Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

VINÍCIUS GUTIERRES MELLO FACHIANI

PERÍCIA DIGITAL NA IDENTIFICAÇÃO DE ESTEGANOGRAFIA EM IMAGENS E ARQUIVOS

Assis/SP
2018

Av. Getúlio Vargas, 1200 – Vila Nova Santana – Assis – SP – 19807-634
Fone/Fax: (0XX18) 3302-1055 homepage: www.fema.edu.br

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

VINÍCIUS GUTIERRES MELLO FACHIANI

PERÍCIA DIGITAL NA IDENTIFICAÇÃO DE ESTEGANOGRAFIA EM IMAGENS E ARQUIVOS

Exame de Qualificação do projeto de pesquisa apresentado ao Curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Vinícius Gutierres Mello Fachiani
Orientador(a): Prof. Me. Fábio Eder Cardoso

Assis/SP
2018

FICHA CATALOGRÁFICA

F139p FACHIANI, Vinícius Gutierres Mello.

Perícia Digital Na Identificação de Esteganografia em Imagens e Arquivos/ Vinícius Gutierres Mello Fachiani. Fundação Educacional do Município de Assis – FEMA – Assis, 2018.

49p.

Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis

Orientador: Prof. Me. Fábio Éder Cardoso.

1. Esteganografia. 2.Criptografia. 3.Segurança.

CDD: 005.8
Biblioteca da FEMA

PERÍCIA DIGITAL NA IDENTIFICAÇÃO DE ESTEGANOGRAFIA EM IMAGENS E ARQUIVOS

VINÍCIUS GUTIERRES MELLO FACHIANI

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____

Prof. Me. Fábio Éder Cardoso

Examinador: _____

Prof. Dr. Luiz Carlos Begosso

DEDICATÓRIA

Dedico este trabalho a minha família e amigos que sempre estiveram do meu lado e jamais me abandonaram sempre que precisei, nos momentos difíceis estiveram comigo para me dar apoio e sempre me mantiveram para cima.

AGRADECIMENTOS

Agradeço minha família que sempre esteve ao meu lado me apoiando, principalmente minha mãe, Solange Gutierres Mello Fachiani, que meio a vários problemas jamais deixou de me apoiar e sempre me dando forças independente da ocasião.

A minha amada noiva Bianca de Oliveira Moretti, que meio a tantos problemas sempre manteve um tempo especial a me ajudar e entender as dificuldades vindas, e podendo me manter no caminho da calma e paciência para resolver todos os problemas que apareceram e jamais desistir dos meus objetivos.

Aos meus amigos Leonardo de Castro Palma e Igor Delgado, por estarem ao meu lado nas dificuldades e orientarem o meu caminho a meio de dificuldades e tentativas de desistências.

Ao meu orientador Fábio Éder Cardoso, por manter a paciência em orientar, e estar presente compartilhando seus conhecimentos e experiências como ajuda para elaborar este trabalho.

E por fim, a quem sempre me motivou a continuar nos estudos e a jamais desistir do que eu sempre quis, não importando as dificuldades, e nem que se todos duvidassem de mim, era para sempre manter de cabeça erguida e continuar até o fim, que daria certo, ao meu pai, Mauro Roberto Fachiani, que por uma infelicidade não está entre nós, mas espero estar trazendo felicidade e orgulho para ele.

“Os que se encantam com a prática sem a ciência são como os timoneiros que entram no navio sem timão nem bússola, nunca tendo certeza do seu destino”.

Leonardo da Vinci

RESUMO

Este trabalho descreve a utilização e a explicação de ferramentas para aplicação da esteganografia para que possam ocultar mensagens e deixá-las seguras para a leitura apenas do seu emissor e de seu destinatário, evitando assim o roubo de informações e/ou senhas. Isso é feito em seu *bit* menos significativo (Técnica LSB), mostrando como esta técnica é efetuada e como ela pode ajudar muitas pessoas caso tenham seus arquivos roubados ou extraviados na Internet. Esta técnica é considerada muito segura e utilizada juntamente com a criptografia, podendo assim ser uma segurança ainda maior além da já existente, por não possuir um meio de visualizar se um arquivo está ou não estenografado a olho nu, a pessoa que visualizar o arquivo esteganografado não saberá dizer se este arquivo esconde algo ou não.

Palavras-chave: Esteganografia, Técnica LSB, Criptografia, Segurança.

ABSTRACT

This paper describes the use and explanation of steganography application tools so that they can hide messages and leave them safe to read only from their sender and recipient, thus avoiding the theft of information and / or passwords. This is done in its least significant bit (LSB Technique), showing how this technique is performed and how it can help many people if they have their files stolen or lost on the internet. This technique is considered very safe and used in conjunction with encryption, so it can be an even greater security than the existing one, because it does not have a means of visualizing whether or not a file is stenographed with the naked eye, the person who views the file steganography will not know if this file hides something or not.

Key-Words: Stenograph, LSB technique, Encryption, Security.

LISTA DE ILUSTRAÇÃO

Figura 1: Explicação Esteganografia no bit menos significativo (Técnica LSB).....20

Figura 2: Porção de pixels de uma imagem.....20

Figura 3: Porção de pixels com alteração da técnica LSB.....21

Figura 4: Cifra de César.....21

Figura 5: Trecho do código FileReader.....23

Figura 6: Inserção do Image Object dentro do Canvas.....24

Figura 7: Chamada e Utilização da Biblioteca SJCL.....25

Figura 8: Funções “charAtCode” e “bitwise” do Javascript.....26

Figura 9: Array recebendo os pixels da imagem.....26

Figura 10: Código que gera um local aleatório.....27

Figura 11: Código inserindo a mensagem codificada.....28

Figura 12: Imagem sem esteganografia, exemplo original.....28

Figura 13: Imagem esteganografia, com a mensagem citada.....29

Figura 14: Tela de apresentação da Aplicação WEB.....31

Figura 15: Tela de explicação breve sobre Esteganografia.....32

Figura 16: Tela da Aplicação WEB, “Esteganografia na Prática”.....33

Figura 17: Opção de seleção de uma imagem.....34

Figura 18: Seleção de um arquivo de Imagem para a esteganografia.....34

Figura 19: Pré-visualização da imagem escolhida pelo usuário.....35

Figura 20: Apresentação dos botões de configuração.....36

Figura 21: Botão codificar para a inserção de uma mensagem.....37

Figura 22: Liberação das áreas para a inserção da mensagem.....38

Figura 23: Exemplo de mensagem para inserção.....39

Figura 24: Mensagem de sucesso ao esteganografar.....40

Figura 25: Mensagem muito longa para a imagem enviada.....40

Figura 26: Imagem esteganografada.....41

Figura 27: Escolher imagem para a leitura da esteganografia.....42

Figura 28: Botão decodificar para realizar a leitura de uma mensagem.....42

Figura 29: Área para inserção da senha liberada.....43

Figura 30: Senha inserida para a remoção da esteganografia.....44

Figura 31: Mensagem revelada após a inserção da senha.....44

Figura 32: Alerta sobre Senha Incorreta ou nenhuma mensagem Inserida.....45

Figura 33: Alerta sobre a aplicação travada.....46

Figura 34: Quantidade de caracteres em uma mensagem.....46

LISTA DE ABREVIATURAS E SIGLAS

LSB – *Least Significant Bit*

ASCII - *American Standard Code for Information Interchange*

RGB – *Red, Green and Blue*

API – *Application Programming Interface*

HTML – *HyperText Markup Language*

SJCL – *Stanford Javascript Crypto Library*

AES – *Advanced Encryption Standart*

JSON – *Javascript Object Notation*

SUMÁRIO

1. INTRODUÇÃO 14
1.1 OBJETIVO 14
1.2 JUSTIFICATIVA 15
1.3 MOTIVAÇÃO 15
1.4 PERSPECTIVAS DE CONTRIBUIÇÃO 16
1.5 METODOLOGIAS DE PESQUISA 16
1.6 ESTRUTURA DO TRABALHO 17

2. ESTEGANOGRAFIA E CRIPTOGRAFIA 18
2.1 ESTEGANOGRAFIA 18
2.2 TÉCNICA LSB (LEAST SIGNIFICANT BIT) 19
2.3 CRIPTOGRAFIA 21

3. BIBLIOTECA PIXELJIHAD 22
2.1 INTRODUÇÃO 22
2.1 PIXELJIHAD 22

4. APLICAÇÃO WEB ESTEGANOGRAFIA 30
4.1 INTRODUÇÃO 30
4.2 APRESENTAÇÃO SOBRE ESTEGANOGRAFIA 30
4.3 ESTEGANOGRAFIA NA PRÁTICA 32
4.4 ESTEGANOGRAFANDO UMA MENSAGEM 36
4.5 REALIZANDO A LEITURA DA MENSAGEM 41
4.6 LIMITAÇÃO DO USO DA APLICAÇÃO 45

5. CONCLUSÃO 47

6. REFERÊNCIAS 48

1. INTRODUÇÃO

A perícia forense computacional tem sido aprimorada cada vez mais, no qual o objetivo é identificar, recuperar e apresentar evidências digitais que possam incriminar ou facilitar na procura do malfeitor. De acordo com FREITAS (2006) a Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, quer sejam os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.

