CENTRO UNIVERSITÁRIO SAGRADO CORAÇÃO

ANÁLISE E IMPLEMENTAÇÃO DE TÉCNICAS DE ESTEGANOGRAFIA EM IMAGENS: SEGURANÇA E PRIVACIDADE NA INTERNET

BAURU
2021

NATHAN CASARINI BOLONHA

ANÁLISE E IMPLEMENTAÇÃO DE TÉCNICAS DE ESTEGANOGRAFIA EM IMAGENS: SEGURANÇA E PRIVACIDADE NA INTERNET

Monografia de Iniciação Científica apresentada a Pró-Reitoria de Pesquisa e Pós-Graduação.

Orientador: Prof. Dr. Elvio Gilberto da Silva

BAURU

2021

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

Bolonha, Nathan Casarini

B693a

Análise e implementação de técnicas de esteganografia em imagens: segurança e privacidade na internet / Nathan Casarini Bolonha. -- 2021.

55f. : il.

Orientador: Prof. Dr. Elvio Gilberto Da Silva

Monografia (Iniciação Científica em Ciência da Computação) - Centro Universitário Sagrado Coração - UNISAGRADO - Bauru - SP

1. Esteganografia. 2. Segurança da Informação. 3. Criptografia. 4. Técnicas de Esteganografia. 5. Imagens. I. Silva, Elvio Gilberto da. II. Título.

Elaborado por Lidyane Silva Lima - CRB-8/9602

RESUMO

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

Palavras-chave: Esteganografia. Segurança da Informação. Criptografia. Técnicas de Esteganografia. Imagens.

ABSTRACT

Information security is a topic of great importance in the area of information technology. Considering the great technological advance, issues such as confidentiality, integrity and privacy are crucial points that must be maintained for Internet users, who are connected in various ways through the transmission of thousands of pieces of information, whether personal or even commercial, the interception of these messages in an illegal way could generate serious consequences. Steganography is synonymous with hidden writing, which consists of hiding some type of information in files such as images, videos, sounds and texts. It can be compared to cryptography, which consists in transmitting information securely to the recipient. The intention of these techniques is that the transmission of information is done securely and that there is no intervention from other users. Experts in the field of digital security are increasingly seeking to develop digital security techniques to combat the large mass of cybercrimes that are also evolving in the digital world. This paper presents a theoretical reference on information security and the use of steganography. The proposal of this work consisted of practical tests using three steganography tools to insert a message in some predefined image formats, so that it was possible to evaluate the efficiency of each tool, and thus collaborate with stakeholders in the area of digital information. After the results were generated, they were analyzed so that it was possible to identify which tool presented the most satisfactory results.

Keywords: Steganography. Information Security. Cryptography. Steganography techniques. Images.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A tecnologia é algo que tem evoluído muito. A cada dia que se passa ela está mais e mais presente nos mais diversos campos, já é possível ver o avanço da tecnologia em hospitais, no *business*, nas escolas etc. E tem ajudado muito o homem a progredir mais rapidamente, já que com tarefas que a 20 anos demoravam meses, dias ou horas, tornaram-se possíveis através de um clique. Porém por outro lado o homem foi se tornando cada vez mais refém e dependente dessa própria tecnologia.

E com a expansão da tecnologia a informação tornou-se bem mais acessível, sendo considerada sinônimo de poder, já que saber uma pequena coisa a mais que o concorrente se tornou diferencial e o que dita o sucesso e o fracasso de uma empresa. Em uma sociedade informatizada como a de hoje, o maior patrimônio de uma empresa é a sua informação (DIAS, 2000), ou seja, tornou-se inaceitável perder informação e o mais que essencial o total sigilo delas.

Essa expansão também trouxe uma vasta gama de novos crimes, como roubo de informação e deterioração dela, além do mais criou-se uma dúvida: como transmitir algo pela rede sem que todos possam ficar sabendo? Então foi necessário a criação de técnicas e ferramentas para que essas informações pudessem chegar ao seu destino final com confidencialidade, integridade e autenticidade intactas - sendo isso possível de duas maneiras, através da criptografia que oferece um conjunto de princípios e técnicas empregadas para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas e da esteganografia que é uma técnica que consiste em esconder um arquivo dentro do outro, de forma criptografada. Porém, ao contrário da criptografia, que visa deixar as mensagens incompreensíveis, esta tem como objetivo esconder a existência de uma determinada mensagem, camuflando-a dentro de outros arquivos tais como: imagens, músicas, vídeos ou textos. Sendo assim, é possível, por exemplo, esconder mensagens dentro de imagens sem que outras pessoas desconfiem que existe alguma coisa escrita ali.

Apesar de se falar-se mais sobre a Criptografia, tanto na literatura quanto nas demais fontes, e também ser bem mais usada na informática, muitos ainda consideram a esteganografia uma técnica mais segura, visto que a esteganografia muitas vezes passa desapercebida e a criptografia é mais fácil de ser notada.

2 OBJETIVOS

A seguir são apresentados o objetivo geral e específicos que norteiam esta pesquisa.

2.1 OBJETIVO GERAL

Aplicar a esteganografia utilizando ferramentas esteganográficas apresentando suas técnicas de inserção, análise e detecção de dados e informações em imagens contribuindo assim com usuários que tenham interesse na área de segurança digital, com a intenção de adquirir novos conhecimentos, assim como, peritos forenses, que tem por necessidade tais informações.

2.2 OBJETIVOS ESPECÍFICOS

a) Estudar métodos de esteganografia e perícia forense digital;
b) pesquisar e selecionar ferramentas que utilizem técnicas diferentes de esteganografia;
c) aplicar e analisar métodos de esteganografia utilizando as ferramentas selecionadas;
d) comparar a funcionalidade dos métodos aplicados entre as ferramentas propostas;
e) verificar a integridade e a segurança dos dados que foram inseridos nosarquivos;
f) apresentar os resultados e comparativos apontando as características e funcionalidades das ferramentas utilizadas.

3 JUSTIFICATIVA

Algumas das aplicações de esteganografia são escapar da censura, aumentar a banda de comunicação, substituir códigos de barras por informações que são apenas visíveis e decodificadas por celulares, colocar dados de pacientes embutidos em seus exames devido a necessidade de confidencialidade, ao mesmo tempo mantendo uma ligação entre os dados e o exame.

Todavia, a esteganografia pode ser usada incorretamente. Relatos dão conta de que ela também é utilizada para troca de mensagens de redes terroristas, embora estudos não tenham encontrado evidências disso. No entanto, exemplos de extração de informações confidenciais de empresas, sem seu conhecimento e divulgação pornografia infantil na Internet já são realidade.

Além disso, em atividades militares, a esteganografia é muito utilizada para esconder um sinal contendo comunicação secreta ou informação. Isto é, a simples descoberta de uma mensagem secreta discrimina a existência de um inimigo e a posição dele. Sendo assim, a aplicação da criptografia aliada à esteganografia utilizando técnicas como modulação em espalhamento de espectro dificulta a descoberta destes sinais.

A esteganografia também é capaz de burlar diversos níveis de segurança. Por exemplo, em redes com vários níveis de segurança, um programa malicioso é capaz de infiltrar-se nesse sistema e ir passando entre os níveis de segurança, dos inferiores aos superiores. Ao atingir o nível desejado, ele é capaz de enviar informações sigilosas para níveis de segurança menores utilizando técnicas de ocultamento para esconder as informações confidenciais desejadas. Assim, o sistema acreditará que os arquivos com essas informações são arquivos comuns e poderão trafegar pelos níveis de segurança livremente até os menos seguros, onde sua extração será mais fácil.

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

Com base nesse contexto, o presente trabalho tem como intuito contribuir com interessados na área de segurança, como por exemplo peritos forenses, ou até mesmo estudantes das áreas de tecnologia da informação, técnicas de inserção,

análise e detecção de dados e informações em imagens, bem como, estabelecer comparativos de ferramentas de esteganografia, que possam ser úteis para futuros trabalhos, e para o uso do perito forense, que tem por necessidade conhecere explorar as diversas técnicas existentes de análise de informações digitais, que a princípio foram desenvolvidas com o objetivo de manter a integridade e a segurança da informação.

4 REVISÃO DA LITERATURA

A seguir serão apresentados alguns tópicos iniciais que norteiam o desenvolvimento desta pesquisa.

4.1 EVOLUÇÃO DA INTERNET

A internet que é um dos meios de comunicação mais usados do mundo, independente das questões financeiras e sociais é fato que ela se tornou essencial. Foi criada em meados da Segunda guerra mundial, tendo por objetivo o rastreamento de informações, para que os pontos inimigos pudessem ser atacados com maior eficaz e precisão.

Por volta de 1969, nos Estados Unidos, interligava laboratórios de pesquisas do departamento Norte-Americano, no auge da Guerra Fria, porém o termo Internet ainda não existia, nesse tempo essa rede era conhecida como “ARPHANET” (SILVA, 2001). Posteriormente a isso, o termo Internet foi criado, e durante cerca de duas décadas ela ficou restrita ao ambiente acadêmico e científico, e aos poucos foram sendo ampliados a outros países (TAIT, 2007).

Em 1987 a internet foi liberada para uso comercial, porém só se tornou conhecida após a criação da Web, que ocorreu em 1991 e servia para conectar laboratórios e exibir documentos científicos de forma simples. No Brasil essa tecnologia só foi chegar em 1994, com acessos discados e fins comerciais, mas entraram em 1995 (TAIT, 2007).

A internet evoluiu e tem evoluído a cada dia, fazendo parte do dia a dia de cada um, seja no trabalho, no lazer, nos estudos, com objetivo de proporcionar cada vez maior estabilidade e segurança aos seus usuários, entretanto, foi necessária a criação de técnicas de segurança, para que se pudesse confiar dados a uma rede, já que esses dados transitam em vários lugares antes de chegar ao seu destinatário final.

4.2 SEGURANÇA DA INFORMAÇÃO

Graças ao avanço tecnológico a comunicação está muito mais acessível e disseminada. A informação tornou-se algo essencial, visto que é a forma de transmitirmos as pessoas o que pensamos, sentimos e até mesmo acreditamos.

A internet tem sido um dos meios mais usados de se transmitir essa informação, substituindo até os meios mais convencionais e tradicionais, como as revistas jornais e programas televisivos, por ser muito mais acessível, podendo ser acessada em qualquer hora não sendo necessário aguardar o próximo capítulo ou horário para receber informações “quentes” e hoje em dia podendo ser acessada de qualquer lugar através de dispositivos móveis como o celular, notebooks, tablets, etc. Além de ser um meio totalmente decentralizado de construção de informação, visto que a internet em si não pertence a nenhuma instituição privada e há milhões de opções de fontes confiáveis para que a informação possa ser conferida e comparada para averiguar sua veracidade.

Segundo Kolling ([20--]), quando nos referimos a segurança da informação, não estamos tratando apenas da internet, mas também dos demais meios de comunicação. Sabendo-se que a internet e uma das principais vias de informação é necessário se atentar para três características segundo o autor supracitado:

a) **confidencialidade**: trata-se de entregar a informação somente ao destinatário e garantir que pessoas indesejadas ou não autorizadas não tenham acesso a essa informação;
b) **integridade**: entregar a informação original ao remetente, sem qualquer tipo de alteração durante a transmissão e impedir que o documento sejaalterado ou até mesmo apagado por terceiros;
c) **disponibilidade**: a informação deve estar disponível para aqueles que tenham a devida permissão de acesso a qualquer momento.

Para que exista segurança dentro de uma empresa é necessário que exista organização e uma política de segurança extremamente bem estabelecida, impondo regras e tonando clara a extrema importância da informação, desde que ela é criada, a etapa de transferência, até que ela chegue ao seu destinatário final (BOTURA,

2014).

É possível realizar praticamente tudo pela internet, e, transações bancárias e comerciais estão incluídas nesse contexto, evitando claro, fila, trânsito, e demais variáveis que fazem o indivíduo perder tempo e dinheiro, visto que no mundo atual tais palavras se tornam praticamente sinônimos. Mas essas vantagens também tornam o ambiente mais propicio para que o usuário se sinta cada vez mais confortável e acabe sendo um pouco menos cuidadoso, abrindo assim brechas para cibercriminosos[1] e um aumento nos crimes virtuais.

