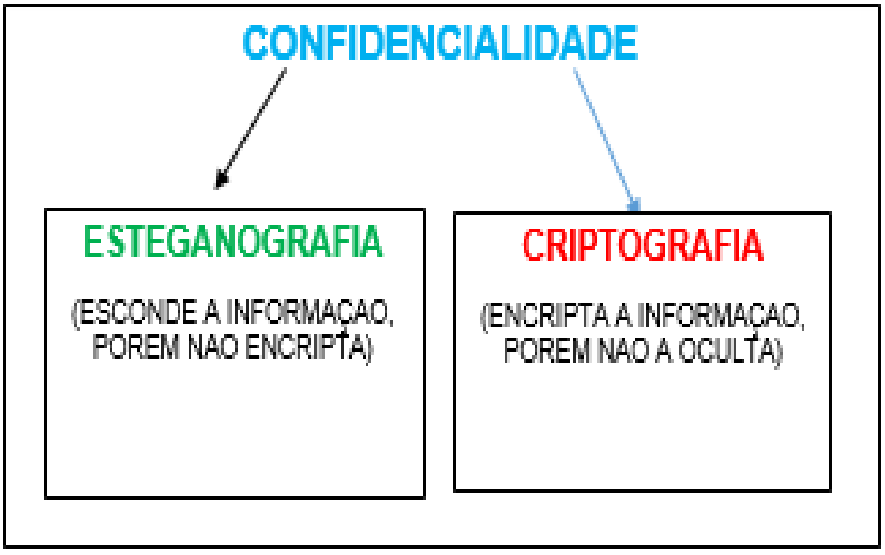

Figura 10– Criptografia contra Esteganografia
Fonte: (PETRI, 2004)

Inclusive os dois métodos (Criptografia e Esteganografia) podem ser usados juntos no intuito de garantir uma maior Segurança da Informação. Por exemplo, pode-se criptografar uma informação e em seguida estenografar, utilizando a técnica LSB, e então transmitir a imagem. Se por algum evento a imagem for interceptada, o intruso primeiro terá que descobrir a mensagem dentre os *bits* da imagem, e, então terá que decriptografar a mensagem.

3.9 Trabalhos relacionados

Camaleão é um software para esteganografia em imagens estáticas, desenvolvido por Rocha, Anderson de Rezende na Universidade Estadual de Campinas (Unicamp).

O software foi desenvolvido na linguagem de programação JAVA orientada a objeto e tem característica interessante a inserção de informações oculta em diversos formatos, como por exemplo, arquivos textos, imagens e executáveis. O camaleão, implementa a inserção de esteganografia em imagens por meio do LSB (*Bit* menos significativo). (ROCHA, 2003).

Esteganografia em Áudio e Imagens utilizando técnica LSB, desenvolvido por Cantanhede, Hugo Silva na Universidade Federal de Goiás (Campus Catalão).

Esse trabalho apresenta a implementação de um e um software escrito na linguagem JAVA orientada a objeto, utilizando a técnica esteganografica LSB (Least Significant *Bit)* que oculta mensagem texto em arquivos de imagem ou arquivo de áudio. (CANTANHEDE, 2009).

Analise e Implementação de Algoritmos para Manipulação de Esteganografia em Imagens, desenvolvido por Honda, Raphael Rodrigues no Centro Universitário Eurípedes de Marilia (UNIVEM).

Esse trabalho apresenta a implementação de algoritmos escritos na linguagem JAVA orientada a objeto, utilizando a técnica esteganografica LSB (*Least Significant Bit)* e suas variações, que oculta mensagem texto em arquivos de imagem. (HONDA, 2011).

Desenvolvimento de um software para Segurança Digital utilizando Esteganografia, desenvolvido por Rocha, Anderson de Rezende na Universidade Federal de Lavras.
Esse trabalho apresenta uma pesquisa sobres as tecnicas esteganográficas clássicas e digitais existentes, e o desenvolvimento de um software com a finalidade de estudar algumas tecnicas esteganográfica afim de solucionar algumas desvantagens. (ROCHA, 2003).

Ferramenta de software para ocultar texto criptografado em imagens digitais, desenvolvido por Jascone, Fábio Luís Tavares na Regional de Blumenau.
Esse trabalho apresenta a especificações e implementações de uma ferramenta para ocultar mensagens criptografadas em imagens digitais, utilizando algoritmo de Criptografia *Advanced Encryption Standard* (AES) em conjunto com o método *Last Significant Bit (*LSB) da Esteganografia. (JASCONE, 2003).

Esteganografia, desenvolvido por Petri, Marcelo na Sociedade Educacional de Santa Catarina (SOCIESC).
Esse trabalho apresenta um estudo sobre as principais técnicas de Esteganografia e suas aplicações em imagens e texto bem como alguns métodos e aplicações da esteganálise. (PETRI, 2004).

Esteganografia, projeto desenvolvido Lucas, Guilherme na Universidade Federal Fluminense.
Esse trabalho apresenta a história e tecnicas da Esteganografia, explicando o início da sua expansão até chegar nas técnicas modernas da chamada Esteganografia digital. (LUCAS, 2017).

Implementação de um sistema esteganográfico para inserção de textos em sinais de áudio, produzido por Casierra, Jinnett Pamela Carrión na Universidade Federal do Pernambuco.
Esse trabalho apresenta a implementação e análise de métodos estenográficos em áudio, em outras palavras inserção de textos curtos em arquivos de áudio no formato wav, com a finalidade de assegurar a autenticidade dos arquivos. (CASIERRA, 2009).

Ferramenta de software para ocultar textos compactados em arquivos de áudio utilizando Esteganografia, desenvolvido por kobuszewski, André na Universidade Regional de Blumenau.

Este trabalho apresenta a especificação e implementação de uma ferramenta de software para incluir mensagens de texto compactadas em arquivos de áudio digitais, utilizando compactação de dados em conjunto com Esteganografia. Utilizou-se do algoritmo de Huffman, técnica estatística de compressão de dados para a compactação de textos, em conjunto com o método de Esteganografia *Last Significant Bit* (LSB), para ocultar mensagens compactadas em arquivos de áudio no formato *Wave.* (KOBUSZEWSK, 2004).

Ocultação de texto criptografado em imagem JPEG, produzido por Moura, Daniel Ribeiro no Centro Universitário de Brasília (UNICEUB).

Este trabalho apresenta a implementação de um aplicativo com uma interface gráfica, capaz de ocultar/extrair um texto criptografado em uma imagem no formato JPEG, utilizando-se da técnica de Esteganografia LSB (*Least Significant Bit)*, em conjunto com o recurso criptográfico MD5 (*Message Digest* 5). (MOURA, 2006).

Esteganografia – Inserção de Texto ou de Arquivo em Vídeo MPEG-1, desenvolvido por Passos, Henrique Lanna no Centro Universitário de Brasília (UNICEUB) e na Faculdade de Ciências Exatas e Tecnologia (FAET).

Este trabalho apresenta a implementação de uma ferramenta, escrito na linguagem C, que utiliza uma técnica de Esteganografia para esconder uma mensagem de texto ou um arquivo, em qualquer formato, dentro de um vídeo do formato MPEG-1. (PASSOS, 2006).

Esteganografia e Marca D`água: A busca por algoritmos robustos, produzido por Hoppen, Caesar Ralf Franz na Universidade Federal do rio Grande do Sul.

Este trabalho apresenta a implementação de algoritmos esteganográficos, LSB e outro utiliza o domínio de frequência e sub amostragem da imagem original e compara os dois a respeito das mudanças visuais. (HOPPEN, 2010).

4 METODOLOGIA DA PESQUISA

Para o desenvolvimento do trabalho foi realizado uma pesquisa exploratória em materiais e métodos encontrados em livros, artigos e trabalhos de conclusão de curso disponíveis na internet ou em bibliotecas, afim de um levantamento bibliográfico sobre o tema do trabalho. Posteriormente foi realizado um estudo sobre a definição da Esteganografia clássica e atual, da sua classificação de suas tecnicas atuais.

Após realizar os estudos em torno da Esteganografia, foi feito uma contextualização sobre o que seria a Esteganografia propriamente dita, sobre as mudanças que ocorreram nos meios de utilização, sobre as áreas de aplicação.

Feito isso, parte-se para o estudo de algumas tecnicas esteganográficas digitais, afunilando o estudo aos métodos computacionais que trabalhem com a ocultação de textos em imagens ditais.

Na ocultação do texto em imagem foi escolhida para implementar a técnica LSB (*Least Significant Bit)*, em outras palavras *bit* menos significativo de cada *pixel* da imagem, por ser um dos métodos mais comuns e utilizados atualmente para esconder informações dentro de imagens, também por possuir um acervo para pesquisa bastante farto, e fácil de ser encontrado em livros e principalmente na internet.

5 ANALISE

A análise tem como proposta realizar o comparativo dos algoritmos LSB esteganográficos quando aplicados em imagens, vídeos e áudios, implementado nos trabalhos referenciados, tendo como base a segurança e sua usabilidade.

Para uma melhor analise foram escolhidos 3 trabalhos que implementaram a sua ferramenta utilizando a técnica do *bit* menos significativo em áudio, vídeo e imagens.

O primeiro trabalho analisado foi o de Kobuszeski (2004) intitulado de Protótipo de software para ocultar textos compactados em arquivos de áudio utilizando Esteganografia.