PINHEIRO (2005) descreve que, ao contrário da criptografia, que procura esconder a informação da mensagem, a esteganografia consiste em ocultar uma determinada informação, seja um arquivo de texto ou uma imagem, dentro de outro arquivo, de tal maneira que não será possível (de forma normal) perceber a existência dessa informação. Apenas o emissor e o destinatário da imagem "estenografada" conseguem ver o texto, através do uso de um programa apropriado e de posse da chave usada nesse processo.

De acordo com TECHNOLOGY (2010), esteganografia moderna funciona substituindo *bits* de dados inúteis ou não utilizados em arquivos de computador comuns com *bits* de informações diferentes e invisíveis. Quando um arquivo não pode ser criptografado, a próxima melhor opção para transferência segura é esteganografia. A esteganografia também pode ser usada para complementar a criptografia. Quando usado dessa maneira, a esteganografia fornece uma dupla medida de proteção, pois o arquivo criptografado, uma vez decifrado, não permitirá uma mensagem escondido por esteganografia para ser visto. O receptor do arquivo precisa usar um *software* especial para decifrar uma mensagem escondido pela esteganografia.

1.1. OBJETIVO

O objetivo desse trabalho é o de elaborar uma ferramenta de aplicação web para apresentar as técnicas e realizar a identificação de imagens e arquivos que estejam estenografados, com isso, realizar seus devidos testes para demonstrar os métodos que são realizados na esteganografia, mostrando o passo a passo de como e o porquê utilizam esta tecnologia nos dias de hoje, utilizado juntamente com a criptografia.

Com os métodos e ferramentas que serão utilizados na aplicação da esteganografia neste trabalho, devidamente apresentados e explanados, será elaborada e demonstrada uma Aplicação Web para atestar na prática a utilização e função da Esteganografia, para a criptografia e ocultamento de uma mensagem, e na identificação da mesma.

1.2. JUSTIFICATIVA

Para a análise forense é um grande desafio acompanhar os avanços da tecnologia pelo fato da vasta amplitude que a internet representa e a quantidade de malfeitores presentes nela, assim não podendo proteger todos os usuários que a utilizam, seja para uso pessoal, comercial ou militar. A esteganografia permite um meio a mais para a proteção de seus dados, porém podendo ser utilizada legalmente ou ilegalmente. Com isso, é necessária uma ferramenta, e um estudo que auxilie na identificação da esteganografia e comprove sua existência.

1.3. MOTIVAÇÃO

O aperfeiçoamento deste trabalho de pesquisa baseia-se no fato de que a esteganografia é um tema ainda pouco conhecido e pode contribuir com a segurança de dados de muitos usuários.

A Esteganografia ajuda a manter dados seguros e possibilita a transmissão de mensagens, textos ou documentos sem que possa ser possível identificar que esteja sendo transmitido, tendo aplicações em várias áreas, como por exemplo comercial e militar.

Sendo aplicada na área comercial, um exemplo de uso seria na inserção de marcas d’água digitais, onde é inserido dentro da imagem não podendo ser identificado, onde apenas o autor saberá de sua existência, e caso contestado a sua veracidade e propriedade da imagem, poderá ser apresentada a prova da assinatura digital existente dentro da mesma.

Já sua aplicação na área militar poderia ser utilizada para a transmissão de mensagens sigilosas, localizações ou qualquer outra opção desejada com o envio de uma simples imagem de um pôr-do-sol por exemplo, mesmo que interceptada, seria apenas uma imagem comum.

Do mesmo modo, pode ser utilizada ilegalmente, por exemplo para terrorismo, transmitir uma mensagem de ataque ou localização de suprimentos, sem a detecção de ninguém, ou para uso mais pessoal, na ocultação de dados fraudulentos de uma empresa ou espionagem industrial por exemplo.

Portanto uma ferramenta para sua identificação ou aplicação, e um estudo mais aprofundado sobre a Esteganografia para apresentar seus métodos é necessário para o maior conhecimento e explanar seus meios de aplicações para esta.

1.4. PERSPECTIVA DE CONTRIBUIÇÃO

Este trabalho propõe com sua finalidade propagar um maior conhecimento quanto a Esteganografia e suas aplicações práticas nos dias de hoje, fornecendo um histórico de sua utilização e como podendo ser aplicada atualmente. Com isso elaborando também uma aplicação web para a demonstração com maior efetividade de sua funcionalidade e disponibilizando também, o código em modo aberto, caso haja a curiosidade de um seguimento com este trabalho por outras pessoas em busca deste mesmo assunto, sendo disponibilizado posteriormente no *github*.

1.5. METODOLOGIA DE PESQUISA

Para a realização deste trabalho, a metodologia utilizada foi a realização de pesquisas em sites da internet através de artigos científicos, apostilas, sites e outros trabalhos de conclusão de curso. Para aplicação final foi utilizada a tecnologia HTML5 para a base da aplicação, juntamente com CSS para a estilização da página e JavaScript como linguagem principal para a parte do Back-end, juntamente com a biblioteca PixelJihad, feita totalmente em JavaScript, contendo toda a configuração para a utilização e aplicação da esteganografia, e possuindo internamente a biblioteca SJCL para a aplicação de criptografia e inserção de senha.

1.6. ESTRUTURA DO TRABALHO

O trabalho está estruturado como o Capítulo 1 apresentando a Introdução e os objetivos sobre este trabalho de conclusão de curso, juntamente com a metodologia usada e a perspectiva de contribuição. O Capítulo 2 explica sobre Esteganografia e Criptografia, definindo melhor sobre cada item, explicando detalhadamente o que é a esteganografia, suas aplicações práticas, a técnica utilizada e como aplica-la, e na criptografia, qual será utilizada e um resumo breve sobre tal. O Capítulo 3 define a biblioteca e as tecnologias que serão utilizadas para a elaboração da aplicação web, explanando o que a biblioteca PixelJihad faz por completo, desde receber a imagem até a exportação da imagem já esteganografada. O Capítulo 4 será apresentada a aplicação web e uma explicação detalhada de todas as suas funções e como utiliza-las completamente, podendo ter uma utilização melhor dela de todos os modos. O Capítulo 5 apresenta todas as conclusões tiradas ao decorrer deste trabalho, desde aprendizados até a aplicações práticas para a esteganografia. E por fim, as referências

2. ESTEGANOGRAFIA E CRIPTOGRAFIA

Neste capítulo será explanado o significado de Esteganografia, sua origem e suas aplicações ao decorrer dos anos, o método mais utilizado para a aplicação, e sua interação com a criptografia para tornar mais seguro.

2.1. ESTEGANOGRAFIA

A esteganografia é um procedimento no qual é possível ocultar mensagens sem que possa ser descoberto a sua existência por uma pessoa na qual não saiba que aquela mensagem esteja ali encoberta, imperceptível a olho nu, apenas quem efetuou a esteganografia e quem ele deseja que conheça a sua existência estarão ciente dela.

A criptografia utiliza ferramentas matemáticas para manipular os dados originais até se obter uma nova sequência de dados, derivada a partir do original e de uma chave de criptografia, conseguindo assim, proteger o conteúdo da informação. Essas duas técnicas não são de forma alguma incompatíveis. De fato, muitas aplicações buscam utilizar ambas em conjunto. (GIL, Fernando O.; MALANDRIN, Leandro José A. A.; MORIGAKI, Roberto. H.; BARRETO, Paulo. S. L. M., 2008).

A esteganografia aplicada a imagens busca transformar os bits de pixels menos significativos nos bits da mensagem que se deseja esconder. Logicamente, esse processo envolve uma perda da qualidade da imagem original. No entanto, dependendo do algoritmo utilizado, a imagem contendo a mensagem secreta e a imagem original não apresentam diferenças que possam ser identificadas a olho nu pelo ser humano. (GIL, Fernando O.; MALANDRIN, Leandro José A. A.; MORIGAKI, Roberto. H.; BARRETO, Paulo. S. L. M., 2008).