4.2.1 Assinatura digital

A assinatura digital tem como intuito conservar a segurança, integridade e procedência da do documento, ou seja, assegurar que o documento não seja modificado entre a emissão e a recepção e averiguar se quem recebeu ele é realmente quem deveria tê-lo recebido.

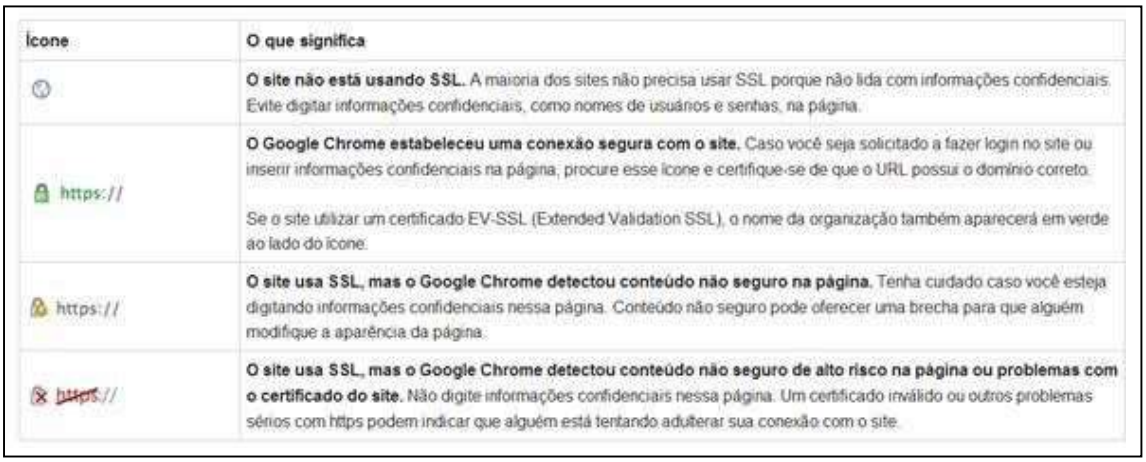
Para receber uma assinatura digital, é preciso que o usuário contate o órgão vigente solicitando uma chave privada, que no caso do Brasil é o Instituto Nacional de Tecnologia da Informação, essa chave possui um conjunto criptografado de bits que permite ao usuário habilitar apenas algumas pessoas selecionadas a enviar e receber dados. Obtendo uma chave privada o usuário poderá repassar dados com a sua própria identidade, se for uma chave pública o usuário poderá acessar dados e repassá-los a outras pessoas, porém constatara a sua identificação do verdadeiro emissor do documento, garantindo assim a responsabilidade do documento a ele (CARVALHO, [20--]).

Para transmitir a informação de maneira segura é preciso usar um *hash*, que é responsável por criptografar os dados e gerar uma identidade única para os dados usados. Após isso é gerado e emitido um certificado para que seja estabelecida uma comunicação entre os usuários, com a condição de que pelo menos um deles tenham a chave privada ou seja a chave simétrica e o outro possua a chave pública, ou seja, assimétrica (GAZZARRINNI, 2012).

Ainda segundo Gazzarrinni (2012), cada *browser* identifica cada problema de maneira diferente, eles conferem os certificados dos sites de acessados a todo o momento. Se houver a falha na verificação de algum site, aparecerá um aviso (Figura

1) comunicando ao usuário e lhe perguntando se ele deseja dar continuidade aquela conexão ou não, tornando o usuário total responsável, caso ocorra algum problema.

Figura 1 - Certificados de autenticação



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

Fonte: Reprodução/Google (2014).

4.2.2 Protocolo de autenticação

A autenticação em si é a forma com que o processo confirma a identificação de um usuário ou ferramenta. Os protocolos de segurança têm por sua função validar se uma página de web ou programa é seguro, verificar *logins,* como nome de usuário e senha necessários para acessar algum tipo de conta, além de autenticar certificados e assinaturas digitais (MICROSOFT, 2005). A Figura 2 ilustra este contexto.

Figura 2 – Protocolos de autenticação

(continua)

PROTOCOLOS DE AUTENTICAÇÃO	DESCRIÇÃO
Autenticação Kaberos V5	Um protocolo usado com uma senha ou um cartão inteligente para *logon* interativo. É também o método padrão de autenticação de rede para serviços.

(conclusão)

Autenticação SSL/TLS	Um protocolo usado quando um usuário tenta acessar um servidor web seguro.
Autenticação NTLM	Um protocolo usado quando o cliente ou servidor usa uma versão anterior doWindows.
Autenticação Digest	A autenticação *Digest* transmite credenciais através da rede como um *hash* MD5 ou *Message Digest*.
Autenticação de passaporte	A autenticação de passaporte é um serviço de autenticação de usuário que oferece *logon* único.

Fonte: Microsoft (2005).

É possível perceber que o número de técnicas computacionais que buscam melhorar a experiência e segurança do usuário é diário, mas esse avanço também traz novas falhas e meios de invadir e roubar informações de forma maliciosa, tornando-se cada vez mais importante investir em pesquisa e descoberta de novos meios para melhorar mais e mais a segurança dos dados e informações.

4.3 CRIPTOGRAFIA

A palavra criptografia tem sua origem na cultura grega e tem o significado de “escrita secreta”, ela se refere a transformar mensagens em códigos, tornando-a em caracteres ilegíveis e que não possam ser decifrados. O conceito busca que apenas quem possua a chave de decriptação consiga transformar esses códigos ilegíveis em informações verdadeiras e uteis, fazendo com que essas informações torne-se inúteis ou ilegíveis a usuários sem a chave de acesso, de maneira que essas informações consigam ser transmitidas de um local para o outro sem a chance de serem modificadas e consigam chegar ao seu destino com total integridade (PEREIRA, 2013).

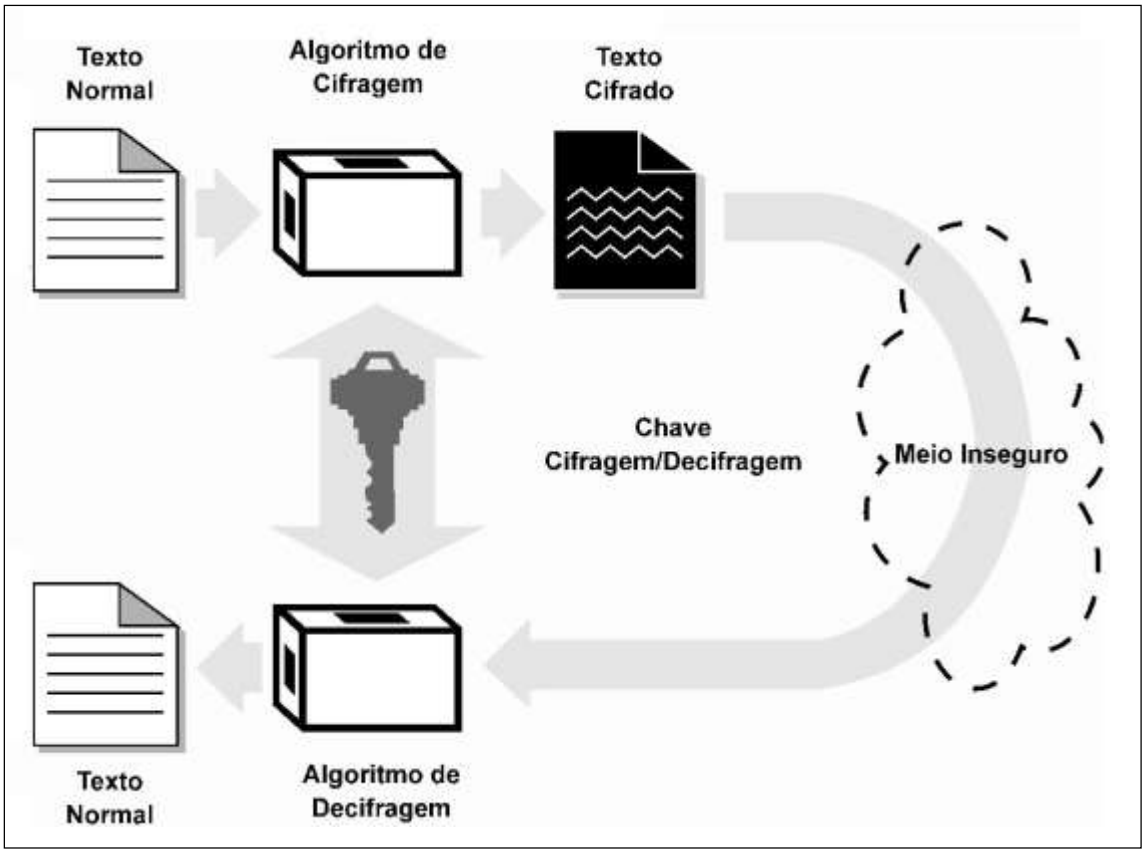
A criptografia é capaz de transformar toda a informação em um conteúdo totalmente incompreensível, porém não invisível, ou seja, será possível ver a mensagem mas não compreende-la, deixando os demais usuários cientes de que existe algo importante por traz de todos aqueles códigos. É possível falar sobre duas

formas de criptografia, a convencional também chamada de simétrica e a criptografia por chave pública também nomeada de assimétrica, tendo nas duas formas o envolvimento de chaves criptográficas.

4.3.1 Criptografia de chave simétrica

É a técnica mais antiga e conhecida, ela faz uso de uma única chave para criptografar e decriptação da informação, tornando o processo mais ágil (OLIVEIRA, 2007). A Figura 3 mostra como funciona o processo.

Figura 3 – Processo criptografia simétrica



Fonte: Trinta e Macedo (1998).

Como pode ser observado na simplicidade do algoritmo, essa técnica é significativamente mais rápida que a outra, tendo em mente que algoritmos mais simples tem uma maior facilidade de serem processados e também uma maior facilidade de implementação.

A principal desvantagem dessa técnica é ter apenas uma chave, seja para

criptografar e descriptografar a informação, sendo assim necessário o compartilhamento prévio dessa chave entre o usuário que irá realizar o envio da informação e o remetente, podendo ser interceptada por um usuário malicioso no meio do caminho, fazendo com que assim ele possa ter acesso a informações indevidas. A Figura 4 ilustra os tipos de algoritmos.

Figura 4 – Tipos algoritmos criptografia simétrica

(continua)

Algoritmo	Tamanho da Chave	Descrição
DES (Data Encryption Standard)	64 bits	Criado em 1977, sendo muito usado desde então. Foi adotado pelo National Bureau of Standards, atualmente conhecido como National Institute of Standards and Technology. Basicamente seu funcionamento consiste na criptografia de blocos de 64 bits de entrada com uma chave de 56 bits, gerando blocos de 64 bits como saída. Utiliza o Algoritmo de Feistel.
DES Triplo	112 bits	Alternativa do DES original, com variação de três diferentes chaves. O DES é aplicado três vezes, com a mesma chave ou com chaves diferentes.
IDEA (International Data Encryption Algorithm)	128 bits	Criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo de cifra de bloco que tem uma estrutura semelhante ao DES. Sua implementação em software é mais fácil do que a implementação deste último. Como uma cifra de bloco, também é simétrica. O algoritmo foi concebido como um substituto para o Data Encryption Standard (DES). O algoritmo é usado tanto para a cifragem quanto para a decifração.