Esse trabalho foi escolhido por utilizar a Técnica LSB em arquivos de áudio. A sua ferramenta faz ocultação de mensagens compactadas em áudio no formato wav, analisando o seu teste que ele aplicou no áudio estenografado, utilizando editores de áudio, nota-se pequenas variações que segundo o mesmo será imperceptível ao ouvido humano, que segundo Kobuszewsk (2004), é uma forma eficaz e segura no envio de mensagens e que dificilmente será interceptada ou violada.

O segundo trabalho analisado foi o de Moura (2006), intitulado de Ocultação de texto criptografado em imagem JPEG.

O trabalho foi escolhido por implementar a técnica LSB em imagens. O seu artefato oculto textos em imagens no formato JPEG, ao analisar os testes propostos em seu trabalho, cuja a própria ferramenta realiza, nota-se uma pequena variação no tamanho do arquivo em disco, que segundo Moura (2006), essa alteração é imperceptível a visão humana, tornado uma forma eficaz e segura de transmissão de mensagens sigilosas.

O terceiro trabalho escolhido foi o de Passos (2006), intitulado de Esteganografia – Inserção de Texto ou de Arquivo em Vídeo MPEG-1. A sua ferramenta proposta oculta textos em vídeos no formato MPEG-1, ao analisar os seus testes realizados no trabalho a uma alteração drástica no arquivo de vídeo estenografado em relação ao original.

O desenvolvimento do presente estudo possibilitou uma análise e como base nos resultados obtidos nos trabalhos descritos anteriormente. Conclui-se que a técnica estenográfica do *bit* menos significativo quando usado para autenticidade e direitos autorias, tanto em imagens, como em áudio ou vídeos é segura e bastante

eficaz, já para a transmissão de dados a ocultação da informação tem suas limitações, pois a implementação da esteganografia dependerá do tamanho do dado a ser embutido e do meio que servira como objeto estegano, pois a Esteganografia propriamente dita trabalha em cima dos sentidos humanos (visão, audição, olfato e tato). Já a sua usabilidade, sobre o meu ponto de vista, é mais eficaz quando aplicado em imagens, visto que na atualidade a uma gama de aplicativos que compartilham imagens, atentando-se para o fato que as ferramentas analisadas só estenografam não a uma função para envio do objeto esteganográfico.

.

6 DESENVOLVIMENTO DA FERRAMENTA

Neste capítulo serão descritas as especificações e implementações do desenvolvimento de uma ferramenta para demonstração da Esteganografia em imagens, proposto neste trabalho

6.1 Requisitos principiais da Ferramenta

A ferramenta proposta como exemplo neste trabalho, utilizar a Esteganografia para ocultar mensagens de texto em imagens digitais, implementada na linguagem Java e desenvolvida na plataforma Netebeans. A Esteganografia é feita através do método de inserção do último *bit* menos significativo. Foram utilizados e adaptados algoritmos de terceiros na implementação da ferramenta, cujo o código documentado o mesmo está no anexo.

Teremos dois tipos de usuários:

a) Emissor: este terá como dados, a mensagem de texto digitada a ser ocultada em uma imagem, e como saída terá a imagem com a mensagem oculta posteriormente enviada ao receptor;

b) Receptor: com a posse da imagem esteganografada, terá que extrair a mensagem oculta na imagem e como saída terá a mensagem secreta disponibilizada pelo emissor.

Após o emissor realizar a inserção da mensagem na imagem, é gerado uma nova imagem já esteganografada, por tanto, um estego-objeto. Já o receptor tem como finalidade retirar da imagem a mensagem nela oculta.

E através da ferramenta é possível realizar uma comunicação segura, sem que possa levantar suspeitas e sem que o emissor e o receptor estejam on-line ao mesmo tempo. Podendo o emissor disponibilizar uma imagem esteganografada em algum site ou enviar por algum aplicativo de comunicação, disponível no mercado, o receptor conhecedor da imagem e do que ela realmente transporta ele pode ler a mensagem, já para outros usuários ou invasores essa imagem seria insignificante, ou seja seria uma imagem qualquer, portanto sem valor.

6.2 Diagrama de Casos de Uso

Essa ferramenta possui apenas dois tipos de casos de uso como demostra a Figura 11: insere mensagem na imagem, retira mensagem da imagem.

Insere mensagem na imagem é responsável por inserir a mensagem na imagem e é identificada pelo emissor.

O caso de uso retira mensagem da imagem é responsável por retirar a informação oculta da imagem e é identificada pelo receptor.

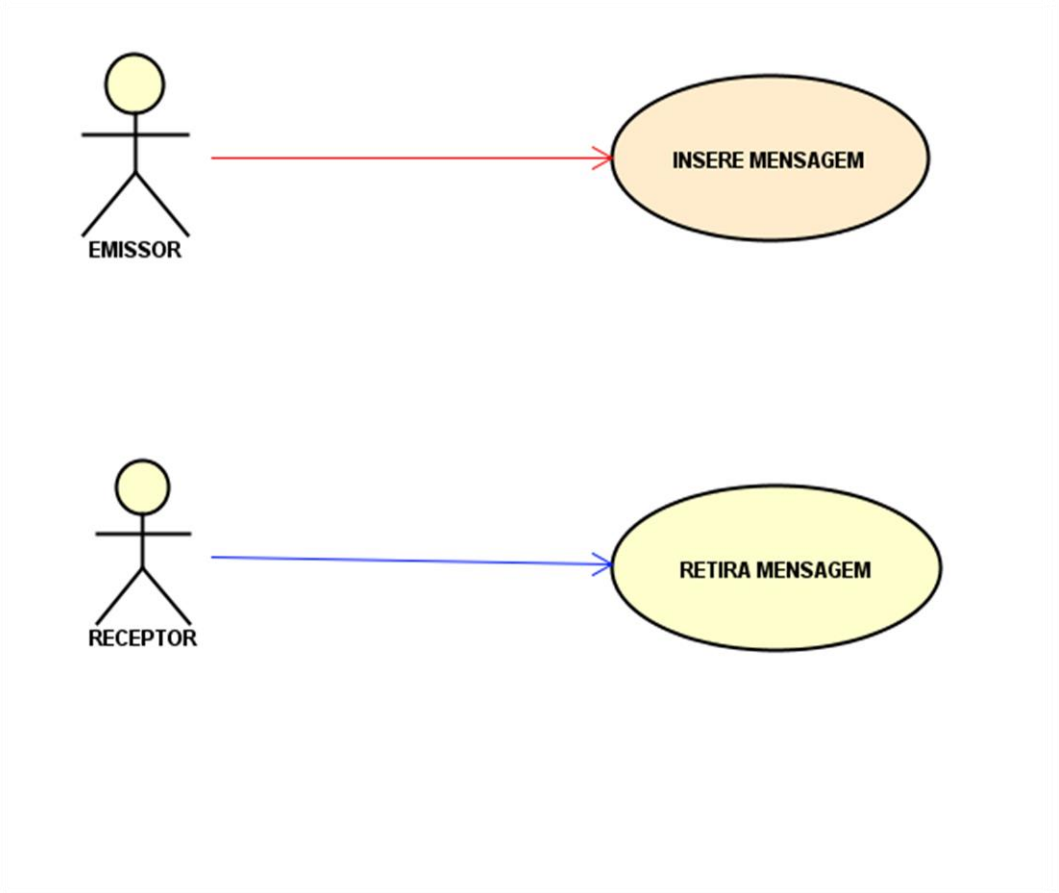

Figura 11- Caso de uso
Fonte: Própria autoria.

6.3 Diagrama de Classes

O diagrama de classes tem a finalidade de mostra a estrutura de uma classe. Nesse artefato há três classes envolvidas na sua construção. São elas, Tela Principal, Imagem e Estegano.

A classe principal do projeto é a Tela Principal, pois nela está a interface gráfica do sistema e com isso toda a ligação entre o sistema, ela é responsável pela visualização das imagens e do campo texto onde é digitada a mensagem. A classe imagem é responsável pela manipulação da imagem, nela há os métodos de abrir e guardar imagens. Já a classe estegano é responsável por aplicar a técnica de inserção e extração no *bit* menos significativo.

A Figura 12 apresenta o diagrama de classe completo, gerado automaticamente pelo plug-in easyUML[5], e mostrando as interações, demostrando assim o funcionamento em sua totalidade.