A técnica que altera os bits menos significativos para a inserção de caracteres para esconder a mensagem na imagem se chama Técnica LSB (*Least Significant Bit*), que será utilizada para o desenvolvimento da aplicação web.

A esteganografia por si só, se torna impossível detecta-la, mas com a utilização da criptografia a torna ainda mais segura. Pois eventualmente alguma aplicação detecte a

presença de uma mensagem esteganografada dentro de uma imagem, ela poderá ser lida normalmente, mas com a presença de uma criptografia juntamente com esteganografia, a mensagem poderá ser interceptada, mas sem a *hash* utilizada, que é gerada unicamente junto com a senha fornecida para criptografa-la, será impossível ler a mensagem.

2.2. TÉCNICA LSB (*LEAST SIGNIFICANT BIT*)

Uma imagem digital é constituída por uma quantidade de *pixel* (a menor proporção da imagem), e cada *pixel* possui as camadas de cores vermelho, verde e azul (alguns formatos de imagens podem possuir a camada de cor *Alpha,* onde é tratada a transparência da imagem), que são uma sequência de 8 *bits* cada uma das cores, ou seja, cada *pixel* é representado por uma sequência de 24 *bits.* Caso seja feita uma alteração nos 4 bits menos significativos de cada cor (vermelho, verde ou azul), representaria uma mudança quase que imperceptível na imagem. Os códigos *ASCII (American Standard Code for Information Interchange)* que são utilizados para formar o alfabeto da linguagem inglesa em computação, no qual cada caractere de sua linguagem é formado por 8 bits, sendo assim, cada *pixel* possuindo 24 bits, utilizando 4 bits de cada, podemos inserir 1,5 caractere por *pixel* de cada imagem. Para uma noção um pouco melhor, uma imagem retirada da internet de 5 *megapixels,* possui cerca de 5 milhões de *pixels*, é possível inserir uma média de 7,5 milhões de caracteres nesta imagem, sem nenhuma alteração gráfica visível a alguma pessoa que analise a imagem.

Na figura 1, pode-se entender um pouco sobre o método LSB.

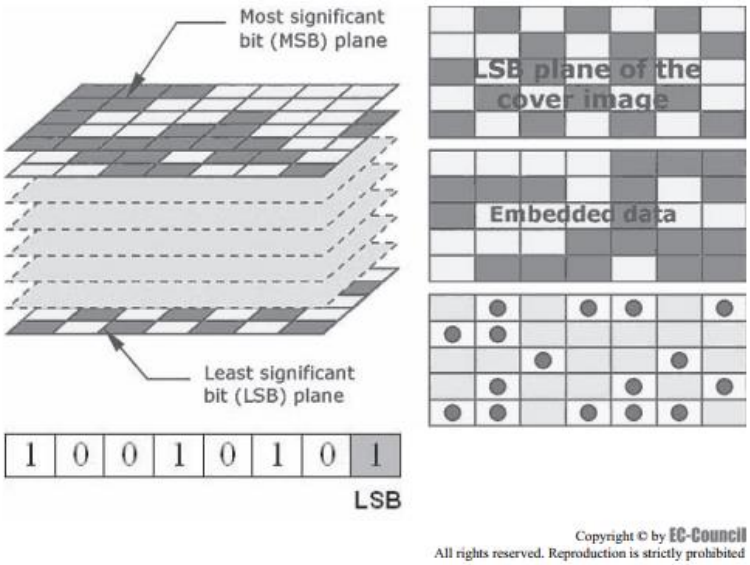

Figura 1: Explicação Esteganografia no bit menos significativo (Técnica LSB).
Fonte: TECHNOLOGY (2010). Acessado em: 28JUL2018

Representado na figura 2, temos um exemplo de porção de *pixels* de uma imagem, com os canais de RGB, sendo respectivamente *Red*, *Green* e *Blue*, ou seja, os canais de cores vermelho, verde e azul que constituem um *pixel*. Para podermos inserir a letra **V**, que seu código *ASCII* em binário se torna **01010110**, algumas alterações nos bits menos significativos desta imagem são necessárias.

(01001101 11001101 11100010) [R, G, B]
(10100011 00110110 10011100) [R, G, B]
(11001100 11001111 00100111) [R, G, B]

Figura 2: Porção de *pixels* de uma imagem.
Fonte: elaborado pelo autor.

Na figura 3, já foram realizados os ajustes necessários para a inserção da Letra **V** com a técnica LSB, em sublinhado estão os *bits* que foram modificados, e como são os menos significativos, nenhuma alteração visual poderá ser notada na imagem, caso seja analisada em busca de alterações visíveis.

(01001100 11001101 11100010) [R, G, B]
(10100011 00110110 10011101) [R, G, B]
(11001101 11001110 00100111) [R, G, B]

Figura 3: Porção de *pixels* com alteração da técnica LSB.

Fonte: elaborado pelo autor.

2.3. CRIPTOGRAFIA

Criptografar é a arte de transformar textos ou dados em um código secreto, ou seja, converter em um texto incompreensível uma mensagem escrita normalmente, de forma que apenas quem escreveu e quem saiba decifrar saiba o que esteja escrito ali. Para podermos criptografar ou decifrar uma mensagem criptografada é necessária uma sequência numérica denominada chave, tornando mais seguro a mensagem sendo que apenas quem tivesse aquela chave ou senha poderia decifrar a mensagem. Atualmente se utiliza uma *hash,* que é uma sequência aleatória de números e caracteres no qual torna ainda mais segura essa criptografia, tendo milhões de combinações possíveis e tornando cada vez mais impossível de se decifrar sem a presença dessa hash.

Uma das primeiras criptografias conhecidas é chamada de Cifra de César, que foi elaborada pelo General Júlio César do Império Romano. Como podemos ver na Figura 4, ele substituiu a letra que gostaria de escrever pela 3 letra seguinte do alfabeto, sendo a letra “A” equivalente a letra “D”, a letra “B” equivalente a letra “E” e assim subsequentemente.

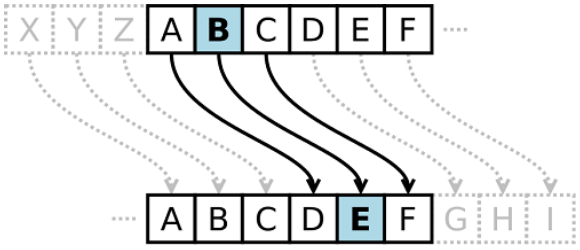

Figura 4: Cifra de César.

Fonte: <http://www.facom.ufu.br/~albertini/prossiga/images/4/4f/Cifczar.PNG**>**

Acessado em: 28JUL2018

3. BIBLIOTECA PIXELJIHAD

3.1. INTRODUÇÃO

Neste capítulo será apresentada a biblioteca utilizada na criação da aplicação web para demonstrar a esteganografia na prática. Foi utilizada a biblioteca PixelJihad, totalmente feita em JavaScript e de fácil aplicação. Já implementada nela temos a biblioteca SJCL.js, utilizada para a criptografia e a inserção de senha, caso o usuário escolha, dentro da mensagem que será inserida na imagem, dando assim uma segurança a mais para a nossa esteganografia e tornando a aplicação mais completa.

3.2. PIXELJIHAD

Com a tecnologia presente nos *browsers* atualmente, há a possibilidade de realizar a técnica LSB sem a necessidade da utilização de um servidor como meio de intermédio para a realização da modificação e tratamento da imagem em nível binário para a inserção dos caracteres desejados.

Com o *FileReader*, presente nativamente no *JavaScript*, é utilizado para a leitura e o carregamento de arquivos pelo usuário, enviando para uma memória temporária no próprio navegador, para um acesso posterior mais rápido e sem a obrigação da busca do mesmo em seu computador novamente, e sem a necessidade de um upload a um servidor para ser acessado mais uma vez, podendo assim ser utilizado sem a necessidade de uma acesso à internet ou um servidor mesmo que local, tornando mais prática a utilização da aplicação, mesmo sendo web, pode-se usar *off-line.* E com esta API nativa, podemos realizar a modificação da imagem com a utilização juntamente da ferramenta *Canvas*

A ferramenta *Canvas* na qual já está atribuída no HTML e *Javascript*, é unicamente um container para desenho dentro do HTML, podendo assim inserir a imagem e manuseá-la da forma necessária, e então realizar a implementação da técnica de LSB, inserindo a

imagem que foi recebida pelo usuário e armazenada pela *FileReader*, para a esteganografia sem a utilização de um servidor para o tratamento e a implementação do código.