(conclusão)

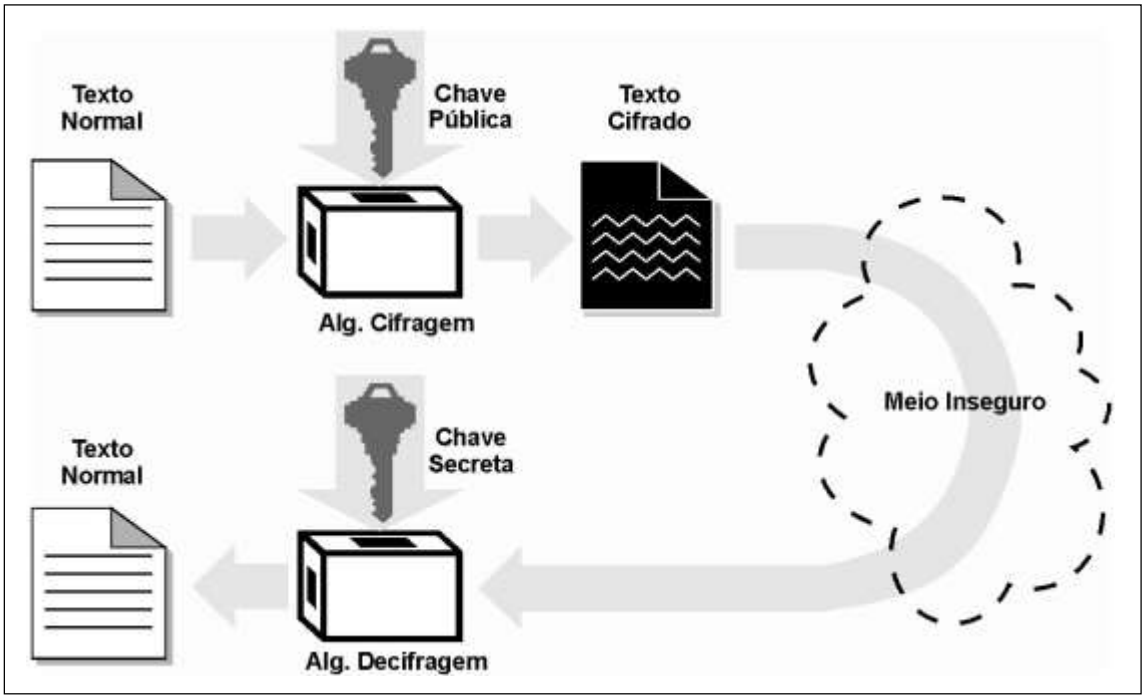
RC (Rivest Ciphers) RC2, RC4 e RC5	Tamanho variável	Todas as suas versões são algoritmos simétricos. O RC2 caracteriza-se por blocos de entrada de 64 bits, contudo podem ser usadas chaves com vários tamanhos. Já o RC4 não é uma técnica de blocos, mas sim de fluxo de entrada de bytes e saída de bytes cifrados ou decifrados conforme o caso. Esta é uma técnica atualmente muito usada, por um lado porque funciona em fluxo continuo e por outro lado porque é bastante rápida. Por fim o RC5 é uma técnica de cifragem em bloco, ele caracteriza-se por uma grande flexibilidade e possibilidade de parametrização.
BLOWFISH	32 a 448 bits	A criptografia é feita através de uma função com 16 interações. A cifragem do texto é feita em blocos de 64 ou 128 bits, nos quais os bits não são tratados separadamente, mas em grupos de 32 bits. A fim de aumentar sua eficiência, foi escolhido usar na confecção deste algoritmo funções simples para os microprocessadores, tais como XOR, adição e multiplicação modular.

Fonte: Oliveira (2007).

4.3.2 Criptografia de chave assimétrica

A criptografia assimétrica, também nomeada de chave pública é o método mais seguro de criptografia. Ela utiliza um par de chaves, onde uma dessas chaves é usada para criptografar (chave pública) e a outra (chave privada) é utilizada na descriptografia do arquivo. A sua desvantagem em relação a técnica de criptografia simétrica é que ele é um algoritmo mais complexo, fazendo com que perca significativamente desemprenho em relação a agilidade (OLIVEIRA, 2007). A Figura 5 demonstra este contexto.

Figura 5 – Processo criptografia assimétrica



Fonte: Trinta e Macedo (1998).

A vantagem dessa técnica é que qualquer usuário é capaz de distribuir essa informação, usando a chave pública de seu receptor. Graças a chave pública ser amplamente disponível, não há necessidade do envio de chaves, como feito na técnica simétrica. A informação tem garantia de estar segura e intacta desde que a chave privada esteja em posse apenas de seu respectivo receptor. A Figura 6 ilustra os tipos de algoritmos para este contexto.

Figura 6 – Tipos de algoritmo criptografia assimétrica

(continua)

ALGORITMO	DESCRIÇÃO
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. No Brasil, o RSA é utilizado pela ICP-Brasil, no seu sistema de emissão de certificados digitais, e a partir do dia 1º de janeiro de 2012, as chavesutilizadas pelas autoridades certificadoras do país, passam a serem emitidas 5 com o comprimento de 4.096bits, em vez dos 2.048 bits atuais.

(conclusão)

ElGamal	O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste Criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie-Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública, o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Fonte: Oliveira (2012).

A técnica de criptografia é muito eficiente para transferir informações entre um emissor e um receptor sem intervenções de usuários não permitido. Porém mesmo sendo uma técnica muito segura pode chamar a atenção das pessoas, sendo que é visível e muito claro que há algo de importante escondido por traz dos códigos. Também existem países em que o uso da criptografia é um proibido por lei. Tornando assim necessário o desenvolvimento de novas técnicas para transmitir a informação, de modo que só o emissor e o receptor sejam capazes de realmente entender a mensagem. Suprindo essa lacuna, apesar de pouco divulgada e muito menos utilizada, encontra-se a esteganografia que é uma técnica muito eficiente, que busca camuflar uma respectiva mensagem, informação, dentro de uma imagem, áudio ou até mesmo um vídeo, passando desapercebido por muitos e sendo muito mais difícil de ser detectada (PISA, 2013).

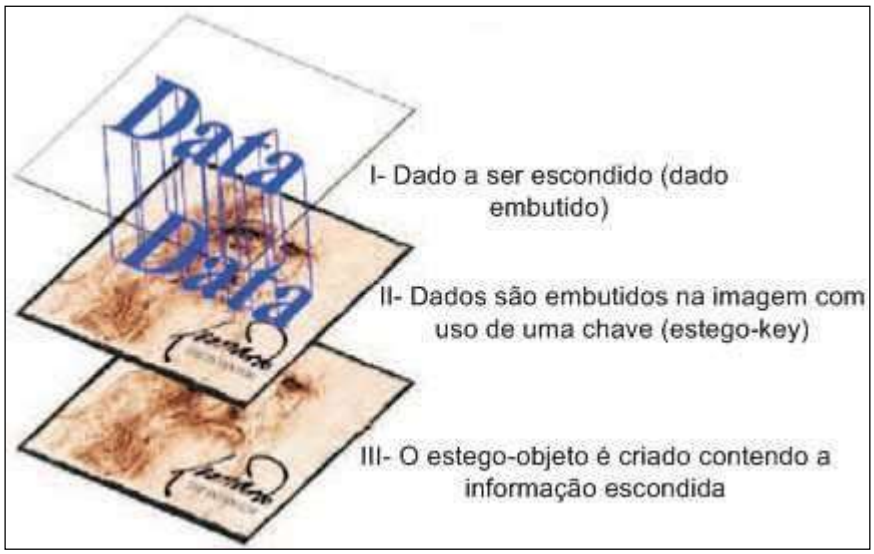
4.4 ESTEGANOGRAFIA

A palavra esteganografia vem de *Stegano* que significa esconder, e a palavra grafia escrita ou desenho.

A esteganografia (Figura 7) é a técnica de ocultar mensagens ou informações com o objetivo de se comunicar em segredo, diferenciando-se da criptografia, que também possibilita a privacidade entre o emissor e o receptor da mensagem, porém é muito mais visível do que a esteganografia, atraindo assim olhares maliciosos que podem tentar achar modos de quebrar o código. A esteganografia já é muito mais discreta e possibilita total segredo, já que sua presença é muito mais difícil de ser notada.

Uma de suas técnicas usadas é a alteração do seu bit menos significativo dentro de um pixel de uma imagem, conhecida como LSB, correspondendo a um bit de mensagem que será ocultada (CHIRIGATI; KIKUCHI; GOMES, 2006).

Figura 7- Processo de esteganografia



Fonte: Brazil e Albuquerque (2013).

O dado embutido ou *embedded data* é a informação que será inserida em algum arquivo, de maneira que possa ser transferida sigilosamente. A mensagem de cobertura ou *cover-message* é o arquivo que servirá de esconderijo, esse arquivo pode ser de áudio, uma imagem ou até mesmo um texto. *Stego-key* é a chave que pode ser usada para inserir os dados na mensagem de cobertura, e por fim, *Stego-object* é o resultado de uma mensagem de cobertura já possuindo a mensagem que será transmitida secretamente.

4.4.1 História da esteganografia

A esteganografia é uma técnica muito mais antiga, que já era usada a milhares de anos, na época da Grécia antiga os gregos já utilizavam pedaços de madeira cobertos com cera, onde a mensagem era escrita sobre a cera e quando já não fosse mais necessário o seu uso, a cera era derretida e a mensagem que havia ali era totalmente perdida. Alguns também escreviam a mensagem na madeira e a encobriam com cera, para que outras pessoas não pudessem ver o que havia ali escrito.

Uma técnica também utilizada por volta de 440 a.c., criada pelo general Histiaeus consistia em raspar a cabeça de um escravo de confiança, tatuar uma mensagem em seu couro cabeludo e quando o cabelo já estivesse crescido, de forma que não fosse possível visualizar a mensagem, ele era enviado ao destinatário da

mensagem e a mensagem era entregue com total sigilo (PETRI,2004).

Na Grécia antiga existia a técnica Astrogal, criada por Enéas, consistia em uma madeira com vários furos, onde cada furo representava uma letra do alfabeto, por esses furos eram passado um barbante e para ser decodificada o destinatário teriaque acompanhar as ligações feitas pelos furos (CHIRIGATI; KIKUCHI; GOMES, 2006).

O termo “esteganografia em si, só surgiu no século XV, quando o monge Johannes Trithemius publicou uma série de livros abordando sobre o tema, ele detalhava várias técnicas de como transmitir uma mensagem de um modo a qual não se fosse detectado, porém acabou sendo muito criticado, pois o seu livro falava muito de magias e espíritos (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Durante a Segunda Guerra Mundial, foi criada um tipo de tinta invisível, que para que se tornasse visível, o papel onde se encontrava a respectiva mensagem tinha que ser aquecido. Também foi criada a técnica de microponto, onde fotografias eram reduzidas a um ponto muito pequeno para serem enviadas (PETRI, 2004).

Técnicas mais modernas de esteganografia hoje em dia envolvem, cifradores nulos, onde apenas uma letra de cada palavra é usada e resto é descartado, porém o para o remetente e o destinatário da mensagem tem que entender a mensagem da mesma forma, um exemplo é utilizar apenas e a primeira letra de cada palavra descartando todo o resto. Porém essa técnica é bem trabalhosa, porque apesar das demais letras serem descartadas, a escrita no geral ainda deve fazer algum sentido, tendo em vista que pode ser interceptada no meio do caminho. Outro recurso muito usado é a Marca D’Água, muito utilizado por artistas e músicos para se protegerem da pirataria (JULIO; BRAZIL; ALBUQUERQUE, 2007).

4.4.2 Utilização

Apesar de pouco divulgada, a esteganografia é uma técnica que vem se disseminando com o tempo, porém sua utilização nem sempre é feita para o bem.

A esteganografia na maioria dos casos é utilizada para comunicação de forma sigilosa, de maneira que a impedir que a informação ocultada em seu interior seja acessada por terceiros não autorizados, sendo infelizmente usada para o planejamento de crimes, de forma que mesmo que os elementos sejam deflagrados, não seja possível identificar nada de errado na mensagem ou na imagem (PEREIRA,

2013).

Técnicas de esteganografia também são usadas para realizar uma Marca d'água digital, escondendo a mensagem nos bits de uma mídia digital (como imagens, vídeos e áudios), que contém informações usadas para identificar seu autor ou proprietário intelectual (PUSAN, 2009). Várias das técnicas consistem em inserir essa mensagem nos bits da mídia de forma que um rastreador web consiga identificar cópias não autorizadas (JEFFREY, 2002).

A marca d'água é de grande interesse comercial, sendo usada por autores e compositores, sendo escondidas em seus produtos, com a finalidade de que haja uma certa garantia de comprovação de qualidade, além da proteção de seus direitos autorais.

4.4.3 Requisitos para sistemas esteganográficos

Para Júlio, Brazil e Albuquerque (2007), para um software de esteganografia ser considerado de qualidade deve atender os seguintes respectivos:

a) Segurança: A ferramenta não deve levantar suspeitas de usuários durante a transferência dos arquivos, mantendo o conteúdo oculto imperceptível e mantendo também sua total integridade;
b) Carga útil: é necessário poder grande capacidade de inclusão, sendo possível inserir toda a informação;
c) Robustez: é a capacidade de resistência a compressão de uma imagem, já que a maioria das imagens são comprimidas antes de poderem ser postadas e divulgadas online.