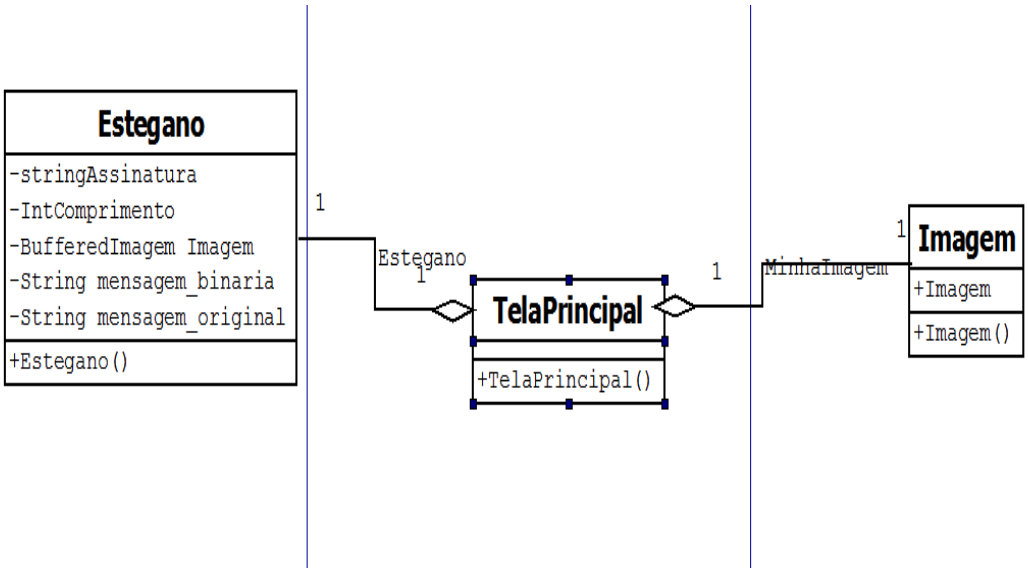

Figura 12- Digrama de Classe
Fonte: Própria autoria.

6.4 Diagrama de Atividades

O diagrama de atividades mostra o fluxo de procedimentos ou atividades que ocorrem em uma determinada classe. As Figuras 13 e 14 demonstram o funcionamento desse diagrama em questão. O diagrama de atividade foi dividido em duas partes para melhor compreensão.

[5] easyUML é uma ferramenta de diagrama UML para NetBeans que fornece recursos para criar e trabalhar facilmente com diagramas UML. Atualmente, ele suporta apenas diagramas de classes que fornecem o editor visual de arrastar e soltar para desenho de diagrama, geração de código Java a partir de diagramas e "engenharia reversa" para criar diagramas de classes a partir do código Java. É muito adequado para o ensino de design de software. Disponível em: http://plugins.netbeans.org/plugin/55435/easyuml

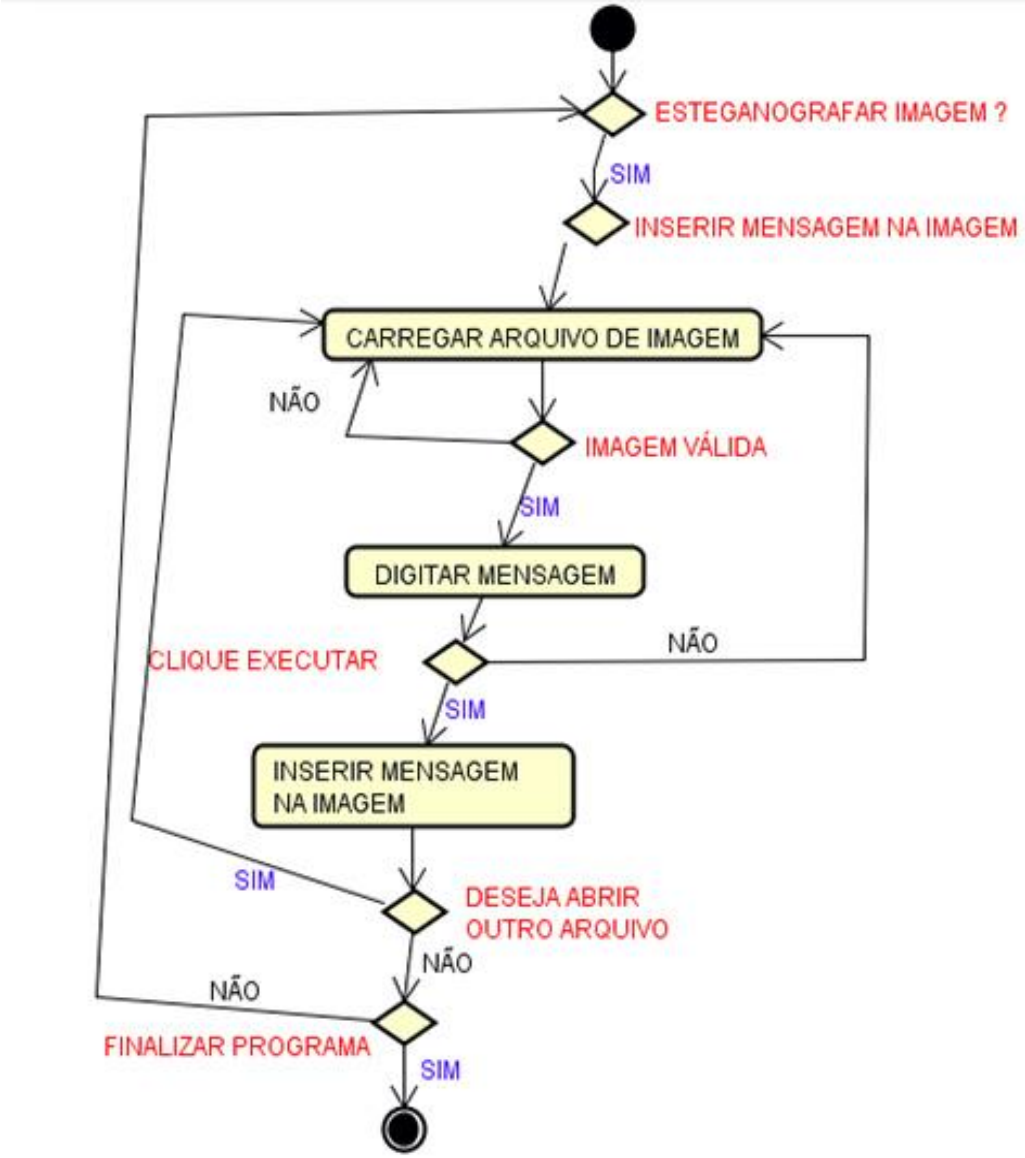

Figura 13– Diagrama de Atividade: Inserção da mensagem na imagem
Fonte: Própria autoria.

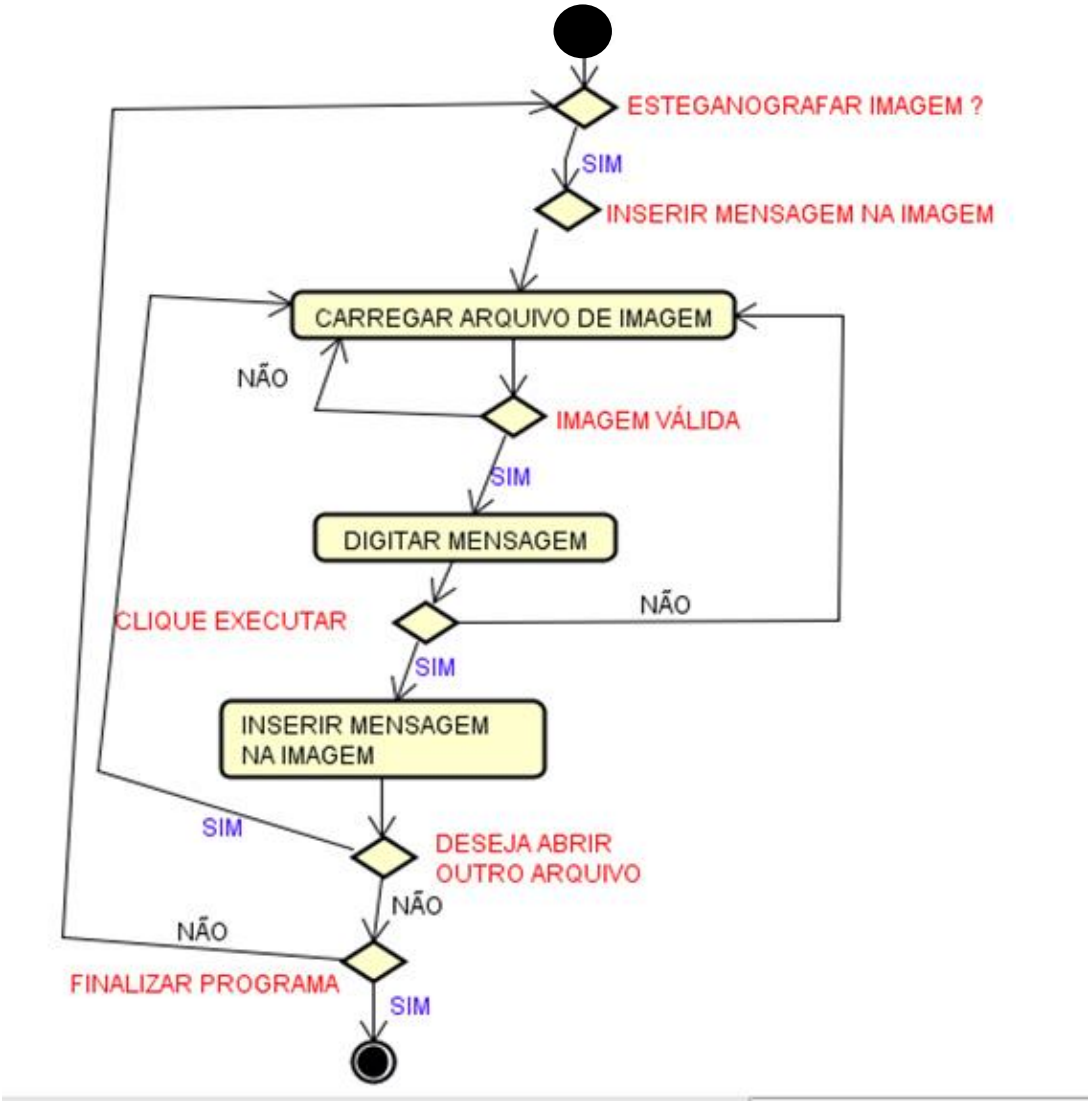

Figura 14- Diagrama de atividade: Remoção da mensagem em imagem
Fonte: Própria autoria.