Para realizar todos os processos da Esteganografia com as ferramentas anteriormente mencionadas, será utilizada a biblioteca *PixelJihad*, criada pelo programador Zach Oakes, em 25 de junho de 2012, que utiliza puramente HTML 5, feito apenas em JavaScript, sem a necessidade da utilização sequer de *JQuery (*uma ferramenta mais avançada de JavaScript).

A Esteganografia se torna mais acessível e fácil sua prática através da utilização da aplicação web, onde a biblioteca se torna responsável pela leitura da imagem fornecida pelo usuário, através do *FileReader,* e a transforma em um objeto para então ser feita a inserção dela no canvas, podendo assim ser feito a leitura e a modificação de sua estrutura binária.

Com uma "*Text Area*" disponível, é feita a leitura da mensagem da qual o usuário deseja inserir, então com a utilização de uma outra biblioteca inseria dentro da *PixelJihad,* a SJCL (Stanford Javascript Crypto Library), uma biblioteca de criptografia na qual utiliza de SHA256 para criptografar, é enviada a mensagem juntamente com a senha fornecida pelo usuário, então se retorna os dados gerados e criptografado, transformado em dados binários e então inseridos dentro da imagem após uma seleção aleatória de qual pixel será o inicial.

Primeiramente, iremos ter que fazer a leitura da imagem na qual o usuário irá implementar a esteganografia, como visto no trecho de código da Figura 5 a seguir, utilizaremos o FileReader, como está ferramenta recebe todos os arquivos, podemos limita-la a apenas imagens para mantermos nosso foco neste método, sendo o apresentado atualmente.

```
var reader = new FileReader();
reader.onload = function(event) {
  var dataUrl = event.target.result;
  // ...
};
reader.readAsDataURL(e.target.files[0]);
```

Figura 5: Trecho do código *FileReader*.

Fonte: <https://sekao.net/pixeljihad/about.html**>**

Acessado em: 28JUL2018

Com o arquivo aberto pelo *FileReader*, podemos manipula-lo da maneira que seja necessária, então colocaremos o arquivo dentro de um *Image Object* para então realizarmos a inserção em um *Canvas,* podendo assim ser manipulado os dados binários da imagem sem restrição, e sem a alteração visual na imagem selecionada. Na Figura 6 podemos visualizar o trecho que realiza a inserção do *Image Object* dentro do *Canvas.*

```
var img = new Image();
img.onload = function() {
  var canvas = document.getElementById('canvas');
  var ctx = canvas.getContext('2d');
  ctx.canvas.width = img.width;
  ctx.canvas.height = img.height;
  ctx.drawImage(img, 0, 0);
  // ...
};
img.src = dataUrl;
```

Figura 6: Inserção do *Image Object* dentro do *Canvas*.
Fonte: <https://sekao.net/pixeljihad/about.html>
Acessado em: 28JUL2018

Para uma segurança extra na sua esteganografia, podemos ter a opção em nossa aplicação para a inserção de uma senha em nossa mensagem, ouse já, uma encriptação dos dados a serem inseridos, com uma própria *hash,* inserida pelo usuário, tornando assim a decriptação dela única, sendo realizada apenas com a presença desta senha, garantindo que os únicos que terão acessos a este dado esteganografado, serão o emissor e o receptor.

Com o objetivo de realizar esta encriptação, iremos utilizar uma biblioteca externa para garantir que seja mais seguro e não tenhamos que nos preocupar com esta parte do trabalho, podendo assim assegurar mais tempo para a técnica em foco, a LSB. Eventualmente com o aperfeiçoamento de nossa aplicação *web*, optaremos com o aperfeiçoamento desta técnica implementando uma biblioteca para esta tarefa.

A biblioteca selecionada para a encriptação será a SJCL (Stanford Javascript Crypto Library), acessível gratuitamente na plataforma *github*, utiliza a tecnologia de algoritmo AES

(Advanced Encryption Standart), sendo o padrão no qual o governo dos Estados Unidos da América adota para a implementação de criptografias. Podendo ser criptografados em 128, 192 ou até mesmo 256 *bits*, com vários métodos não listados aqui por não ser o foco de nosso estudo, apenas um meio para atingir nosso objetivo, o principal é o método SHA256 com hash, será a ferramenta que iremos estar utilizando e mostrando nesta pesquisa. Na figura 7 podemos visualizar como efetuamos sua chamada e utilização de sua ferramenta, passando a senha que o usuário irá inserir através da variável "*password*", seguido da mensagem que será criptografado em seguida com a utilização da senha. Caso não seja colocada senha alguma pelo usuário, o tratamento "else" apenas transforma a mensagem em um JSON, para o melhor tratamento e utilização.

```
if (password.length > 0) {
  message = sjcl.encrypt(password, message);
} else {
  message = JSON.stringify({'text': message});
}
```

Figura 7: Chamada e Utilização da Biblioteca SJCL.

Fonte: <https://sekao.net/pixeljihad/about.html>

Acessado em: 28JUL2018

Para que a mensagem possa ser esteganografada, é necessário que seja convertida em binário, ou seja, transformar a mensagem desejada em 1s e 0s. Para isso ser possível, será usada outra função já nativa do *JavaScript*, o "*charCodeAt*", como podemos ver na figura 8 a sua utilização. Esta função nos retornará um valor de 2-*byte*, então teremos que pegar os valores separados de cada *bit* com a função "*bitwise*".

```
var getBit = function(number, location) {
  return ((number >> location) & 1);
};

var getBitsFromNumber = function(number) {
  var bits = [];
  for (var i = 0; i < 16; i++) {
    bits.push(getBit(number, i));
  }
  return bits;
};

var messageBits = [];
for (var i = 0; i < message.length; i++) {
  var code = message.charCodeAt(i);
  var bits = getBitsFromNumber(code);
  messageBits = messageBits.concat(bits);
}
```

Figura 8: Funções "charAtCode" e "bitwise" do Javascript.
Fonte: <https://sekao.net/pixeljihad/about.html>
Acessado em: 28JUL2018

Com a imagem selecionada pelo usuário já inserida no Canvas demonstrado anteriormente, o trabalho se torna simples daqui em diante, pois ele retorna todos os *pixels* da imagem, em forma de um *array*, sendo o *array*[0] o "*red*" do primeiro *pixel*, *array*[1] o "*green"* do primeiro *pixel*, *array*[2] o "*blue"* do primeiro *pixel*, array[3] o *alpha* (caso o formato da imagem suporte *alpha color*) do primeiro *pixel,* já o *array*[4] se torna o "*red*" do segundo *pixel,* assim iniciando o ciclo novamente. Como demonstrado na figura 9, temos o trecho do código que recebe o *array* dos *pixels* da imagem na variável "colors".

```
var imgData = ctx.getImageData(0, 0, width, height);
var colors = imgData.data;
```

Figura 9: Array recebendo os *pixels* da imagem.
Fonte: <https://sekao.net/pixeljihad/about.html>
Acessado em: 28JUL2018

A partir deste momento há a necessidade de inserir a mensagem que foi criptografada (caso tenha sido a escolha do usuário) e transformado em sequência binária. A anexação comum

aconteceria com início no primeiro *pixel*, o *array*[0], no entanto, resultaria em uma maneira muito fácil de se detectar caso a imagem fosse analisada a nível binário em busca de algo fora do comum ou até a nível visual, por ocorrências de combinações binarias, ser geradas algumas manchas brancas nos *pixels*. Neste caso, uma técnica na qual se usa a *hash* gerada a partir da senha que o usuário forneceu (caso não tenha sido fornecida uma senha, é gerada uma hash diferente, porém continua sendo funcional), para escolher os *pixels* que serão alterados para a mensagem codificada ser armazenada, e assim tornar-se mais difícil a identificação tanto a nível binário quanto a nível visual. Como pode ser visto na figura 10, o trecho do código no qual gera este local aleatório para a inserção dos caracteres.

```
var hash = sjcl.hash.sha256.hash(password);
var pos = 0;
while (pos < messageBits.length) {
  var rand = hash[pos % hash.length] * (pos + 1);
  var loc = Math.abs(rand) % colors.length;
  // ...
  pos++;
}
```

Figura 10: Código que gera um local aleatório.

Fonte: <https://sekao.net/pixeljihad/about.html>

Acessado em: 28JUL2018

Neste momento, com a localização já devida randomicamente a partir do *hash*, pode-se inserir enfim a mensagem com a utilização do “*bitwise*”, para nos localizar o *bit* 0 (menos significativo) das cores (*red, green, blue* e *alpha* casa haja no formato identificado) de cada *pixel* selecionado, que segue no trecho da figura 11.

```
var setBit = function(number, location, bit) {
  return (number & ~(1 << location)) | (bit << location);
};
// ...
colors[loc] = setBit(colors[loc], 0, messageBits[pos]);
```

Figura 11: Código inserindo a mensagem codificada.