4.4.4 Métodos de esteganografia

A esteganografia como visto anteriormente, não consiste apenas no mundo digital, técnicas como tatuar o couro cabeludo de um escravo, tintas que reagem ao calor e muitas outras, também são consideradas modos de ocultar uma mensagem.

4.4.4.1 Esteganografia em textos

A técnica de esteganografia em textos consiste em esconder uma mensagem real dentro de um texto. Para que essa mensagem consiga chegar ao seu destino intacta e de forma sigilosa sem que ninguém perceba, faz-se necessário que o texto como um todo tenha algum sentido.

Chamada cifradores nulos, essa técnica consiste em usar apenas algumas letras do todo, ou seja, letras e até palavras são descartadas e consideradas nulas (JULIO; BRAZIL; ALBUQUERQUE, 2013).

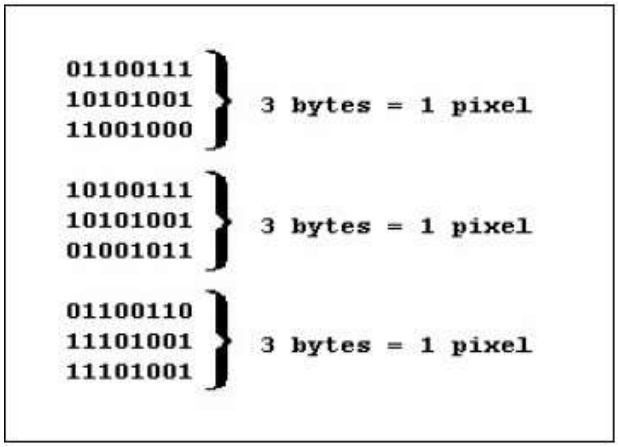
Porém faz-se necessário que ambas as partes conheçam o protocolo usado na confecção dessa mensagem, pois é necessário saber identificar as letras certas e pode ser necessário até a inclusão de letras para que a mensagem final realmente tenha algum sentido (PEREIRA, 2013).

4.4.4.2 Esteganografia em Imagens

A técnica LSB consiste na troca dos bits menos significativos dos pixels que compõe a imagem por stego-dados. Em um esquema complexo, locais de inclusão são adaptativamente selecionados. Pequenas distorções podem ocorrer e são até aceitas, desde que não chamem grande atenção das pessoas e comprometam o sigilo da mensagem (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Utilizando essa mesma técnica, é possível em uma imagem de 24 bits implementar até 3 bits por pixel. A Figura 8 exemplifica os pixels de uma imagem.

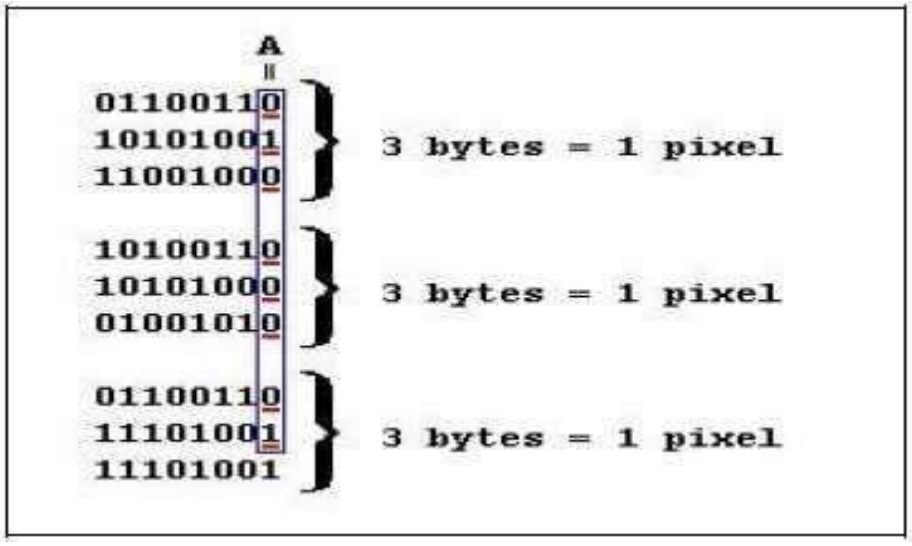
Figura 8 – Pixels de uma imagem



Fonte: Pereira (2013).

A Figura 9 exemplifica a inserção da letra “A” dentro da imagem, que representada em binaria possui o seguinte valor: 0 1 0 0 0 0 0 1, utilizando a técnica LSB.

Figura 9 – Inserção da letra “A” em uma imagem



Fonte: Pereira (2013).

Como pode ser observado na Figura 9 recebem destaque os pixels que foram modificados. A imagem representada sofreu uma pequena alteração de cor, porém imperceptível a olho humano.

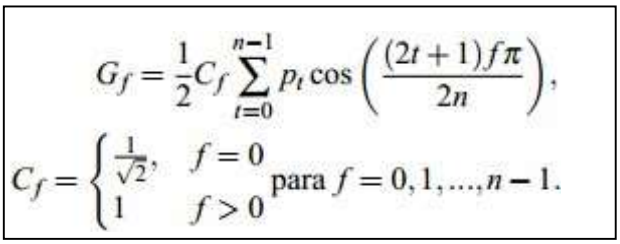
A técnica de filtragem e mascaramento é mais robusta que a LSB, ou seja, as estego-imagens criadas são mais imunes a compressão e ao recorte, que geralmente sites fazem para se tornar mais fácil sua divulgação. Ela funciona no sentido oposto da técnica LSB, alterando apenas os bits mais significativos da imagem, gerando uma desvantagem em relação a outra técnica, já que as imagens necessitam estar em tons cinzas, pois alterando os bits mais significativos de um pixel, gera-se também maior quantidade de cores e artefatos modificados, concluindo-se assim que essa técnica não é a melhor opção para aqueles que desejam trabalhar com imagens coloridas, já que nelas suas alterações se tornam mais evidentes e consequentemente mais fáceis de serem detectadas (JULIO; BRAZIL; ALBUQUERQUE, 2013).

Existem também as técnicas de algoritmos e transformações, elas são capazes de tirar proveito do problema da técnica LSB, que é a compressão. Pode-se citar a transformada de Fourier discreta, transformada de cosseno discreta e transformada Z (PEREIRA, 2013).

Baseando-se no funcionamento dessas técnicas, é correto afirmar que seu funcionamento consiste na transformação de blocos de 8x8 de pixels nas imagens, sendo que em cada bloco coeficientes menos importantes e redundantes são selecionados, para serem posteriormente usados na inserção do dado ou informação que se deseja esconder, por fim cada um desses coeficientes e substituído por valor pré-determinado para bits de 0 ou 1 (JULIO; ALBUQUERQUE; BRAZIL, 2007).

A transformada de cosseno discreta ou DCT, consiste na utilização de uma fórmula matemática que é muito utilizada no processamento e compressão de imagens e dados digitais. A Figura 10 representa a fórmula.

Figura 10 – Fórmula de compressão

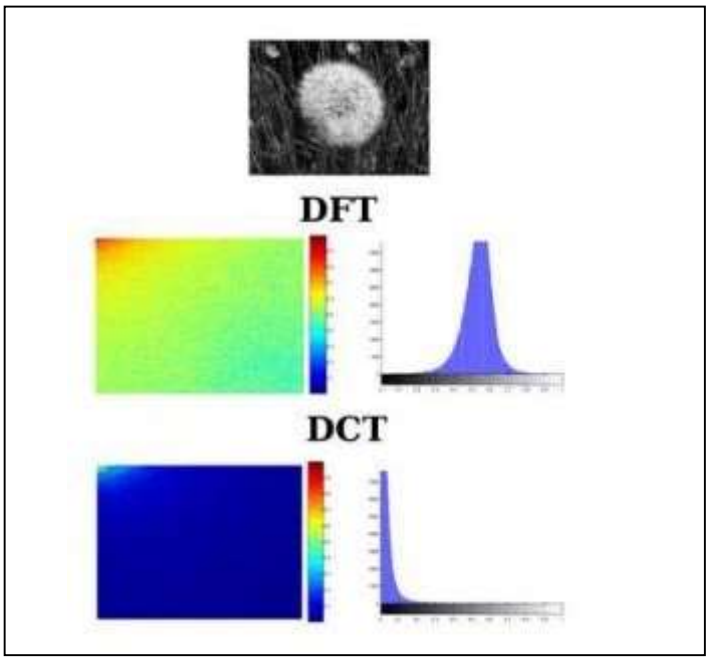


Fonte: Júlio, Brazil e Albuquerque (2013).

Segundo os autores citados anteriormente, a matriz da transformada é composta por vetores ortonormais, sendo então uma matriz rotacional. Quando acontece a compressão dos dados, a transformada é muito utilizada, por ser capaz de transferir a maior parte das informações para os primeiros elementos do vetor, otimizando assim o armazenamento e facilitando a quantização dos vetores.

A Figura 11 mostra um comparativo entre a transformada Fourier discreta e a DCT. É valido observar que a maioria dos coeficientes que são mais significativos, estão no canto encontram-se no canto direito superior, possibilitando assim uma maior compressão.

Figura 11 - Comparativo DCT e DFT

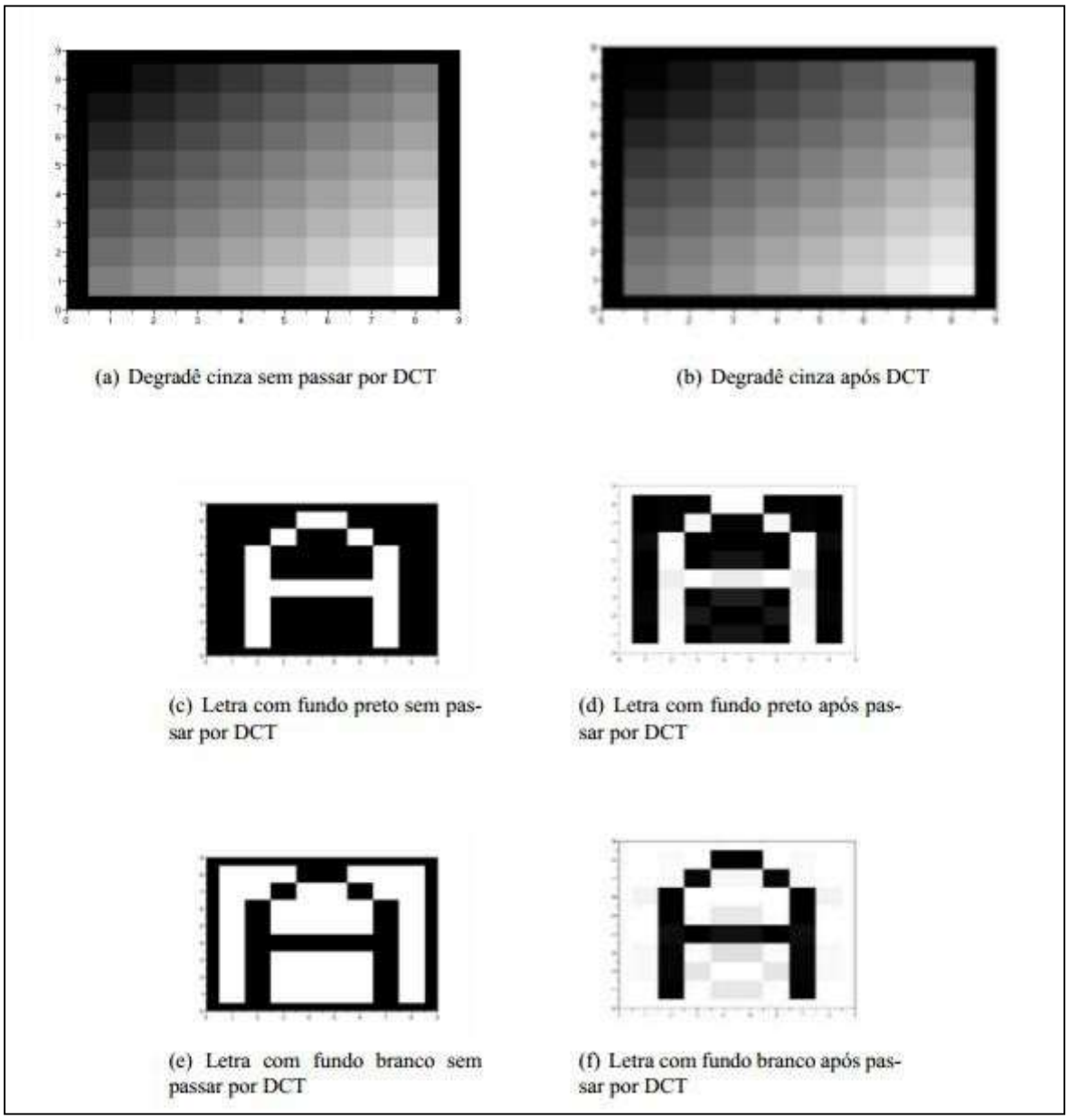


Fonte: Júlio, Brazil e Albuquerque (2013).