6.5 Implementação

Nesta seção é apresentada a implementação da ferramenta que foi desenvolvido no ambiente de programação Netbeans IDE 8.0.2, utilizando a linguagem de programação JAVA.

Java por ser uma linguagem orientada a objetos ela facilita a modulação do programa e a sua visualização em um diagrama UML. O que permite manter uma documentação sobre o programa permitindo assim futuras alterações.

Possui também, uma vasta quantidade de APIs além de ser documentada facilitando ao programador a visualização e o entendimento de funcionalidades.

A implementação da Esteganografia através do artefato se dá através de duas etapas. Na primeira é feita uma análise da imagem, o qual contém informações de sua formatação, para saber se este é um arquivo válido e para guardar as principais características que serão usadas para o processamento do algoritmo de Esteganografia.

Em uma segunda fase, o processo de Esteganografia, é feito uma análise dos *bits* menos significativos da imagem, onde será inserida a mensagem ou então onde estarão os dados para a extração da mensagem.

Os processos que estão ligados a Esteganografia como o ocultar e extrair a mensagem da imagem, utilizam tratamento e conversões de binários. A imagem escolhida é lida *pixel* a *pixel*, cada *pixel* com seus 24 *bits* ou 3 *bytes*, de cada *byte* é lido o *bit* menos significativo o conjunto desse bit s dá lugar a mensagem.

Na Figura 15 é mostrada a interface do sistema, que é bastante simples de fácil utilização. Tem um campo para digitar a mensagem e um painel para visualização da imagem escolhida entre outros componentes.

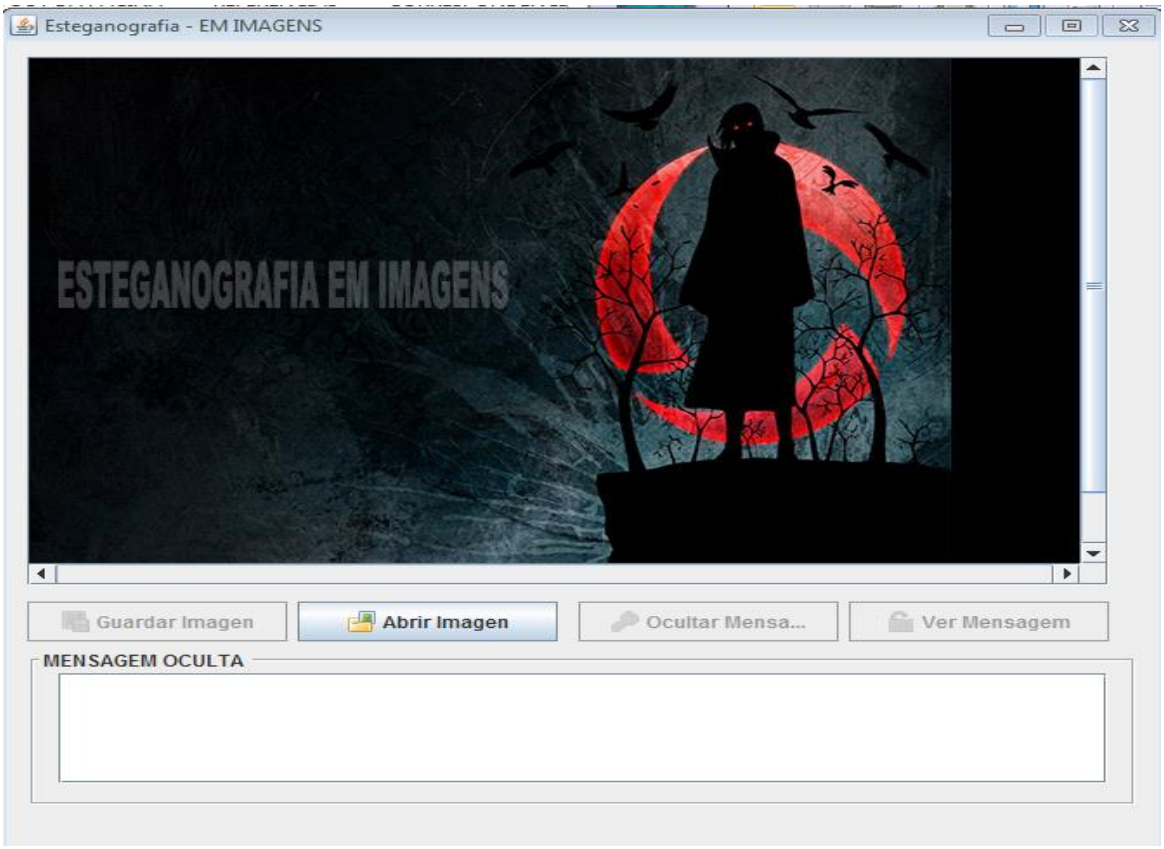

Figura 15– Tela Principal da ferramenta
Fonte: Própria autoria.

A ferramenta necessita apenas de uma imagem para realizar a Esteganografia, a partir dessa imagem é que pode ser extraída ou ocultada uma mensagem. Os botões ver mensagem ou ocultar mensagem ficam desabilitados se não houver nenhuma imagem selecionada e aberta no painel de visualização, caso tenha uma imagem aberta os botões são habilitados menos o de guardar imagem.

Para inserir uma mensagem em uma imagem, todo esse processo é ilustrado na Figura 16, no qual se deseja ocultar a mensagem “Hoje é o grande dia, vamos ao ataque pela tarde...”em uma imagem.

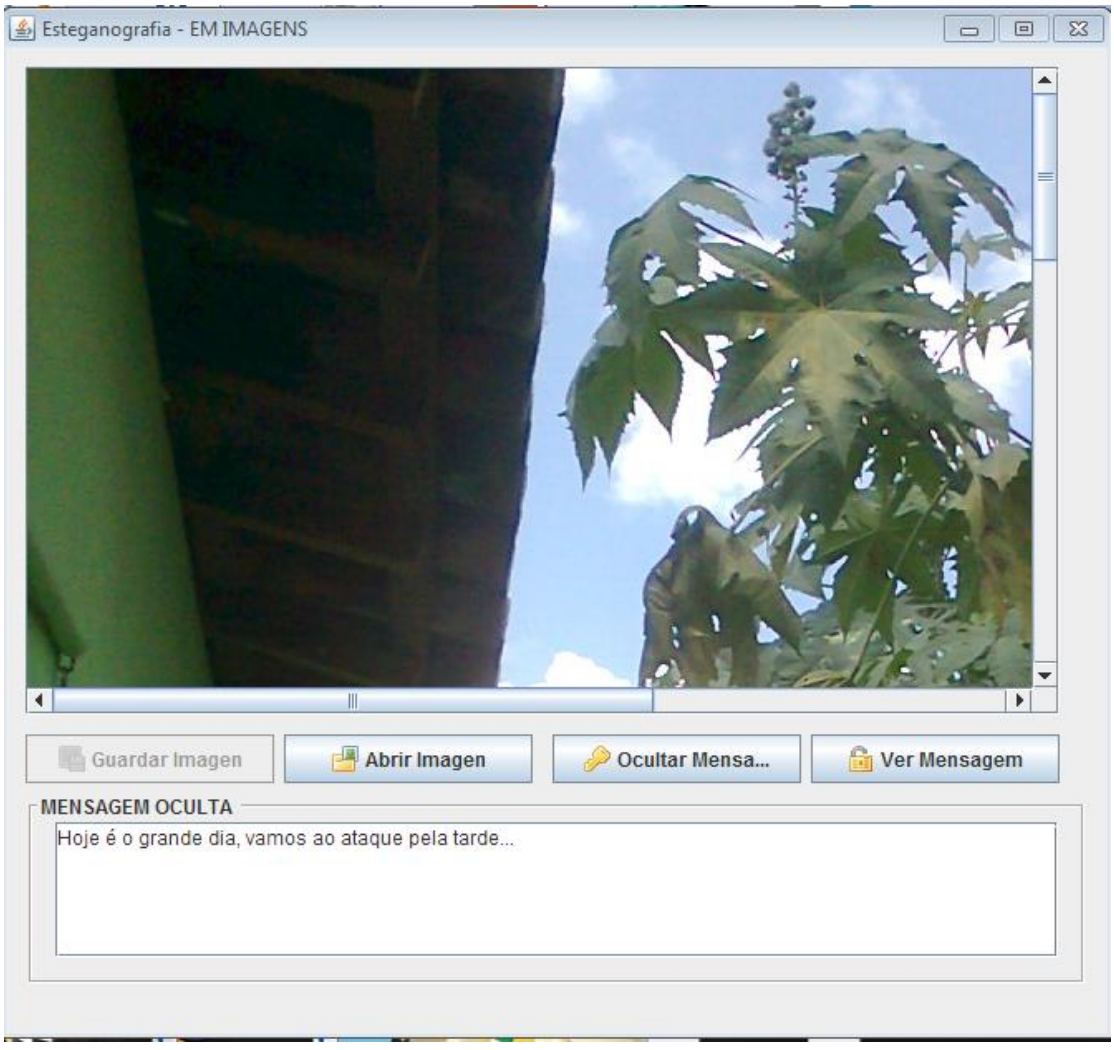

Figura 16– Inserindo uma mensagem na imagem
Fonte: Própria autoria.