Fonte: <https://sekao.net/pixeljihad/about.html>

Acessado em: 28JUL2018

A seguir é apresentado um exemplo de uma imagem na qual foi utilizado o método acima para a aplicação da esteganografia com senha para a criptografia da mesma, e assim para demonstrar que não há nenhuma alteração visual para a aplicação da mensagem e alteração do *bit* menos significativo de cada *pixel*. A figura 12 apresenta a imagem sem alteração, usaremos ela como exemplo para a aplicação da mensagem.

Figura 12: Imagem sem esteganografia, exemplo original.

Fonte: <https://www.assisnews.com.br/wp-content/uploads/2017/10/FEMA-800x610.jpg>

Acessado em: 28JUL2018.

Agora a figura 13 apresentara a mensagem inserida com esteganografia utilizando a técnica LSB e os métodos acima demonstrado, com o conteúdo: “Imagem de exemplo para o TCC sobre Esteganografia”, e a senha utiliza será “FEMA”.

Figura 13: Imagem esteganografia, com a mensagem citada.

Fonte: <https://www.assisnews.com.br/wp-content/uploads/2017/10/FEMA-800x610.jpg>

Alterado pelo autor. Acessado em: 28JUL2018

4. APLICAÇÃO WEB ESTEGANOGRAFIA

4.1. INTRODUÇÃO

Para um melhor aproveitamento dos ensinamentos da esteganografia deste trabalho, foi elaborado e construído uma aplicação web para demonstração na prática do uso da esteganografia, tanto para realizar a inserção de uma mensagem, quanto para a identificação e descobrimento da mensagem e remoção da criptografia para apresentar a mensagem escondida.

Será apresentado um passo a passo da utilização da aplicação web para um melhor entendimento de seu uso.

4.2. APRESENTAÇÃO SOBRE ESTEGANOGRAFIA

Para uma explicação e entendimento da utilização da Esteganografia, estará sendo ensinado como realizar e aproveitar o uso da aplicação web.

Primeiramente ao acessar a aplicação, sem nenhuma necessidade da utilização de um servidor, sendo possível a utilização local e sem acesso à internet, será apresentado a página da Figura 14, explanando o propósito da aplicação web. Como é possível ver também, na área superior da aplicação, encontra-se os botões de Home, que retorna o usuário para a área inicial do site, o botão “Sobre Esteganografia”, no qual é apresentado uma explicação breve sobre a esteganografia e possui citações de autores, e por fim, o botão “Esteganografia na Prática”, no qual poderá ser realizada a inserção ou a leitura de uma mensagem dentro de uma imagem, tornando nosso estudo apresentado neste trabalho de conclusão de curso, efetivo na prática.

Figura 14: Tela de apresentação da Aplicação WEB.
Fonte: elaborado pelo autor.

Após a página de apresentação da aplicação, possui um pequeno texto e menção de autores para uma breve explicação sobre o que é Esteganografia, para o usuário que acessar a aplicação entender um pouco melhor sobre o que se trata tal site, como é apresentado na Figura 15.

Figura 15: Tela de explicação breve sobre Esteganografia.
Fonte: elaborado pelo autor.

4.3. ESTEGANOGRAFIA NA PRÁTICA

Na última área da aplicação encontra-se a parte prática na qual irá ser aplicada toda a tecnologia e ensinamento aqui apresentado, para a realização de nossa esteganografia, para a inserção ou leitura de uma mensagem em alguma imagem na qual o usuário irá selecionar. Poderá entrar nesta área ao se rolar a página para baixo, ou clicar no botão que se encontra na parte superior onde está escrito “Esteganografia na prática”, na qual possui uma âncora HTML para ser encaminhado para a área da aplicação, como pode ser visto na Figura 16, está é a parte inicial da aplicação, onde será explanado mais adiante como utilizá-la.

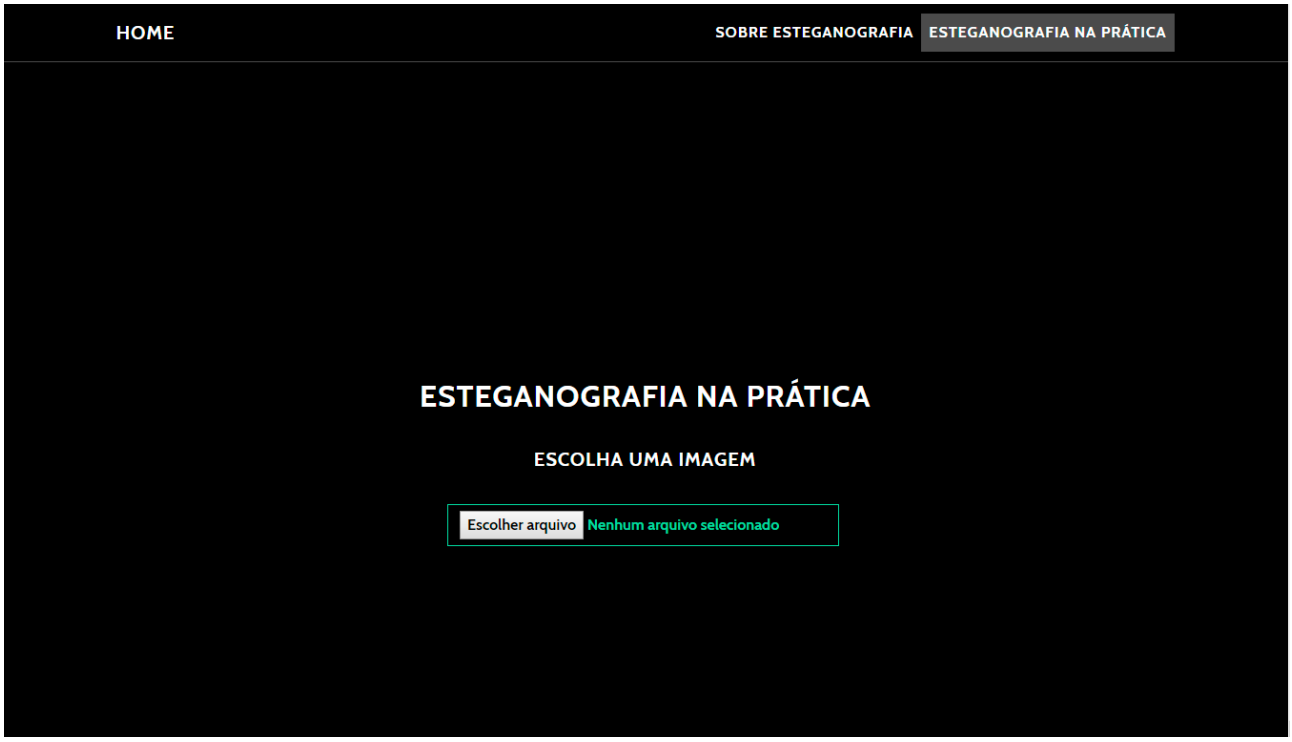

Figura 16: Tela da Aplicação WEB, “Esteganografia na Prática”.
Fonte: elaborado pelo autor.

Agora para ser possível a realização da esteganografia, terá que ser inserido uma imagem dentro da área *FileReader* do HTML para ser liberada as opções de inserir uma mensagem ou ler. Ao clicar em “Escolher Arquivo” será aberta a opção de seleção de uma imagem em seu computador, será possível apenas a seleção de imagens, outros arquivos não aparecerão, pois, a configuração do HTML restringiu para apenas seleção de imagens.

Como é possível ver na Figura 17, ao se clicar em “Escolher Arquivo”, será aberto a opção de seleção de uma imagem, como é possível ver na Figura 18. Será utilizada a figura previamente apresentada no Capítulo anterior, sobre a explanação da biblioteca PixelJihad, para uma melhor visualização.

Figura 17: Opção de seleção de uma imagem.

Fonte: elaborado pelo autor.