No padrão JPEG, coeficientes mais significativos de cada bloco 8x8 são selecionados e separados dos demais, com o objetivo de se ter um maior valor de compressão, além de serem comprimidos usando RLE e Codificação Huffman. Também se vê dentro do padrão uma compressão por meio de uma variante de codificação aritméticas, conhecida como QM (PEREIRA, 2013).

A Figura 12 apresenta exemplos de figuras de tamanho 8x8 pixels transformadas usando a técnica DCT e quantizadas utilizando a tabela JPEG, posteriormente é feito o reverso para que possam ser exibidas e analisadas sem o efeito da compressão. É possível perceber nas imagens nas transições de cores de tons mais suaves, uma melhor recomposição da imagem é proporcionada (JULIO; BRAZIL; ALBUQUERQUE, 2013; PEREIRA, 2013).

Figura 12 – DCT utilizando tabela JPEG



Fonte: Júlio, Brazil e Albuquerque (2013).

Existe também a técnica de espalhamento de espectro, onde dados são inseridos ao longo da imagem de cobertura e utiliza-se uma *stego-key* para selecionar os canais de frequência (PEREIRA, 2013).

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

4.4.4.3 Esteganografia em áudio

A técnica de esteganografia em áudio é um tanto mais complexa que as outras, visto que o ouvido humano consegue detectar um grande espaço de frequências, o que torna perceptível até o menor ruído e perturbação no arquivo de áudio (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Nesse segmento uma técnica muito usada é utilização do eco para ocultação de informações, variando três parâmetros do eco: amplitude, deterioração e a taxa de atraso. Também se coloca esses parâmetros fora do limite sensorial humano, para que não possa ser possível distinguir o mesmo do som original, sendo considerado como uma ressonância (PETRI, 2004).

4.4.4.4 Esteganografia em vídeo

Um vídeo consiste em um conjunto de imagens, que quando exibidas a uma taxa de 24 ou 30 imagens por segundo dão alusão a movimento.

Para inserção e ocultação de imagens em vídeo torna-se necessário manipular as imagens ali contidas. Isso se torna possível, pois a visão humana não tem a capacidade de ressaltar pequenas alterações nas imagens, que são realizadasatravés da modificação dos bits menos significativos dessas imagens (técnica LSB) (CARVALHO, 2008).

4.5 ESTEGANÁLISE

A Esteganálise é o estudo e pesquisas com intuito de descobrir informações que foram ocultadas de alguma forma, tanto em textos, imagens, vídeos e áudios (PETRI, 2004).

A Esteganografia como qualquer outro sistema possui falhas, tornando-se possível por um usuário que se dedique a avaliar detalhadamente algum objeto em busca de informações ocultas, pois como já dito anteriormente, ao se utilizar a técnica da esteganografia, parâmetros acabam sendo degradados, ocorrendo modificações e sendo assim possível definir parâmetros para que se encontre a informação ali ocultada (PETRI, 2004).

Segundo autor citado anteriormente, considera-se três métodos de ataques:

a) ataques aurais: consistem na retirada de partes importantes da imagem, na medida que o olho humano seja capaz de buscar respectivas falhas e alterações.
b) ataques estruturais: a estrutura de um arquivo é alterada na inserção de dados. Com a ajuda de um software é possível analisar a estrutura dessa imagem e analisar se ela foi alterada na inserção dos dados. Temos como exemplo dados inseridos em uma imagem indexada, baseando-se na palheta de cores, a imagem de cobertura acaba tendo suas características modificadas, tornando grande a chance de detecção.
c) ataque estatístico: analisando os bits menos significativos, é possível descobrir uma mensagem ali contida, pela sua redundância ou pela distorção dos dados ali contidos.

Petri (2004) ainda afirma que não há métodos de ataque à esteganografia que sejam universais ou mesmo que correspondam a todos os softwares com essa finalidade. Em um ataque passivo, o intuito é apenas detectar a presença ou ausência de informação no arquivo, já no ativo, detectar e se possível manipular essas informações.

Quando há suspeita de que existe informações ocultas em um arquivo, é necessário a realização de testes e criação de hipóteses para retirada da informação. Quando sabe o software que foi utilizado no processo da ocultação da informação, torna-se mais fácil a análise do processo (CHIRIGATI; KIKUCHI; GOMES, 2006 citado por PEREIRA, 2013).

O avanço da tecnologia trouxe grandes benefícios ao homem, porém não podemos esquecer dos perigos que acompanham esse avanço, já que muitos criminosos agem em meio a rede, bons exemplos desses de crimes realizados pele internet são: pedofilia, roubos, fraudes e pornografia. E para combatê-los foram necessários o treinamento e a formação de profissionais especializados, conhecidos como peritos forenses computacionais.

4.6 PERÍCIA FORENSE COMPUTACIONAL

A perícia forense computacional é uma divisão que foi criada com o objetivo de combater e investigar crimes cometidos digitalmente. Ela utiliza técnicas e ferramentas especificas para coletar, preservar e analisar informações suspeitas em computadores realizados na realização de algum crime, e a partir dessas informações auxiliar na investigação e até mesmo na solução dos casos.

Devido ao constante avanço da tecnologia, essa deve ser uma área a qual se deve buscar aperfeiçoamentos e ser estudada constantemente, já que com avanço também surgem novos crimes cibernéticos, cada vez mais complexos e difíceis de serem resolvidos (GONÇALVES *et al*., 2012).

Uma das formas do perito analisar as provas do crime, é trabalhando com a máquina ligada após a execução do mesmo, porém, e essencial que ele antes faça uma imagem volátil do estado da máquina original, para que não possa existir alegações de adulteração e incriminação na máquina (TOLENTINO; SILVA; MELLO, 2011).

Para se ter uma investigação totalmente eficiente é preciso seguir uma série de etapas. Primeiro é feita a coleta de dados, onde é realizada a captura do equipamento e das informações de maneira que a integridade delas não sejam afetadas, logo após é feito o exame dos dados, onde é realizada a captação das informações mais relevantes à investigação e separada das demais, dessa forma é possível definir um processo mais especifico para que seja realizada a análise das informações, onde o intuito é encontrar dados importantes que auxiliem na resolução do caso. Na última etapa, a interpretação dos resultados consiste em apresentar um laudo técnico contendo todas as informações verídicas dos dados que foram analisados em laboratório (PEREIRA, 2013).

.

5 METODOLOGIA

O seguinte trabalho foi realizado em três etapas, a primeira que consistiu na busca de aspectos teóricos e históricos relacionados ao tema, buscando enriquecer o conhecimento e domínio sobre ele. Na segunda etapa foram pesquisadas ferramentas gratuitas, bem como, versões gratuitas de softwares pagos de esteganografia para serem utilizados, e a terceira consistiu na etapa prática – instalação das ferramentas, aplicação das técnicas de esteganografia e análise dos resultados.

Considerando o contexto desta pesquisa, não foi necessária a submissão do projeto de pesquisa ao Comitê de Ética em Pesquisa (CEP) ou à Comissão de Ética no Uso de Animais (CEUA), devido à pesquisa não envolver seres humanos e nem animais, pois só utilizou métodos de computação envolvendo manipulação de dados, hardwares e softwares

Como dito anteriormente, nessa primeira etapa foi elaborado um levantamento teórico que consistiu em definições sobre esteganografia, histórico, as principais técnicas de esteganografia utilizadas dentro da perícia computacional etc. Também foram abordados temas como segurança da informação, segurança digital e perícia computacional, que são temas essenciais para a compreensão deste projeto de pesquisa.

Como segunda etapa foi realizada uma busca por ferramentas esteganográficas. Foi definido o número de três ferramentas esteganográficas - quantidade definida de forma aleatória pelo pesquisador. O objetivo é buscar/selecionar tanto ferramentas para a plataforma Windows, quanto para o Linux, que são os sistemas operacionais mais comuns que existem para computadores e que o mercado oferece, além de, se tratar de duas plataformas distintas, a fim de descobrir em qual delas o processo realizado foi mais eficiente, e analisar mais de uma técnica e mais de um tamanho de imagem. Vale a pena ressaltar que usando-se dois sistemas operacionais diferentes para a realização das análises, podeser que resulte em resultados diferentes. As ferramentas selecionadas para essa pesquisa são gratuitas, bem como, versões gratuitas de softwares pagos.

As aplicações foram realizadas em um computador, de propriedade do pesquisador com a seguinte configuração: Windows 10 Pro de 64 bits, processador Intel® Core™ i3-3250 (3.50 GHz, cache de 3MB), memória RAM de 8 GB operando a

2.128MHz. A escolha do computador se deu pelo fato de pertencer ao pesquisador, além de ser suficiente para suprir todas as necessidades que surgirão no decorrer do projeto.

Na terceira etapa foram instaladas as ferramentas selecionadas. Após instaladas, técnicas de esteganografia foram aplicadas - uma mensagem criada aleatoriamente, como por exemplo: “Este é um projeto de pesquisa de Iniciação Científica do curso de Ciência da Computação”, foi inserida na imagem em formato JPEG[1] de dimensões 256, 512 e 1024 pixels, para que fosse possível comparar os resultados encontrados e apresentá-los como qual a melhor técnica e ferramenta a ser utilizada, não só por sua eficiência, mas também pela integridade do arquivo após sua modificação, onde a melhor foi considerada aquela que atenda todos ou quase todos os requisitos.

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

Após finalizar as inserções, as imagens originais e modificadas foram dispostas para que fosse possível compará-las e assim, verificar se no arquivo final houve alguma alteração perceptível a olho nu. Por fim, todos os dados foram tabulados em planilhas eletrônicas do Microsoft Excel e quadros comparativos foram confeccionados, bem como, gráficos apresentando o resultado das inserções, apontando qual ferramenta foi capaz de gerar uma imagem segura e íntegra, com o mínimo de alterações possíveis. Como possibilidades de comparação podemos citar:

a) Comparação entre imagens de resolução 256 x 256.
b) Comparação entre imagens de resolução 512 x 512.

[1] Com tantos formatos de imagem, às vezes é difícil decidir qual é o melhor para cada aplicação. Cada uma das extensões possui características próprias, sendo indicadas para situações diferentes. O JPEG é mais utilizado naweb por seu pequeno tamanho, mas o PNG é mais versátil e recomendado para uma qualidade um pouco maior.Procurou-se nesta pesquisa trabalhar com os formatos mais comuns utilizados.

6 RESULTADOS

A seguir são apresentados os resultados obtidos neste projeto de pesquisa.

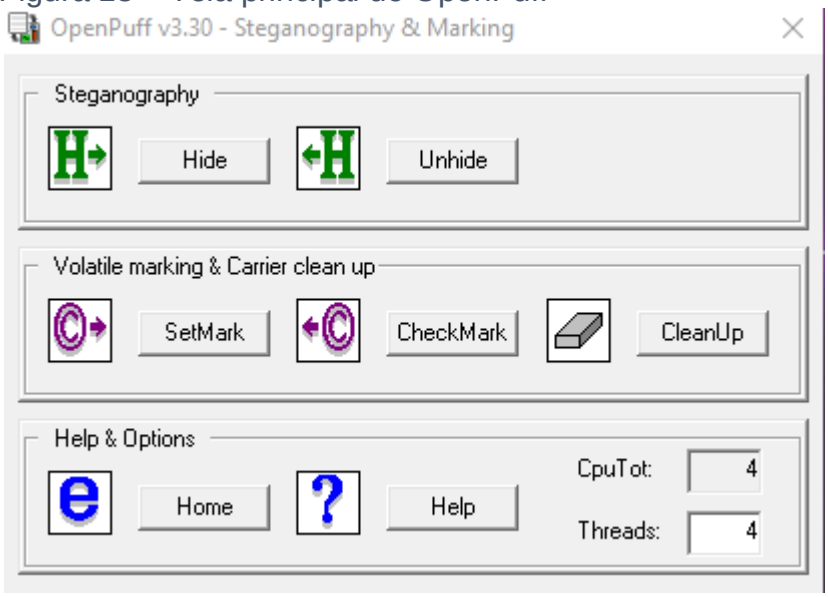
6.1 ANÁLISE: SITES E PESQUISAS

Após o início da Iniciação Científica, houve o começo pela busca bibliográfica através de sites pela internet e pesquisas relacionadas sobre o assunto. Constatou-se que os conteúdos sobre esteganografia ainda são vastos, as pessoas ainda não conhecem esse método de criptografia devido ao fato dele ser mais específico e relacionado a imagens e áudio.