Após isso, basta clicar no botão Ocultar Mensagem para ocultar a mensagem na imagem, quando o processo se encerra será apresentada uma mensagem

confirmando que a mensagem está oculta, e habilitando o botão guarda imagem, como mostra a Figura 17.

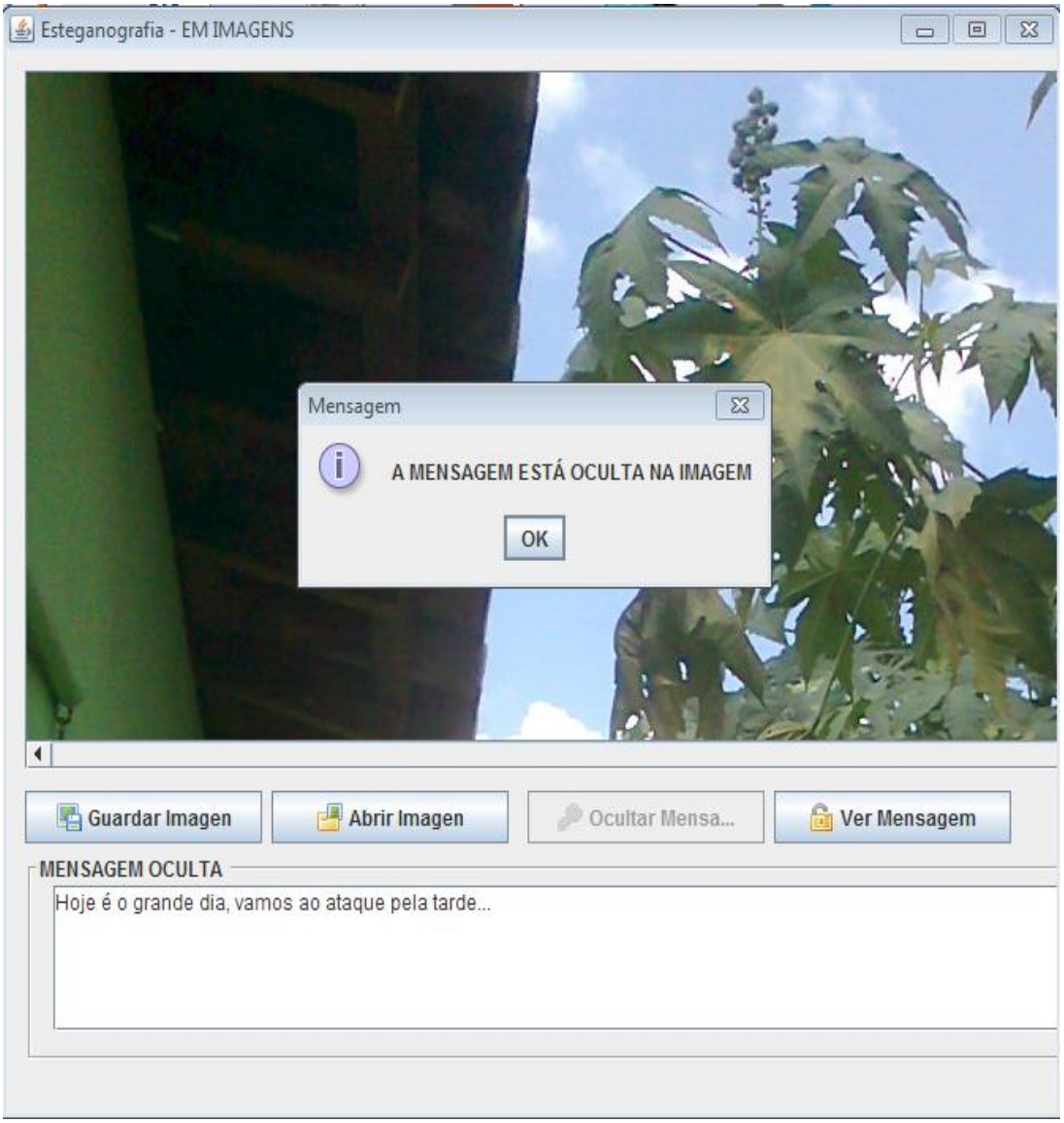

Figura 17– Inserindo uma mensagem na imagem
Fonte: Própria autoria.

Para encerrar o processo é necessário guardar esta imagem que acabou de ser esteganografada gerando assim outra imagem, semelhante à imagem original, como mostra a Figura 18.

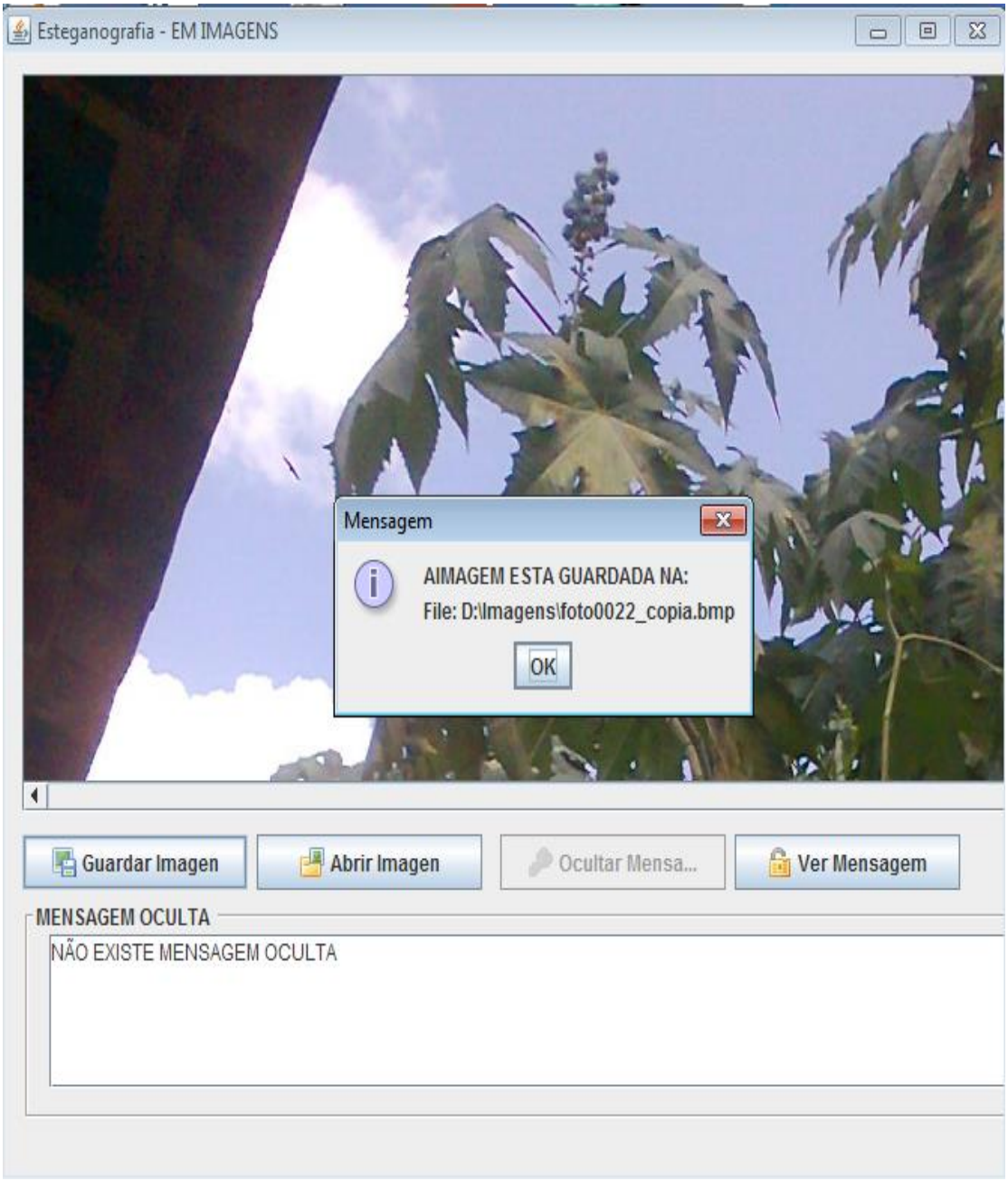

Figura 18– Guardando a imagem
Fonte: Própria autoria.

7 CONCLUSÕES

A Segurança da Informação é um grande desafio em razão de uma grande variedade de tecnicas capazes de quebrar a privacidade. Para torna a transmissão de informações mais seguras e evitar que pessoas não autorizadas tenham acesso a essas informações, diversas tecnicas estão sendo utilizadas, entre elas se inclui a Esteganografia.

Nesse sentido a utilização da Esteganografia pode ser considerada uma proteção e eficiente quando se trata de proteção digital. Já que permite o sigilo entre as comunicações pela rede de computadores ocultando a informação.

Dada à importância do assunto, tornou-se necessário um estudo sobre a Esteganografia e principalmente a sua aplicação em imagens digitais, utilizando-se do método de inserção no ultimo *bit* significativo (LSB), método mais conhecido, na literatura, para o ocultamento de informações em imagens.