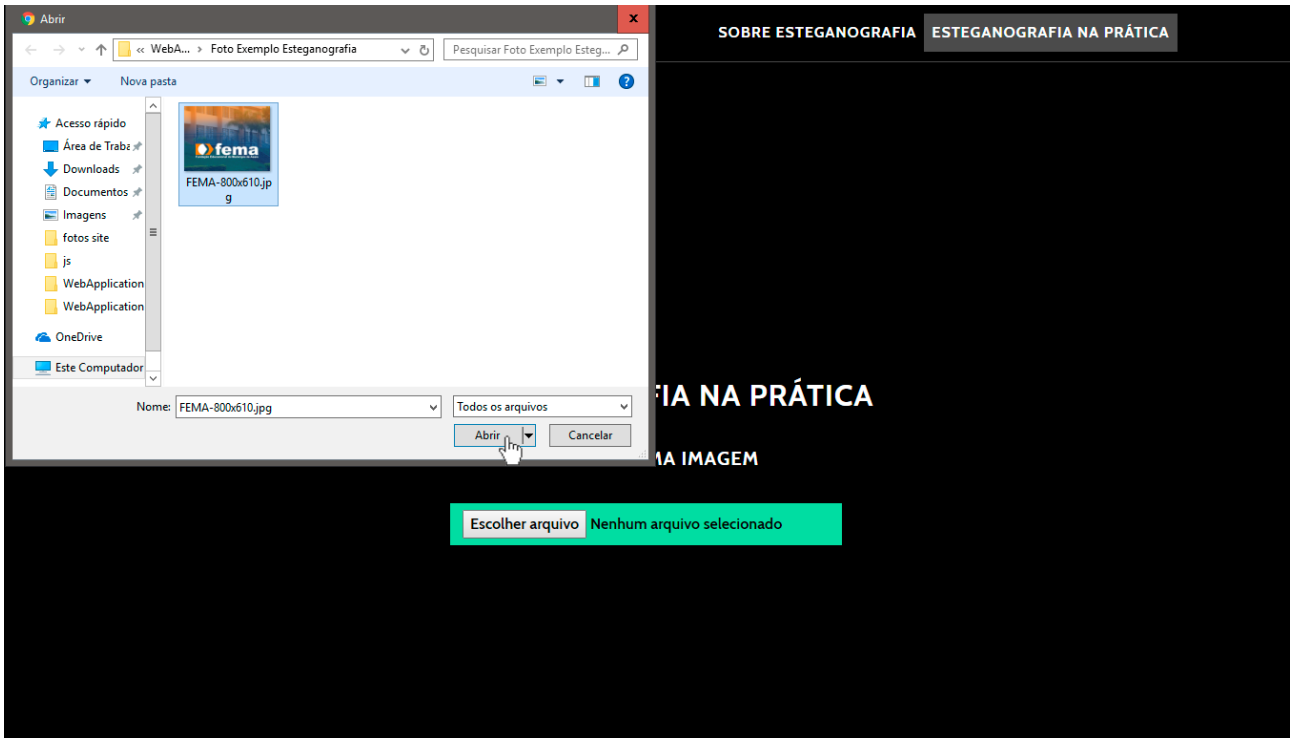

Figura 18: Seleção de um arquivo de Imagem para a esteganografia.

Fonte: elaborado pelo autor.

Após a seleção da imagem e clicado no botão “Abrir”, será enviada para a página web e será exibida uma pré-visualização da imagem para o usuário verificar se aquela imagem pré-carregada é a que ele deseja utilizar para a realização da esteganografia, como pode ser visto na Figura 19, caso a imagem não seja a desejada, poderá ser feita a troca da mesma ao clicar em “Escolher Arquivo” novamente e selecionando a imagem desejada, sem a necessidade de recarregar a página ou executá-la novamente.

Figura 19: Pré-visualização da imagem escolhida pelo usuário.
Fonte: elaborado pelo autor.

Após a inserção da imagem escolhida pelo usuário e a confirmação de que a mesma escolhida está correta, serão liberados dois botões no qual o usuário fará a escolha, se deseja inserir uma mensagem esteganografada na imagem selecionada, ou se deseja realizar a leitura de uma mensagem, mediante a inserção de uma senha. Como podemos visualizar na Figura 20, os botões são apresentados logo abaixo da pré-visualização e são distintos um do outro, com uma explicativa neles mesmo.

Figura 20: Apresentação dos botões de configuração.
Fonte: elaborado pelo autor.

Para um melhor entendimento, serão apresentados os dois métodos da aplicação web para a esteganografia, a inserção e a leitura de uma imagem esteganografada. Para início, será demonstrado como realizar uma inserção de uma mensagem em uma imagem, para após a inserção, será realizada a leitura dessa mesma mensagem na imagem para a confirmação do funcionamento de nossa aplicação.

4.4. ESTEGANOGRAFANDO UMA MENSAGEM

Caso o usuário deseje realizar uma inserção de uma mensagem esteganografada na figura pré-carregada na página web de nossa aplicação, ele deverá apenas clicar em “Codificar”, como podemos ver o exemplo na Figura 21.

Figura 21: Botão codificar para a inserção de uma mensagem.
Fonte: elaborado pelo autor.

Após o usuário selecionar o botão “Codificar” serão liberadas as áreas necessárias para o preenchimento dos dados para a realização da esteganografia, apresentados na Figura 22, como a *TextArea* “Mensagem”, onde a mensagem desejada a ser inserida na imagem deverá ser informada, e um *Input type* de password, onde caso o usuário desejar que a sua mensagem seja criptografa com uma senha por ele fornecida, deverá inserir nesta área, porém, não é obrigatório, podendo deixar vazio caso deseje inserir a mensagem sem alguma senha.

Figura 22: Liberação das áreas para a inserção da mensagem.
Fonte: elaborado pelo autor.

Para o nosso exemplo será inserida a mensagem “Imagem de exemplo para o TCC sobre Esteganografia”, a mesma mensagem apresentada no Capítulo anterior, como pode ser visto na Figura 23, a mensagem está dentro da *TextArea* “Mensagem para Esteganografar”, onde possui um limite de 10000 caracteres para uma mensagem, logo a baixo a senha “FEMA” foi inserida para a criptografia de nossa mensagem.

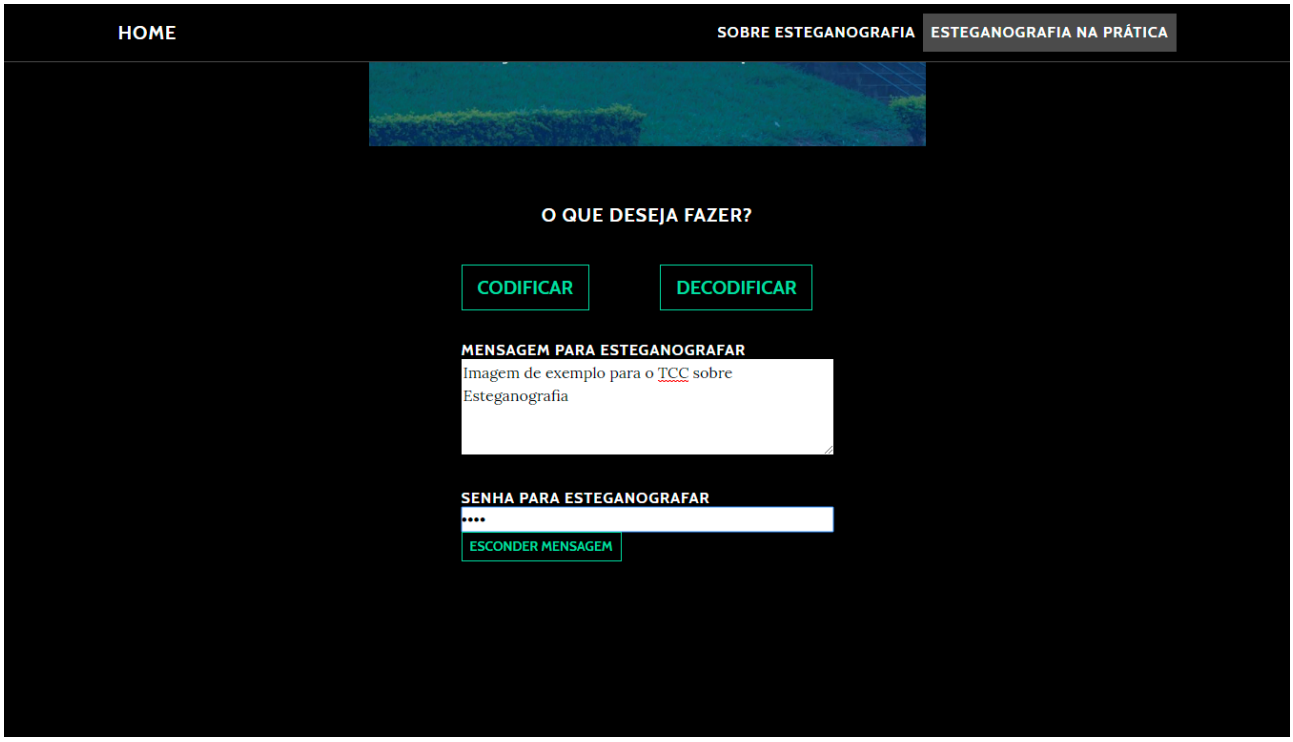

Figura 23: Exemplo de mensagem para inserção.