6.2 BUSCA POR PROGRAMAS

Depois da busca bibliográfica foi feita a busca por programas que realizam o processo de esteganografia. Diversas ferramentas *open source* foram encontradas, e entre elas, as selecionadas: OpenPuff (Figura 13), SilentEye (Figura 14) e Steganography (Figura 15).

Figura 13 – Tela principal do OpenPuff



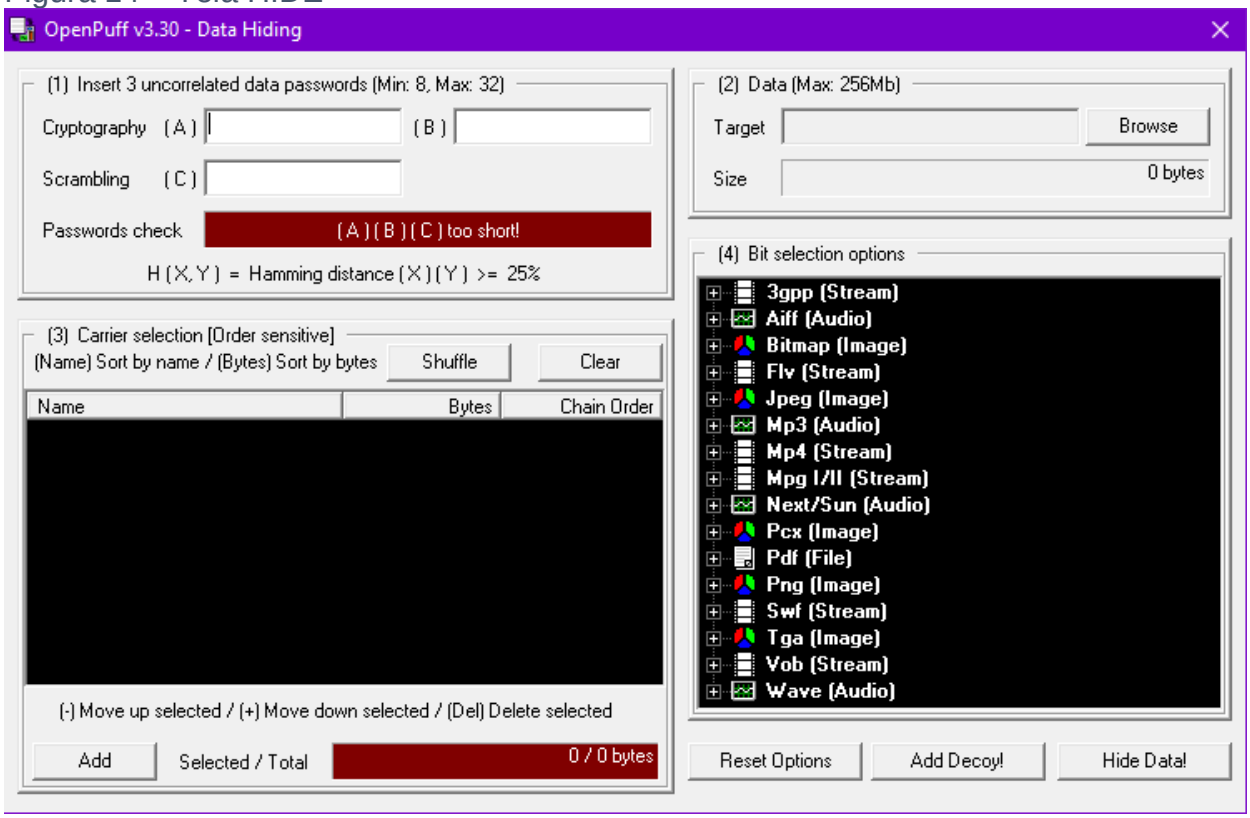
Fonte: Programa “OpenPuff”.

Ao executar o programa, conseguimos ver a janela ilustrada na Figura 13. O

primeiro menu é utilizado para realizar o processo de ocultar/desocultar mensagens de texto nas imagens. O segundo menu é usado para inserir uma marca, para que a imagem selecionada seja reconhecida por quem a fez. No terceiro menu, caso tenha algum problema, é possível visitar o site dos desenvolvedores.

Ao clicar na opção “HIDE” no programa a tela exibida na Figura 14 é apresentada. Ela pode parecer confusa, porém já no primeiro uso é possível entendê-la com facilidade. Há três passos que devem ser seguidos. O primeiro deles é colocar três senhas para deixar a imagem mais protegida. No próximo passo, deve-se selecionar a mensagem que deseja incluir, é importante ressaltar que a mensagem tem um limite de 256Mb. Por fim, inserir a imagem, clicando em “Add”. O tamanho total da imagem varia de acordo com a mensagem colocada. Após todos esses comandos serem concluídos, basta clicar em “Hide Data!” e pronto.

Figura 14 – Tela HIDE

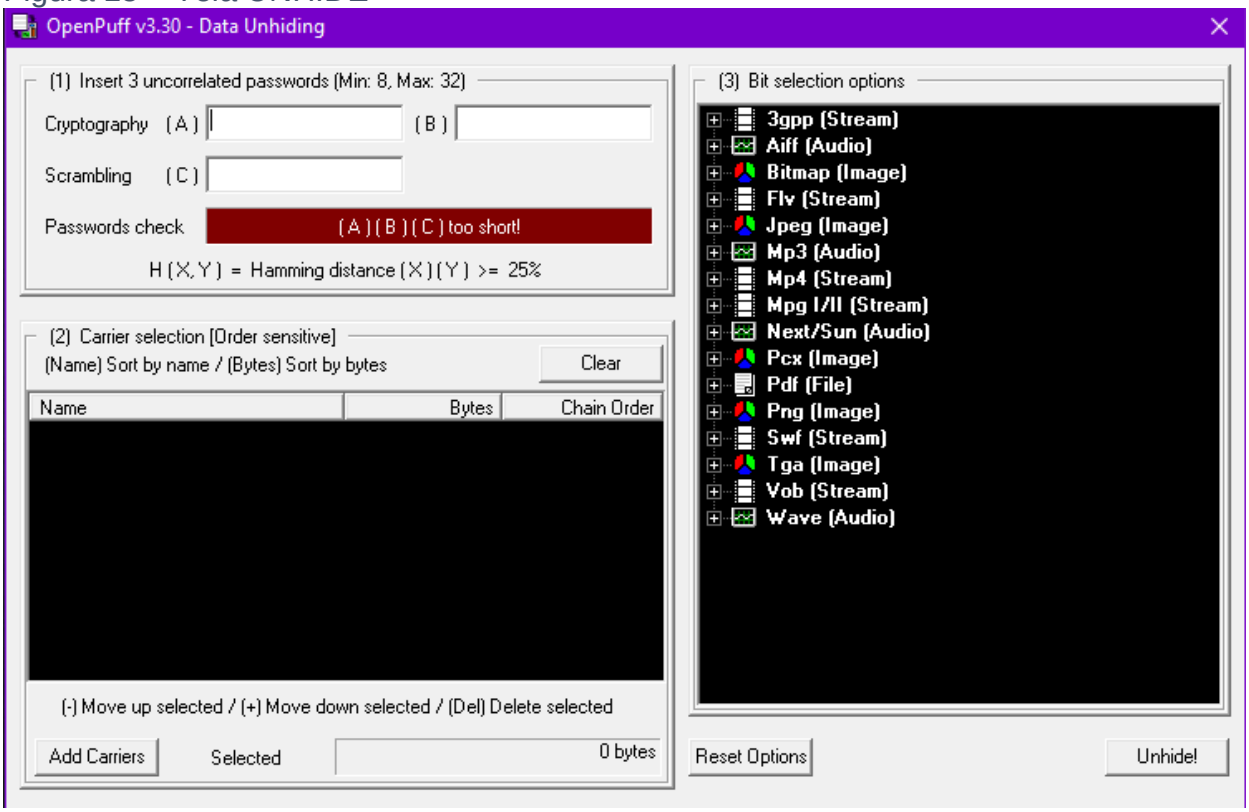


Fonte: Programa “OpenPuff”

Para retirar a mensagem de texto inserida na imagem apresentada na Figura 14 basta clicar na opção “UNHIDE”, clicando é possível ver a tela acima. A primeira coisa a se fazer é colocar as senhas da mesma imagem criadas anteriormente. Após isso, clicando em “Add Carriers”, seleciona-se a imagem que irá ser descriptografada.

Por fim, ao clicar em “Unhide!”, salve na pasta que desejar e aparecerá a imagem e a mensagem que estava escondida nela na pasta em que desejar. A Figura 15 ilustra este contexto.

Figura 15 – Tela UNHIDE



Fonte: Programa “OpenPuff”

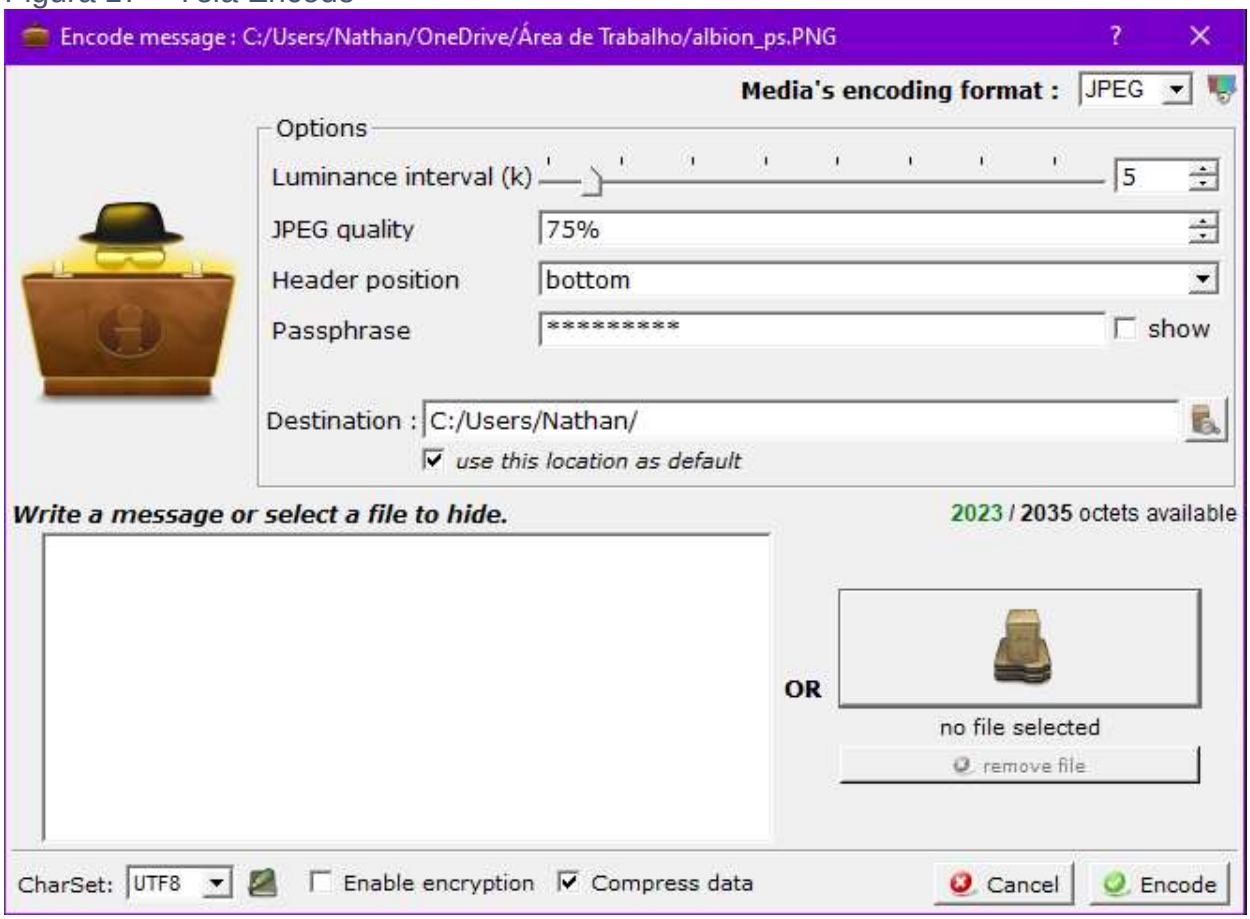
Ao executar a ferramenta SilentEye, o usuário encontra a tela retratada na Figura 16, ela é bem intuitiva, há a possibilidade de clicar ou apenas arrastar a imagem que deseja. Ao arrastar a imagem, as opções embaixo estarão disponíveis e para esconder uma mensagem, basta clicar em “Encode”.