Neste ponto a Esteganografia de dados mostrou-se bastante eficaz e muito útil na proteção de direitos autorais, na autenticação de documentos e envio de pequenas mensagens, já para a transmissão de grandes informações o dado a ser oculto no objeto esteganógrafo causa alterações drásticas, portanto de fácil detecção, então é preciso um estudo mais aprofundado.

Outras dificuldades foram encontradas a respeito do desenvolvimento da ferramenta foi observado que em alguns arquivos escolhidos para serem ocultados o processo de extração da mensagem não era feito corretamente, ou seja, a extração do arquivo ocultado feita na imagem não era obtida com sucesso e outra dificuldade encontrada, foi o levantamento de informações quanto as técnicas esteganográficas para uma possível solução para o meu problema de implementação esteganográfico em arquivos de imagem.

Logo, a aplicação da Esteganografia mostrou-se viável quanto ao princípio da Segurança da Informação o da autenticidade é para transmissão de pequenos dados, dados (por exemplo senhas) de forma oculta e segura. Já para o uso em grande escala é necessário mais estudo entorno dos algoritmos esteganográficos.

Contudo, mesmo com suas limitações o uso da Esteganografia cria uma barreira, a mais contra indivíduos que buscam acesso indevido a informação.

7.1 Trabalhos futuros

Como trabalho futuro, pode-se pesquisa outras tecnicas de Esteganografia que possam ser utilizadas tanto em imagens bem como em outros formatos de arquivos como vídeo e áudio de forma eficaz, podendo ser adicionado a Criptografia como meio de uma proteção ainda maior no que se diz respeito sobre a Segurança da Informação.

Além disso criar uma comunicação usando *sockets* para enviar a mensagem oculta pela internet, como também desenvolver aplicativos *mobile* para esteganografia.

REFERÊNCIAS

ABREU, L. F. D. S. **A Segurança da Informação nas Redes Sociais**, 2011. Disponivel em: <http://www.fatecsp.br/dti/tcc/tcc0023.pdf>. Acesso em: 25 Janeiro 2018.

ABREU, LEANDRO FARIAS DOS SANTOS. **A Segurança da Informação nas Redes Sociais**, São Paulo, 2011. 54.

ALBUQUERQUE, R. B. **Esteganografia: Análise de Algoritmos entre Imagens**, Recife, Novembro 2008. 53.

ARAUJO, R. F. D. **Política de Segurança da Informação**, 2014. 68f.

BARRETO, G. L. **Utilização de técnicas anti-forenses para garantir a confidencialidade.**, 2009. Disponivel em: <https://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC%20-%20Gustavo%20Luis%20Barreto.pdf>. Acesso em: 15 Janeiro 2018.

BAUER, F. L. **Decrypted Secrets**. 4º. ed. [S.l.]: Springer, 2002.

CAHÚ, C. B. G. **Uma Abordagem BSP Tree na Esteganografia,** Recife, 2009. Disponivel em: <http://tcc.ecomp.poli.br/20091/TCC_CarlosBruno-bsptree-vers%E3oFinal.pdf>.

CANTANHEDE, H. S. **Esteganografia em Audio e Imagem utilizando a tecnica LSB**. Catalão: [s.n.], 2009.

CARVALHO, D. F. **Exploração Tecnológica para Esteganografia em Vídeos Digitais**, 2005. Disponivel em: <http://stoa.usp.br/diegofdc/files/-1/1303/TCCMonografia.pdf>. Acesso em: 13 Abril 2017.

CARVALHO, D. R. D. S **Segurança da Informação:** Estudo de Caso da Aplicação da Normas NBR/IEC 1779, 2003. Disponivel em: <http://www.unipac.br/site/bb/tcc/tcc-d5997f5e9aa1d5011dbc1a3d29a45109.pdf>. Acesso em: 12 Dezembro 2017.

CASIERRA, J. P. C. **Implementação esteganográfico para inserção de textos em sinais de áudio**, Recife, Março 2009. 134.

CHANDRAMOULI, R. **A Mathematical Approach to Steganalysis**. [S.l.]: [s.n.], 2002.

COLOMBO, L. G. L. **Inserção de texto em imagem GIF**. Brasília: [s.n.], 2006.

COTRIM, G. **Historia Global Brasil E Geral**. São Paulo: Saraiva, 1999.

COUTINHO, P. S. **Esteganografia**, 2008. Disponivel em: <https://www.gta.ufrj.br/grad/08_1/estegano/TcnicasModernas.html>. Acesso em: 17 março 2018.

CRUZ, E. F. D., 2009.

D.AAI, D. B. **Monitor das Fraudes**, 2018. Disponivel em: <http://www.fraudes.org/showpage2.asp?pg=113>. Acesso em: 15 fev. 2018.

DESOKY, A. **Noiseless Steganography:** The Key to Covert Communications. [S.l.]: CRC Press, 2012.

DIEGO FIORI DE CARVALHO, R. G. **Esteganografia Digital:** Uma abordagem baseada em vídeos. Disponivel em: <https://social.stoa.usp.br/articles/0015/3983/StegoVideoDiegoRudinei_final.pdf>. Acesso em: 20 Janeiro 2018.

DUARTE, O. C. M. B. **Esteganografia**. Disponivel em: <https://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html>. Acesso em: 20 Março 20018.

FONSECA, T. C. gta.ufrj.br. **Esteganografia**, 2007. Disponivel em: <https://www.gta.ufrj.br/grad/07_2/thiago_castello/index.html>. Acesso em: 20 Março 2018.

GUIMARÃES, C. R. **CRIPTOGRAFIA PARA SEGURANÇA DE DADOS**, 2001. 50.

HONDA, R. R. **Análise e Implementação de Algoritmos para Manipulação de Esteganografia em Imagens**. Marília: [s.n.], 2011.

HOPPEN, C. F. F. **Esteganografia e Marcas D`água: A busca por agoritmos robustos**, Porto Alegre, julho 2010. 42.

IBGE. IBGE: 94,2% dos brasileiros usam internet para trocar textos e imagens. **ECONÔMICO VALOR**, 2018. Disponivel em: <http://www.valor.com.br/brasil/5337837/ibge-942-dos-brasileiros-usam-internet-para-trocar-textos-e-imagens>. Acesso em: 30 mar. 2018.

JASCONE, F. L. T. **Protótipo de software para ocultar textos criptografados em imagens**, Blumenau, 02 dez. 2003. 63.

JASPER, N. A. **História, Técnicas e classificação de algoritmos esteganográficos**, São Paulo, 2009. 85.

JULIO, E. P. **Esteganogafia e suas Aplicações**. [S.l.]: [s.n.], 2007.

JUNIOR, G. G. D. C. **Teleco Inteligência em Telecomunicações**, 2004. Disponivel em: <http://www.teleco.com.br/pdfs/tutorialdab.pdf>. Acesso em: 19 Março 2018.

KIPPER, G. **Investigator's Guide to Steganography**. [S.l.]: [s.n.], 2003.

KOBUSZEWSK, **A. Protótipo de Software para Ocultar textos compactados em arquivos de áudio utilizando esteganografia**, Blumenal, 06 fev. 2004. 50.

LUCAS, G. **Esteganografia**. Niterói: [s.n.], 2017.

MANDUCA, F. A. **Seguranaça da Informação em Ambientes Organizacionais:** Uma Abordagem Bibliográfica, 2014. Disponivel em: <https://www.google.com.br/search?q=Um+estudo+sobre+abordagens+computacionais+de+esteganografia+e+estegn%C3%A1lise+em+imagens&oq=Um+estudo+sobre+abordagens+computacionais+de+esteganografia+e+estegn%C3%A1lise+em+imagens&aqs=chrome.69i57.815j0j7&sourceid=ch>. Acesso em: 20 Janeiro 2018.

MANDUCA, F. A. **SEGURANÇA DA INFORMAÇÃO EM AMBIENTES ORGAZACIONAIS: UMA ABORDAGEM BIBLIOGRAFICA**, 2014. 35f.

MARCIANO, J. L. P. **Segurança da Informação - uma abordagem social**. Brasília: [s.n.], 2006.

MEUCARRONOVO. **meucarronovo**, 2018. Disponivel em: <https://www.meucarronovo.com.br/blog/para-evitar-falsificacoes-cnh-tera-mudancas.html>. Acesso em: 14 fev. 2018.

MEZZARI, R. **Utilização de Esteganografia para Ampliar Confidencialidade em Sistemas RFID**. Porto Alegre: [s.n.], 2012.

MITNICK, K. **Tecnologia da Informação da Gestão Pública**. Fonte, Minas Gerais, v. 07, n. 04, p. 112, Dezembro 2007.

MOURA, D. R. D. **Ocultação de Texto Criptografado em Imagem JPEG**, Brasília , Novembro 2006. 64.

OLIVEIRA, R. D. **Segurança da Informação nas Organizações**, 2009. Disponivel em: <http://repositorio.uniceub.br/bitstream/235/9932/1/20400835.pdf>. Acesso em: 23 Julho 2017.

PASSOS, H. L. **Esteganografia - Inserção de texto ou de arquivo em vídeo MPEG** , dezembro 2006. 92.

PEIXOTO, M. C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de janeiro: Brasport, 2006.