Fonte: elaborado pelo autor.

Ao clicar no botão “Esconder Mensagem” um alerta na página HTML será exibido com a mensagem “Mensagem Esteganografada! Faça o download da imagem que aparecer”, informando ao usuário que sua mensagem foi inserida com sucesso, como pode ser visto na Figura 24. Caso a mensagem inserida ultrapasse a quantidade de caracteres possíveis para inserir dentro da imagem enviada (cálculo realizado pela biblioteca PixelJihad, onde pega a quantidade de pixel na vertical, múltipla pela horizontal, e múltipla novamente pela quantidade de canais na imagem, RGBA, obtendo a quantidade máxima de caracteres disponíveis para aquela imagem), será exibido uma mensagem como visto na Figura 25.

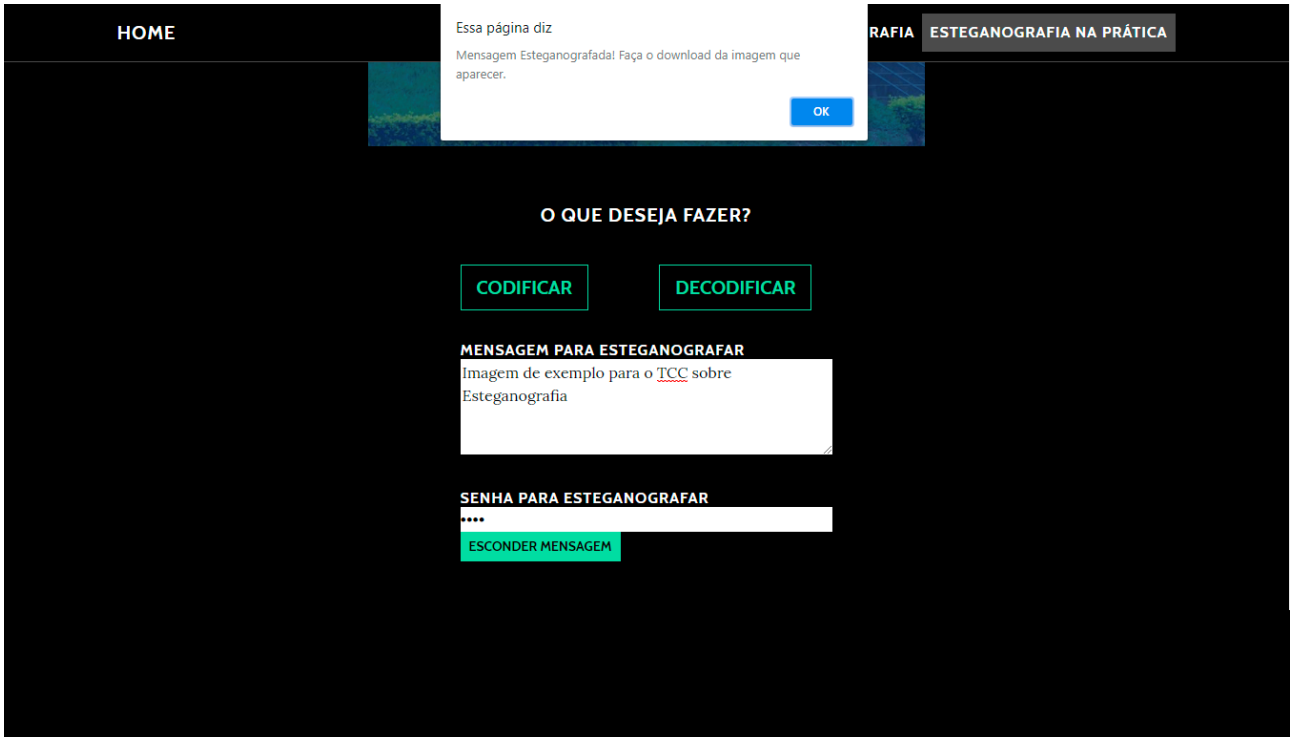

Figura 24: Mensagem de sucesso ao esteganografar.

Fonte: elaborado pelo autor.

Figura 25: Mensagem muito longa para a imagem enviada.

Fonte: elaborado pelo autor.

Ao concluir a esteganografia, uma nova imagem será exibida na parte inferior do site, embaixo de onde inserimos a mensagem e a senha, sendo a nova imagem, já possuindo a mensagem Esteganografada dentro dela, sem nenhuma modificação aparente, sendo imperceptível a quem analise a imagem, estando modificada a nível binária, e criptografa com a senha fornecida pelo usuário, como pode ser visto na Figura 26.

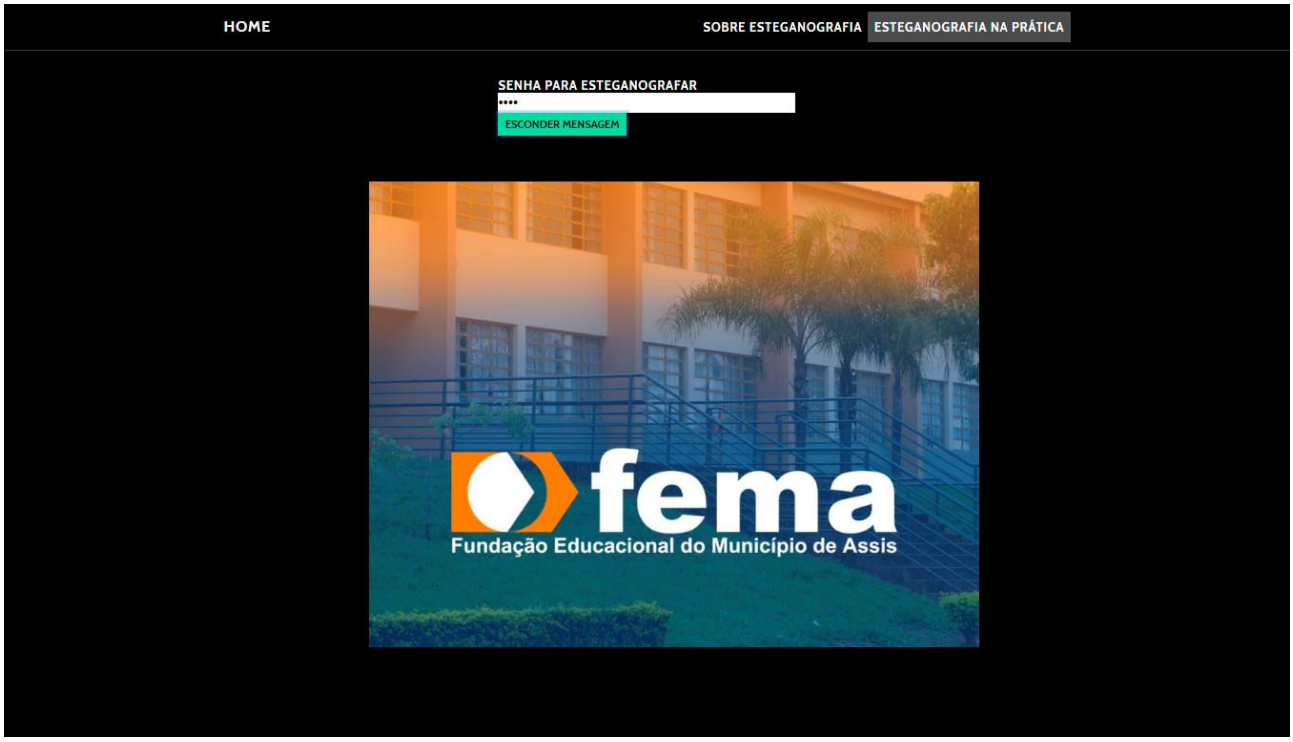

Figura 26: Imagem esteganografada.

Fonte: elaborado pelo autor.

4.5. REALIZANDO A LEITURA DA MENSAGEM

Para ocorrer a leitura de uma imagem e aplicação web verificar e analisar se há alguma mensagem esteganografada nela, e necessário outros passos. Após o carregamento da imagem esteganografada no mesmo local anterior, em “Escolher arquivo”, como pode ser visto na Figura 27, após ser enviado o arquivo, será aberto novamente as opções, porém agora a escolha deverá ser o botão que estará escrito “Decodificar” como na Figura 28.