Figura 16 – Tela principal SilentEye

Fonte: Programa “SilentEye”

Ao selecionar a opção “Encode”, aparece a tela ilustrada na Figura 17. Como já foi selecionada a imagem, basta apenas colocar a mensagem que deseja ou selecioná-la, após isso, basta clicar em “Encode”.

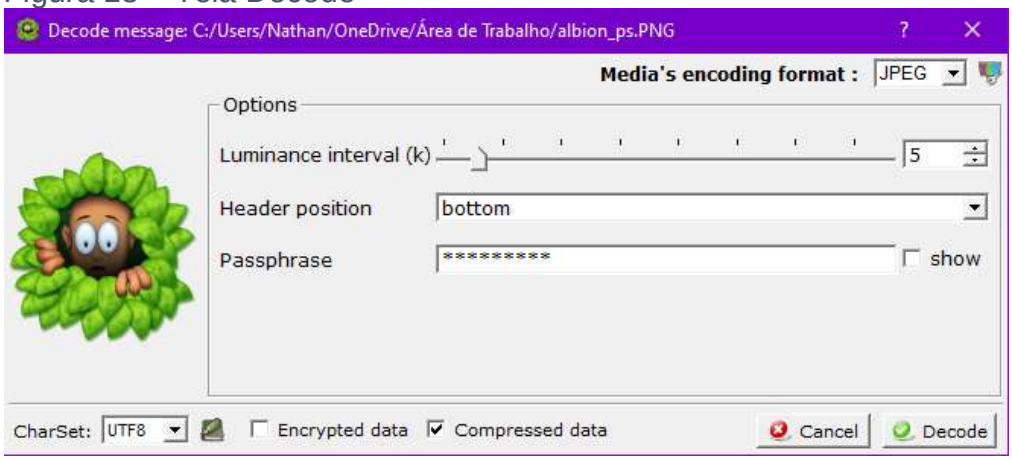
Figura 17 – Tela Encode



Fonte: Programa “SilentEye”

Caso queira descriptografar a imagem anterior, selecione a opção “Decode” (Figura 16). Após isso, será exibida a Figura 18, onde o usuário poderá inserir a imagem com a mensagem oculta.

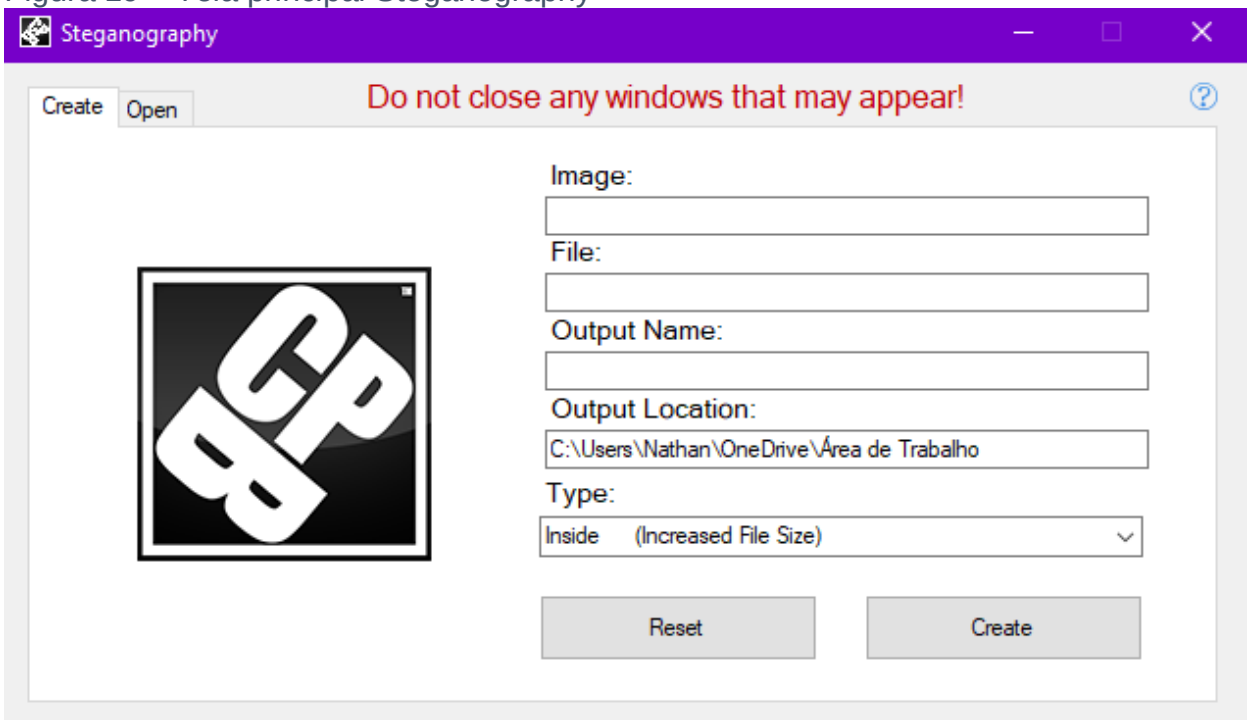
Figura 18 – Tela Decode



Fonte: Programa “SilentEye”

Ao executar o programa, o usuário se depara com a tela ilustrada na Figura 19. A primeira opção “Image” é onde se seleciona a imagem. Na próxima opção “File” se seleciona a mensagem que o usuário deseja esconder, vale lembrar que o programa aceita somente arquivos em zip ou rar nesse comando. Por fim, “Output Name” é usado para colocar um nome na imagem e após isso, clicando em “Create” a imagem é gerada.

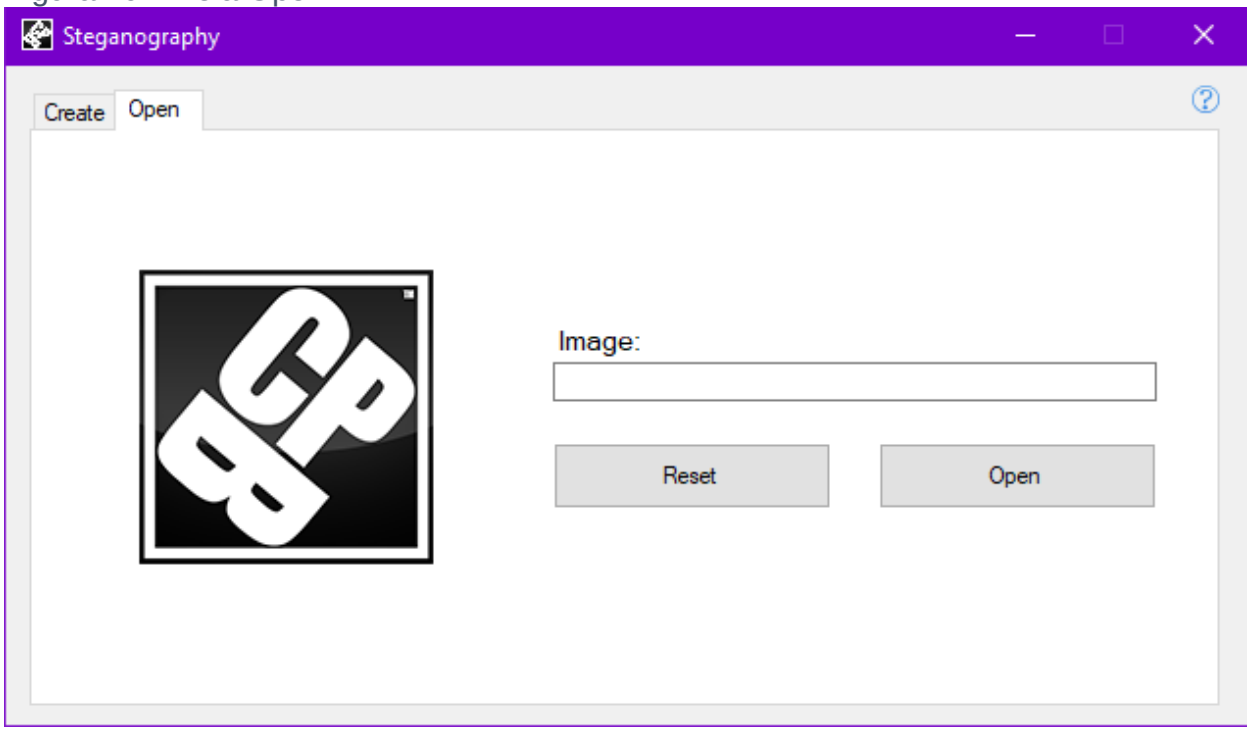
Figura 19 – Tela principal Steganography



Fonte: Programa “Steganography”

Para descriptografar a imagem, basta clicar em “Open” ao lado de “Create”, selecionar a imagem e clicar em “Open” ao lado de “Reset” e pronto, a imagem com o arquivo da mensagem aparecerá na pasta em que o usuário desejar. A Figura 20 ilustra este contexto.

Figura 20 – Tela Open



Fonte: Programa “Steganography”

6.3 Imagens pré-selecionadas

Foram selecionadas para efeito de comparação 2 (duas) imagens por resolução (256, 512, 1024), as quais são apresentadas a seguir.

Imagens 256x256	Imagens 512x512	Imagens 1024x1024
		
		

Fonte: Google (2021).

6.4 RESULTADOS FINAIS

As três ferramentas foram utilizadas com o intuito de aplicar técnicas de esteganografia de maneira que fosse possível analisar qual ferramenta trabalha de maneira mais eficiente, bem como o tamanho do arquivo após a modificação. Para obter uma precisão maior nos resultados, foram testados três arquivos de diferentes tamanhos e com a extensão de acordo com a suportada pela ferramenta.

A Figura 21 apresenta a comparação entre os arquivos originais e os finais criados após a inserção da mensagem, utilizando imagens de 256 pixels. Das três ferramentas utilizadas, uma delas gerou um arquivo com tamanho inferior ao original. Já na ferramenta SilentEye, não houve alteração no tamanho do arquivo.

Figura 21 - Comparação entre imagens de resolução 256 x 256.

FERRAMENTA	ORIGINAL	GERADA	%
Steganography	12,7	13	2,36
SilentEye	12,7	12,7	0,00
OpenPuff	12,7	11	15,45

Fonte: Elaborada pelo autor.

Já a Figura 22, contempla o tamanho dos arquivos antes e depois das inserções utilizando as ferramentas abordada, em imagens JPG de 512 pixels. Nestes testes, assim como no realizado com as imagens de 256 pixels, a ferramenta Steganography apresentou um arquivo menor ao final, entretanto, a ferramenta SilenteEye gerou um arquivo com um tamanho maior que a original.

Figura 22 – Comparação entre imagens de resolução 512 x 512.

FERRAMENTA	ORIGINAL	GERADA	%
Steganography	100	13	669,23
SilentEye	100	254	154,00
OpenPuff	100	101	1,00

Fonte: Elaborada pelo autor.