PETRI, M. **Esteganografia**, Joinville, 16 Dezembro 2004. 56.

PINHEIRO, J. M. S. http://www.projetoderedes.com.br. **Projeto de Redes**, 2005.

RAMÍREZ, D. **Steganogrphy in TCP & IP headers**, 2015. Disponivel em: <https://ddd.uab.cat/pub/tfg/2015/tfg_7618/TFG_danielramirez.pdf>. Acesso em: 28 Julho 2017.

RANGEL, P. E. **Poçítica de segurnça da informação, importante instrumento da gestão corporativa**, Rio de Janeiro, 31 Março 2005. 43.

RANGEL, P. E. **Política de Segurança da Informação, Importante Instrumento da Gestão Corporativa**, 2005. Disponivel em: <http://www.avm.edu.br/monopdf/22/PAULO%20EDUARDO%20RANGEL.pdf>. Acesso em: 4 Março 2017.

REIS, F. A. D. **Esteganografia, a Arte de Ocultar**, 2011. Disponivel em: <http://re.granbery.edu.br/artigos/NDM0.pdf>. Acesso em: 16 fev. 2018.

ROCHA, A. D. R. **Camaleão é um software para esteganografia em imagens estáticas**. [S.l.]: [s.n.], 2003.

ROCHA, A. D. R. **Desenvolvimento de um Software para Segurança Digital Ultilizando Esteganografia**, Lavras, 2003. 30.

SANCHES, F. D. S. C. **Segurança de redes conforme a NBR ISO 27 002**, 2012. 92f.

SCHUTZ, C. A. **SISTEMA DE ESTEGANOGRAFIA EM AUDIO DIGITAL QUE UTILIZA TÉCNICAS EFICIENTES DE INSERÇÃO DE DADOS**, PORTO ALEGRE, 2009. 97.

SECUNDINO, A. A. **Um estudo sobre abordagens computacionais de esteganografia e estegnálise em imagens**, 2013. Disponivel em: <https://www.google.com.br/search?q=UM+ESTUDO+SOBRE+ABORDAGENS+COMPUTACIONAIS+DE+ESTEGANOGRAFIA+E+ESTEGAN%C3%81LISE+EM+IMAGENS&oq=UM+ESTUDO+SOBRE+ABORDAGENS+COMPUTACIONAIS+DE+ESTEGANOGRAFIA+E+ESTEGAN%C3%81LISE+EM+IMAGENS&aqs=chrome.69i57.862j0j7&sourceid=>. Acesso em: 23 Novembro 2017.

SERRANO, M. M. **A comunicação na existência da humanidade e de suas sociedade**, dezembro 2009. Disponivel em: <http://www.periodicos.usp.br/matrizes/article/download/38238/41019>. Acesso em: 19 Março 2018.

SILVA, F. O. B. D. **A Impugnação da Prova Documental no Processo Eletrônico**, 2011. Disponivel em: <https://www.conteudojuridico.com.br/pdf/cj052595.pdf>. Acesso em: 13 Janeiro 2018.

SINGH, S. **O livro dos códigos a ciência do sigilo - do antigo Egito à criptografia quântica**. Rio de Janeir: Record, 2008.

STALLINGS, W. **Network and internetwok security principles and practice**. [S.l.]: [s.n.], 1995.

TANENBAUM, A. S. **Redes de Computadores**. Quarta edição. ed. Amsterdam, Holanda: Campos, v. 4, 1996.

TANENBAUM, A. S. **Computer Networks**. 4º. ed. amsterdam: [s.n.].

TEIXEIRA, M. R. **ESTEGANOGRAFIA EM ARQUIVOS TEXTOSE TÉCNICAS DE DETCÇÃO**, Porto Alegre, 2011. 41.

TEOTÔNIO, Í. D. **Entendendo os Fundamentos da Segurança da Informação**. **Profissionais de TI PTI**, 2013. Disponivel em:

<https://www.profissionaisti.com.br/2013/10/entendendo-os-fundamentos-da-seguranca-da-informacao/>. Acesso em: 11 fevereiro 2018.

THIAGO CASTELLÓ FONSECA, V. T. V. **Assinatura Digital**. Disponivel em: <https://www.gta.ufrj.br/grad/07_1/ass-dig/index.html>. Acesso em: 18 Fevereiro 2018.

TRITHEIM, J. **Steganographia:** Esta é uma arte secreta. Frankfurt: [s.n.], v. 3, 1621.

TRITHEMIUS, J. **A Arte Certa de Divulgação a Intenção de uma Mente para quem está Ausente através da Escrita Secreta**, 1606. Disponivel em: <http://trithemius.com/steganographia-english/>. Acesso em: 10 Janeiro 2018.

Uma Abordagem BSP Tree na Esteganografia, 2009. Disponivel em: <https://www.google.com.br/search?q=Uma+Abordagem+BSP+Tree+na+Esteganografia&oq=Uma+Abordagem+BSP+Tree+na+Esteganografia&aqs=chrome.69i57.947j0j7&sourceid=chrome&ie=UTF-8>. Acesso em: 20 Janeiro 2018.

VANESSA LIMA, L. E. M. E. F. A. B. Redes de Frequência Única. **Revista SET**, 2013. Disponivel em: <http://www.set.org.br/revista-da-set/redes-de-frequencia-unica-2/>. Acesso em: 20 Março 2018.

WAYNER, P. **Disappearing Cryptography:** Information Hiding: Steganography & Watermarking. 2º. ed. San Francisco: Morgan Kaufmann, 2002.

YARI, J. **Esteganografia**. [S.l.]: [s.n.], 2008.

APÊNDICES

APÊNDICE A – CLASS ESTEGANOS

Class Esteganos

java.lang.Object

net.viana.SegDaInforma.Esteganos

---

public class **Esteganos**
extends java.lang.Object

RESUMO

CAMPOS

MODIFICADOR E TIPO	CAMPO E DESCRIÇÃO
private java.lang.String	**assinaturaImagem** a assinatura da imagem permite pecorrer uma imagem e detectar uma mensagem oculta
private int	**b**
private int	**Comprimento**

	armazenara o tamanho da mensagem mais o tamanho do comprimento da imagem(2) mais seu proprio tamanho (2)
private int	**contador**
private java.awt.Color	**cor**
private int	**g**
private java.awt.image.BufferedImage	**Imagem** a imagem
private java.lang.String	**mensagem_binario** armazenar a mensagem decomposta em uma matriz binária
private java.lang.String	**mensagem_original**
private int	**r**

Construtor

Todos os métodos

Modificador e Tipo	Métodos e Descrição

java.awt.image.BufferedImage	**getImagem**()
private java.lang.String	**getLSB**(java.lang.String binario)
private java.lang.String	**getMensagemParaBinario**(java.lang.String mensagem)
java.lang.String	**getMensagemParaImage**(java.awt.image.BufferedImage f)
private java.lang.String	**getMensagemParaString**(java.lang.String[] mensagem)
private boolean	**lerAssinaturaNaImag**(java.awt.image.BufferedImage f) ler os primeiros 6 pixels para formar os bits necessários para "jc" retorna TRUE / FALSE
private void	**LerComprimentoDaMensagem**(java.awt.image.BufferedImage f) ler a parte correspondente ao tamanho total da mensagem
void	**OcultarMensagem**(java.awt.image.BufferedImage f, java.lang.String mensagem) o nome ja diz tudo
private java.lang.String	**paraBinary**(byte caracter)
private java.lang.String	**RecolocarLSB**(java.lang.String corRGB)
private void	**SetMensagem**(java.lang.String mensagem) Dada a Mensagem (String) que deseja ocultar, que se junta ao assinatura da Imagem como o comprimento total de Mensagem

private java.lang.String	**toChar**(java.lang.String binario)
private int	**toCharInt**(java.lang.String binario)

Construtor and Descrisção
Esteganos()

Metodos

Métodos herdadosda class java.lang.Object

clone, equals, finalize, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait

Campos Detalhes

- *assinaturaImagem*

private java.lang.String assinaturaImagem

a assinatura da imagem permite pecorrer uma imagem e detectar uma mensagem oculta

- *Comprimento*

private int Comprimento

armazenara o tamanho da mensagem mais o tamanho do comprimento da imagem(2) mais seu proprio tamanho (2)

- *Imagem*

private java.awt.image.BufferedImage Imagem

a imagem

- *r*

private int r

- *g*

private int g

- *b*

private int b

- *cor*

private java.awt.Color cor

- *mensagem_binario*

private java.lang.String mensagem_binario

armazenar a mensagem decomposta em uma matriz binária

- *mensagem_original*

private java.lang.String mensagem_original

- *contador*

private int contador

Constructor Detail

- *Esteganos*

public Esteganos()

Método Detalhes

- *SetMensagem*

  private void SetMensagem(java.lang.String mensagem)

  Dada a Mensagem (String) que deseja ocultar, que se junta ao assinatura da Imagem como o comprimento total de Mensagem

- *OcultarMensagem*

- public void OcultarMensagem(java.awt.image.BufferedImage f,
  java.lang.String mensagem)

  o nome ja diz tudo

- *lerAssinaturaNaImag*

  private boolean lerAssinaturaNaImag(java.awt.image.BufferedImage f)

  ler os primeiros 6 pixels para formar os bits necessários para "jc" retorna TRUE / FALSE