A Figura 23 apresenta a comparação entre os arquivos originais e finais através das ferramentas definidas, em imagens nos formatos JPG de 1024 pixels, e como pode ser observado, a ferramenta Steganography teve um resultado menor comparado ao original. Já na ferramenta SilentEye, o arquivo sofreu pouca alteração no tamanho, assim como na ferramenta Hide And Reveal, que por sua vez gerou um

arquivo num tamanho igual ao original.

Figura 23 - Comparação entre imagens de resolução 1024 x 1024.

FERRAMENTA	ORIGINAL	GERADA	%
Steganography	231	13	1676,92
SilentEye	231	123	87,80
OpenPuff	200	200	0,00

Fonte: Elaborada pelo autor.

Na Figura 24, os resultados foram separados pelo formato da imagem e pela ferramenta que foi utilizada, de maneira que fosse possível comparar a funcionalidade da mesma individualmente. De acordo com a ferramenta Steganography, esta que proporcionou os piores resultados, os níveis de tamanho de arquivo sofreram grandes mudanças nas resoluções 512 e 1024. De tal forma, pode-se considerar que o melhor resultado obtido foi com a imagem de 256 pixels, esta que teve a menor taxa de alteração no tamanho do arquivo.

Figura 24 – Ferramenta Steganography: Comparação entre resoluções diferentes em imagem do tipo JPG.

256 x 256			**512 x 512**			**1024 x 1024**		
ORIGINAL	GERADA	%	ORIGINAL	GERADA	%	ORIGINAL	GERADA	%
12,7	13	2,36	100	13	669,23	231	13	1676,92

Fonte: Elaborada pelo autor.

A Figura 25 apresenta os resultados gerados pela ferramenta SilentEye, houveram variações no tamanho dos arquivos finais. Por fim, nesta ferramenta, a inserção que apresentou melhor resultado foi novamente, utilizando a imagem de 256 pixels, sendo que esta não sofreu alteração de tamanho.

Figura 25 – Ferramenta SilentEye: Comparação entre resoluções diferentes em imagem do tipo JPG.

256 x 256			**512 x 512**			**1024 x 1024**		
ORIGINAL	GERADA	%	ORIGINAL	GERADA	%	ORIGINAL	GERADA	%
12,7	12,7	0,00	100	254	154,00	231	123	87,80

Fonte: Elaborada pelo autor.

Já a Figura 26, mostra os resultados gerados pela ferramenta OpenPuff. Ao final dos testes, os arquivos tiveram um aumento quase nulo de tamanho nas três resoluções, o melhor resultado apresentado por esta ferramenta, foi utilizando as imagens de 512 e 1024 pixels, já que ela obteve o menor índice de aumento no tamanho do arquivo.

Figura 26 - Ferramenta OpenPuff: Comparação entre resoluções diferentes em imagem do tipo JPG.

256 x 256			**512 x 512**			**1024 x 1024**		
ORIGINAL	GERADA	%	ORIGINAL	GERADA	%	ORIGINAL	GERADA	%
12	11	9,09	100	101	1,00	200	200	0,00

Fonte: Elaborada pelo autor.

Já na Figura 27, os resultados gerados foram dispostos independentes do tamanho da imagem, de forma que seja possível ver qual das ferramentas proporcionou o melhor resultado. A ferramenta OpenPuff foi a que apresentou os melhores resultados, por não gerar alterações consideráveis no tamanho dos arquivos.

Figura 27 - Comparação por ferramenta e resolução de imagem

FERRAMENTA	**256 x 256**			**512 x 512**			**1024 x 1024**		
	ORIGINAL	GERADA		ORIGINAL	GERADA		ORIGINAL	GERADA	
	Tamanho	Tamanho	%	Tamanho	Tamanho	%	Tamanho	Tamanho	%
Steganography	12,7	13	2,3622	100	13	669,23	231	13	1676,92
SilentEye	12,7	12,7	0,00	100	254	154,00	231	123	87,80
OpenPuff	12	11	9,09091	100	101	1,00	200	200	0,00

Fonte: Elaborado pelo autor.

7 CONSIDERAÇÕES FINAIS

As ferramentas escolhidas se destacam por serem gratuitas e por trabalharem com as três resoluções selecionadas, ampliando a possibilidade de diferenciar os resultados finais.

Nos testes realizados na ferramenta Steganography, das três imagens geradas ao final das inserções, os níveis de tamanho de arquivo sofreram grandes mudanças nas resoluções 512 e 1024. De tal forma, pode-se considerar que a ferramenta possui um melhor resultado quando trabalhado com imagens de resolução 256.

Já a ferramenta SilentEye, é uma ferramenta que possui uma interface mais amigável ao usuário, tornando seu uso mais fácil. Já os resultados finais gerados por esta ferramenta, não foram satisfatórios, pois os tamanhos dos arquivos sofreram um aumento significativo na resolução 512 e uma diminuição razoável na resolução 1024. Esta ferramenta não é considerada como uma boa opção de uso para as resoluções 512 e 1024, sendo recomendada para trabalhos de imagens 256 como a ferramenta anterior.

A ferramenta OpenPuff também possui uma interface amigável ao usuário. Nos testes realizados, os arquivos gerados ao final das inserções tiveram modificações razoáveis nos tamanhos dos arquivos finais, apenas uma pequena redução no tamanho da resolução 256, resultado quase nulo com a resolução 512 e nenhuma alteração no tamanho de 1024.

De acordo com os resultados gerados, pode-se perceber que a ferramenta Steganography é uma boa opção para imagens de resolução 256, sendo capaz de ser transmitido sem chamar a atenção. Já a ferramenta SilentEye novamente é indicada para imagens de resolução 256, seguindo os passos da ferramenta anterior. A OpenPuff apresentou bons resultados nas resoluções selecionas, onde teve pequenas alterações nos tamanhos das imagens sendo indicada para se ocultar uma informação em uma imagem.

Considerando todas as análises feitas anteriormente, a sugestão para trabalhos futuros é de estabelecer comparações entre imagens em formatos diferentes, tais como: “GIF”, “PNG”.

8 RISCOS E BENEFÍCIOS

A seguir são apresentados os riscos e benefícios desta pesquisa.

8.1 RISCOS

Este projeto não envolveu acesso direto a seres humanos, portanto não apresentou riscos.

8.2 BENEFÍCIOS

Os benefícios relacionados a este projeto envolvem aqueles decorrentes da aplicação de técnicas de esteganografia, a fim de contribuir com usuários que tenham interesse na área de segurança digital, com a intenção de adquirir novos conhecimentos.

9 ORÇAMENTO

EQUIPAMENTO / MATERIAL PERMANENTE			
qual sua utilização napesquisa	**DISPONÍVEL**		
	Quantidade	lor Unit. (R$)	lor Total(R$)
Intel® Core™ i3-3250 (3.50 GHz, cache de 3MB), memória RAM de 8 GB operando a 2.128MHz.	1	1.153,22	1.153,22
Software open source VirtualBox	1	-	-
Ferramentas de esteganografia (gratuitas)	3	-	-
		TOTAL (R$)	**1.153,22**

MATERIAL DE CONSUMO (Responsabilidade do pesquisador)			
qual sua utilização napesquisa	**DISPONÍVEL**		
	Quantidade	lor Unit. (R$)	Valor Total (R$)
Impressões	200	1,10	220,00
Papel Sulfite A4 Office 210 x 297mm 75g/m² - Pacote 500 Folhas Chamex Branco	3	30,48	91,44
		TOTAL (R$)	**311,44**

ORÇAMENTO DO PROJETO		
DESCRIÇÃO	**DISPONÍVEL Custo do Item (R$)**	**NÃO DISPONÍVEL Custo do Item (R$)**
Equipamento / Material Permanente	3.899,99	
Material de Consumo	311,44	
TOTAL (R$)	**1.464,66**	

CARTA DE DISPENSA

CARTA DE DISPENSA DE APRESENTAÇÃO AO CEP OU CEUA

À
COORDENADORIA DO PROGRAMA DE INICIAÇÃO CIENTÍFICA DA USC

Informo que não é necessária a submissão do projeto de pesquisa intitulado **ANÁLISE E IMPLEMENTAÇÃO DE TÉCNICAS DE ESTEGANOGRAFIA EM IMAGENS: SEGURANÇA E PRIVACIDADE NA INTERNET**, ao Comitê de Ética em Pesquisa (CEP) ou à Comissão de Ética no Uso de Animais (CEUA) devido à pesquisa não envolver seres humanos e nem animais, pois só utilizará métodos de computação envolvendo manipulação de dados, hardwares e softwares.
Atenciosamente

_____

Bauru, 25 de março de 2020.

REFERÊNCIAS

BOTURA, M. J. M. **Esteganografia um comparativo entre as ferramentas Stegdetect, Hide and reveal e Silenteye,** 2014. TCC, Centro universitário Sagrado coração, Bauru, 2014.

CARVALHO, D. F. **Esteganografia em vídeos comprimidos MPEG-4**, 2008. 69 f. Tese (Mestre em Ciência de Computação e Matemática Computacional) - USP, São Carlos, São Paulo, 2008. Disponível em: http://www.teses.usp.br/teses/disponiveis/55/55134/tde-08062009-143448/pt-br.php. Acesso em: 21 mar. 2020.

CARVALHO, G. M. Assinatura Digital. **Assinatura-digital.info**, [20--]. Disponível em: http://assinatura-digital.info/. Acesso em: 21 mar. 2020.

CHIRIGATI, F. S.; KIKUCHI, R. S. A.; GOMES, T. L. Esteganografia. **Gta.ufrj**, c2006. Disponível em: http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html. Acesso em: 21 mar. 2020.

GAZZARRINI, R. O que é assinatura digital? **Techmundo.com.br**, c2012. Disponível em: http://www.tecmundo.com.br/web/941-o-que-e-assinatura-digital-.htm. Acesso em: 19 mar. 2020.

JEFFREY, B., (2002). Certification marks. London: Sweet &Maxwell. ISBN: 0421758201.

JULIO, E. P.; BRAZIL, W. G.; ALBUQUERQUE C. V. N., Esteganografia e suas Aplicações. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 7, 2007, Rio de Janeiro. **Anais eletrônicos**... Rio de Janeiro: UFF, 2007. p. 54-102. Disponível em: http://jeiks.net/wp-content/uploads/2013/11/cap2-esteganografia.pdf. Acesso em: 21 mar. 2020.

KOLLING, G. S. **Segurança da Informação**. [20--]. Disponível em: http://seguranca-da-informacao.info/. Acesso em: 24 mar. 2020.

KOREA, IWDW (Conference) (7th: 2008: Pusan, (2009). Digital watermarking: 7th international workshop, IWDW 2008, Busan, Korea, November 10-12, 2008: selected papers. [S.l.]: pringer. ISBN: 9783642044380.

MICROSOFT, Visão geral sobre os protocolos de autenticação. **Microsoft.com.br**, c2005. Disponível em: http://technet.microsoft.com/pt-br/library/cc739177(v=ws.10).aspx. Acesso em: 18 mar. 2020.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem, c2012. Disponível em: http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf. Acesso em: 18 mar. 2020.

SILVA, A. A. G. **A Perícia Forense no Brasil**, 2010. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2010. Acesso em: 18 mar. 2020.

TAIT, T. F. C. Evolução da Internet: do início secreto à explosão mundial. **Dim.uem.br**, c2007. Disponível em: http://www.din.uem.br/~tait/evolucao-internet.pdf. Acesso em: 18 mar. 2020.

PEREIRA, A. P.; O que é hash³? **Tecmundo**, 2009. Disponível em: http://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm. Acessado em: 21/03/2020.Acessado em :21 mar. 2020.

PETRI, M. **Esteganografia**. 2004. 56 f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Sociedade Educacional de Santa Catarina, Instituto Superior Tupy, Joinville, 2004. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_petri_esteganografia.pdf. Acesso em: 21 mar. 2020.

PISA, P. O que é criptografia? **Techtudo**, c2013. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html. Acesso em: 21 mar. 2020.

Reprodução/Google. Certificados de Autenticação. **Techmundo.com.br**, c2012. Disponível em: http://www.tecmundo.com.br/web/941-o-que-e-assinatura-digital-.htm. Acesso em: 21. Mar. 2020.

TRINTA, F. A. M., MACEDO, C. de. Um Estudo sobre Criptografia e Assinatura Digital. **Di.ufpe.br**, 1998. Disponível em: http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm. Acesso em: 24 mar. 2020.