- *LerComprimentoDaMensagem*

  private void LerComprimentoDaMensagem(java.awt.image.BufferedImage f)

  ler a parte correspondente ao tamanho total da mensagem

- *getMensagemParaImage*

  public java.lang.String getMensagemParaImage(java.awt.image.BufferedImage f)

- *getImagem*

  public java.awt.image.BufferedImage getImagem()

- *paraBinary*

private java.lang.String paraBinary(byte caracter)

- *toChar*

private java.lang.String toChar(java.lang.String binario)

- *toCharInt*

private int toCharInt(java.lang.String binario)

- *getMensagemParaBinario*

private java.lang.String getMensagemParaBinario(java.lang.String mensagem)

- *getMensagemParaString*

private java.lang.String getMensagemParaString(java.lang.String[] mensagem)

- *RecolocarLSB*

private java.lang.String RecolocarLSB(java.lang.String corRGB)

- *getLSB*

private java.lang.String getLSB(java.lang.String binario)

APÊNDICE B – CÓDIGO FONTE

Código Fonte

```
package net.viana.SegDaInforma;
        import java.awt.Color;
        import java.awt.image.BufferedImage;

        public class Esteganos {

            /***a assinatura da imagem permite percorrer uma imagem e
            detectar uma mensagem oculta***/
            private String assinaturaImagem="jc";

            /***armazenara o tamanho da mensagem mais o tamanho do
            comprimento da imagem(2) mais seu  proprio tamanho (2)***/
            private int Comprimento=0;
            /***a imagem***/
            private BufferedImage Imagem=null;
            private int r,g,b;
            private Color cor;
            /***armazenar a mensagem decomposta em uma matriz binária***/
            private String mensagem_binario;
            private String mensagem_original;
            private int contador = 0;

            public Esteganos(){}

           /*** Dada a Mensagem (String) que deseja ocultar,
            que se junta ao assinatura da Imagem como o comprimento total de Mensagem ***/
            private void SetMensagem(String mensagem){
                String bi="";
```

```
      /***o tamanho total de Mensagem
      Comprimento = mensagem.length() + assinaturaImagem.length() * 2;
      transforma o valor inteiro do comprimento num valor binário***/
      for( int i = 15; i>=0; i--){
         bi = bi + ( ( ( Comprimento & ( 1<<i ) ) > 0 ) ? "1" : "0" ) ;
      }
      /***concatenar toda Mensagem ***/
      mensagem_binario = getMensagemParaBinario(assinaturaImagem) + bi
            + getMensagemParaBinario(mensagem);
   }

   /*** o nome ja diz tudo ***/
   public void OcultarMensagem(BufferedImage f,String mensagem){
      int tmp_count=0;
      //chamada para um procedimento privado
      SetMensagem(mensagem);
      //cria uma imagem com a qual você trabalha
      Imagem = new BufferedImage
      (f.getWidth(), f.getHeight(), BufferedImage.TYPE_INT_RGB);
/***pecorre todo o pixel da imagem por pixel adicionando 1 e 0 nos pedaços LSB ***/
      for(int fila=0;fila<Imagem.getHeight();fila++){
        for(int coluna=0;coluna<Imagem.getWidth();coluna++){
    /***pixel de núcleo(ocultar a mensagem) é obtido em coordenadas (i, j)***/
            cor = new Color( f.getRGB(coluna, fila) );
            /***enquanto há uma Mensagem, ele passa a substituir LSB***/
            if(tmp_count<=this.mensagem_binario.length()){
/***Eles são convertidos em seu equivalente binário(mensagem para binario)***/
               String red = paraBinary((byte) cor.getRed() );
               String verde = paraBinary((byte) cor.getGreen() );
               String azul = paraBinary((byte) cor.getBlue() );
               /***ele substitui os últimos bit***/
               red = RecolocarLSB(red);
               verde = RecolocarLSB(verde);
               azul = RecolocarLSB(azul);
               /***mudanças de binário para inteiro***/
```

```
                r = Integer.parseInt(red ,2);
                g = Integer.parseInt(verde ,2);
                b = Integer.parseInt(azul ,2);
            }else{
               r = cor.getRed();
               g = cor.getGreen();
               b = cor.getBlue();
            }
            //colocado na nova imagem com valores de preto e branco
            Imagem.setRGB(coluna, fila, new Color(r,g,b).getRGB());
            tmp_count+=3;
       }
     }
  }

/***ler os primeiros 6 pixels para formar os bits necessários
 para "jc" retorna TRUE / FALSE***/
private boolean lerAssinaturaNaImag(BufferedImage f){
    boolean ok=false;
    String t = "";
     for(int j=0;j<6;j++){
         cor = new Color(f.getRGB(j, 0));
         String red = paraBinary((byte) cor.getRed() );
         String verde = paraBinary((byte) cor.getGreen() );
         String azul = paraBinary((byte) cor.getBlue() );
         red = getLSB(red);
         verde = getLSB(verde);
         azul = getLSB(azul);
         t = t + red + verde + azul;
     }
     if( toChar(t.substring(0, 8)).equals("j")
             &&  toChar(t.substring(8, 16)).equals("c") ){
         ok=true;
     }
    return ok;
```

```
}

/***ler a parte correspondente ao tamanho total da mensagem ***/
private void LerComprimentoDaMensagem(BufferedImage f){
    String t = "";
    for(int j=5;j<12;j++){
       cor = new Color(f.getRGB(j,0));
       String red = paraBinary((byte) cor.getRed() );
       String verde = paraBinary((byte) cor.getGreen() );
       String azul = paraBinary((byte) cor.getBlue() );
       red = getLSB(red);
       verde = getLSB(verde);
       azul = getLSB(azul);
       t = t + red + verde + azul;
    }
    this.Comprimento = toCharInt(t.substring(1, 17));
  }

  /*  */
  public String getMensagemParaImage(BufferedImage f){
    //busca na imagem para ver  se tem na Imagem  a assinatura
    mensagem_original="NÃO EXISTE MENSAGEM OCULTA";
    //se a assinatura da Imagem existe continua
    if( lerAssinaturaNaImag(f) ){
       //chamada de função
       LerComprimentoDaMensagem(f);
       //extrai os bits de imagem e remodela a mensagem oculta
       String[] s = new String[this.Comprimento];
       String tmp="";
       /***pecorre a imagem pixel pixel x inteira***/
       for(int fila=0;fila<f.getHeight();fila++){
          for(int coluna=0;coluna<f.getWidth();coluna++){
        //pixel de núcleo(contem a mensagem) é obtido em coordenadas (i, j)
             cor = new Color(f.getRGB(coluna, fila));
             //Eles são convertidos em seu equivalente binário
```

```
                String red = paraBinary((byte) cor.getRed() );
                String verde = paraBinary((byte) cor.getGreen() );
                String azul = paraBinary((byte) cor.getBlue() );
                /***e obtido os bits LSB***/
                red = getLSB(red);
                verde = getLSB(verde);
                azul = getLSB(azul);
                //quando  terminar de ler obtem a saída da mensagem
                if(tmp.length()<=(this.Comprimento*8)){
                    tmp = tmp + red + verde + azul;
                }else{
                    break;
                }
            }
        }
        /***String obtido a partir de 1 e 0, é separado em uma matriz de bytes***/
        int count_tmp =0;
        for(int a=0; a<(this.Comprimento*8);a = a + 8){
            s[count_tmp]=tmp.substring(a, a + 8);
            count_tmp++;
        }
        //
        //chama um método  para reconstruir a mensagem
        mensagem_original = getMensagemParaString(s);
    }
    return mensagem_original;
}

 public BufferedImage getImagem(){
    return this.Imagem;
}

private String paraBinary(byte caracter){
    byte byteDeCaracter = (byte)caracter;
    String binario="";
```

```
    for( int i = 7; i>=0; i--){
       binario = binario + ( ( ( byteDeCaracter
             & ( 1<<i ) ) > 0 ) ? "1" : "0" ) ;
    }
    return binario;
}

/* converte um valor de caractere em binário */
private String toChar(String binario){
    int i = Integer.parseInt(binario ,2);
    String aChar = new Character((char)i).toString();
    return aChar;
}

private int toCharInt(String binario){
    int i = Integer.parseInt(binario ,2);
    return i;
}

/*   decompõe  em uma String com
     binário equivalente */
private String getMensagemParaBinario(String mensagem){
    String mb = "";
    char[] mensagem_tmp = mensagem.toCharArray();
    for(int i=0; i<mensagem_tmp.length;i++){
       mb = mb + paraBinary((byte) mensagem_tmp[i]);
    }
    return mb;
}

/*reconstrói a mensagem em uma matriz binária para um String */
private String getMensagemParaString(String[] mensagem){
    String mo ="";
    //ler a partir do  5 elemento  e as quatro primeiras são
    //assinaturaImagem e Mensagem comprimento
```

```
        for(int i=4; i<mensagem.length;i++){
            mo = mo + toChar(mensagem[i]) ;
        }
        return mo;
    }

    /* substitui o bit menos significativo com um bits da mensagem */
    private String  RecolocarLSB(String corRGB){
        if(contador < mensagem_binario.length()){
            corRGB = corRGB.substring(0,7)
                    + mensagem_binario.substring(contador, contador+1);
            contador++;
        }
        return corRGB;
    }

    private String getLSB(String binario){
        return binario.substring(7, 8);
    }

}
```