Figura 27: Escolher imagem para a leitura da esteganografia.

Fonte: elaborado pelo autor.

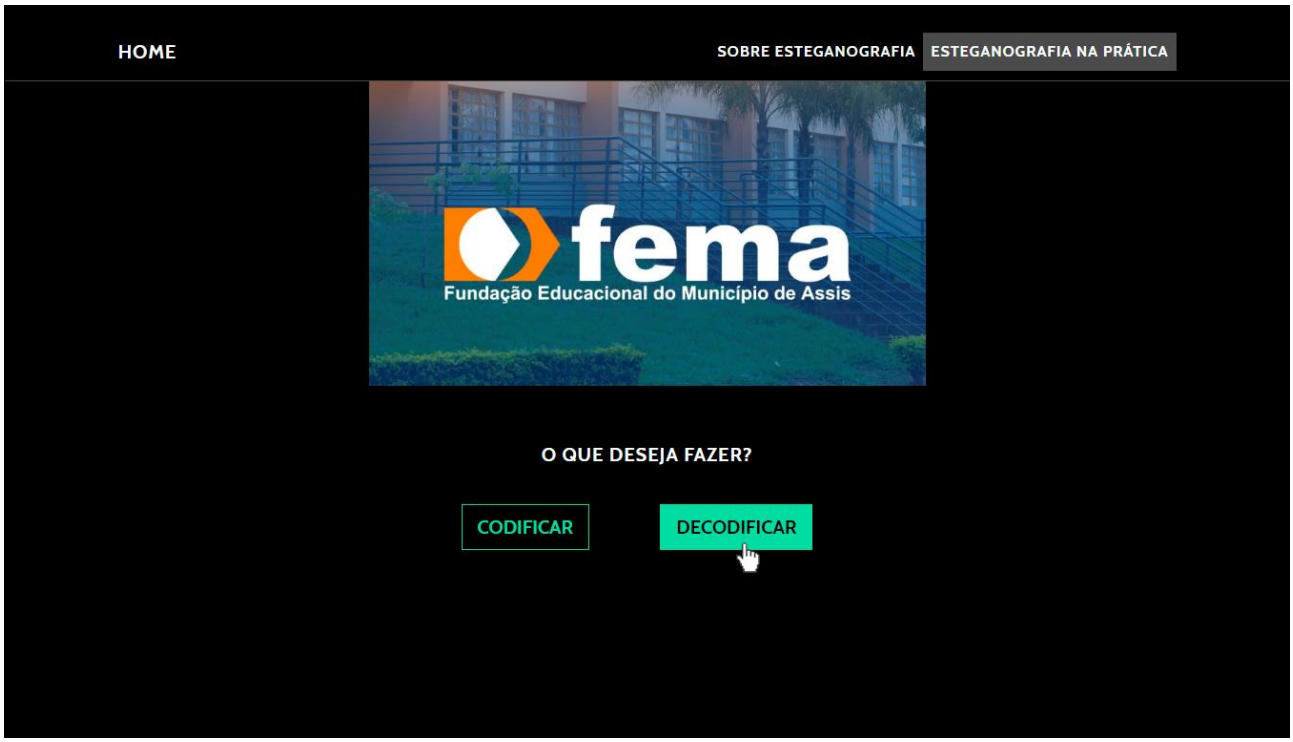

Figura 28: Botão decodificar para realizar a leitura de uma mensagem.

Fonte: elaborado pelo autor.

Após a seleção do botão “Decodificar” será aberto a opção de inserção da senha que foi adicionada quando a esteganografia estava sendo realizada, como podemos ver na Figura 29, esta senha serve para poder localizar onde está a esteganografia dentro da imagem, e poder realizar a remoção da criptografia adicionada, para exibir a mensagem na aplicação.

Figura 29: Área para inserção da senha liberada.

Fonte: elaborado pelo autor.

Após a inserção da senha que foi pedida, que no caso do exemplo foi utilizada a senha “FEMA”, então por último passo deverá ser clicado no botão “Revelar Mensagem” como pode ser visto na Figura 30, para que a aplicação web possa procurar a mensagem inserida dentro da imagem carregada e possa realizar todos os passos necessários para a extração desta mensagem e a exibição na tela, como está demonstrado na Figura 31, a exibição da mensagem.

Figura 30: Senha inserida para a remoção da esteganografia.

Fonte: elaborado pelo autor.

Figura 31: Mensagem revelada após a inserção da senha.

Fonte: elaborado pelo autor.

Caso a imagem enviada para a aplicação, não possua nenhuma mensagem inserida através dessa técnica apresentada neste trabalho, ou tenha sido corrompida durante a inserção da mensagem, ou até caso a senha inserida para a verificação da mensagem esteja incorreta, faltando algo ou inserida incorretamente, um alerta será apresentado na tela do usuário, mas não identificando se está errada a mensagem ou não, apenas informado que pode estar incorreta, ou que não há nenhuma mensagem inserida dentro daquela imagem enviada, como pode ser visto na Figura 32.

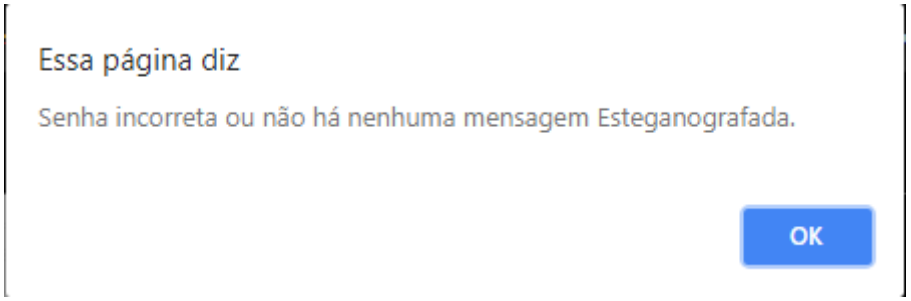

Figura 32: Alerta sobre Senha Incorreta ou nenhuma mensagem Inserida.
Fonte: elaborado pelo autor.

4.6. LIMITAÇÃO DO USO DA APLICAÇÃO

Por ser uma aplicação web que necessita apenas do navegador para estar funcionando, sem a necessidade de um acesso à internet, ou um servidor para realizar o tratamento e um acesso a uma aplicação com um servidor mais potente que o navegador apresentado, a aplicação possui uma limitação de caracteres a serem inseridos dentro da mensagem para que possa funcionar. Caso ultrapasse essa limitação, a aplicação estará travando o navegador e então será necessário o reinício do mesmo, como pode ser visto na Figura 33.

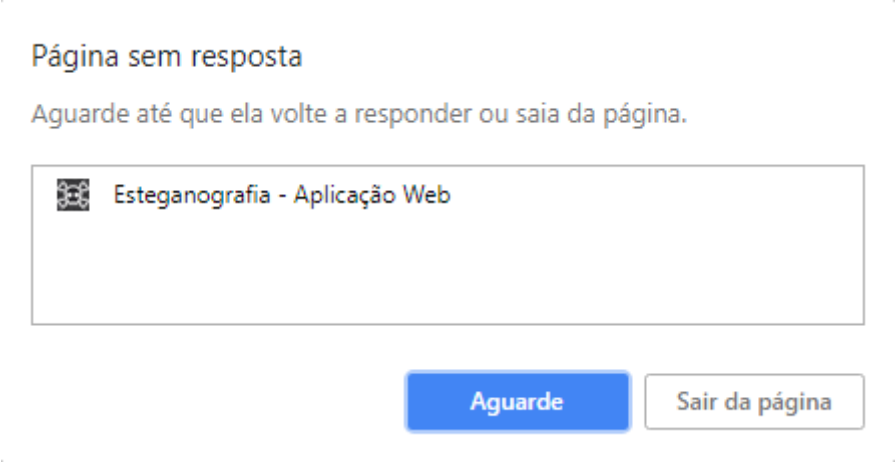

Figura 33: Alerta sobre a aplicação travada.

Fonte: elaborado pelo autor.

Atualmente a aplicação se encontra travada em um uso de 10000 (dez mil) caracteres, que podem ser inseridos dentro da *TextArea* encontrada na página HTML sem nenhum risco de travamento da página, apenas uma lentidão enquanto processa e insere a mensagem, porém, a mensagem a ser inserida dentro da imagem, sobe para um total de 13478 caracteres, como pode ser visto na Figura 34, por estar sendo criptografada coma tecnologia SHA256 apresentada anteriormente, tornando a mensagem segura e apenas podendo ser lida mediante a inserção da senha na qual o usuário informou previamente.

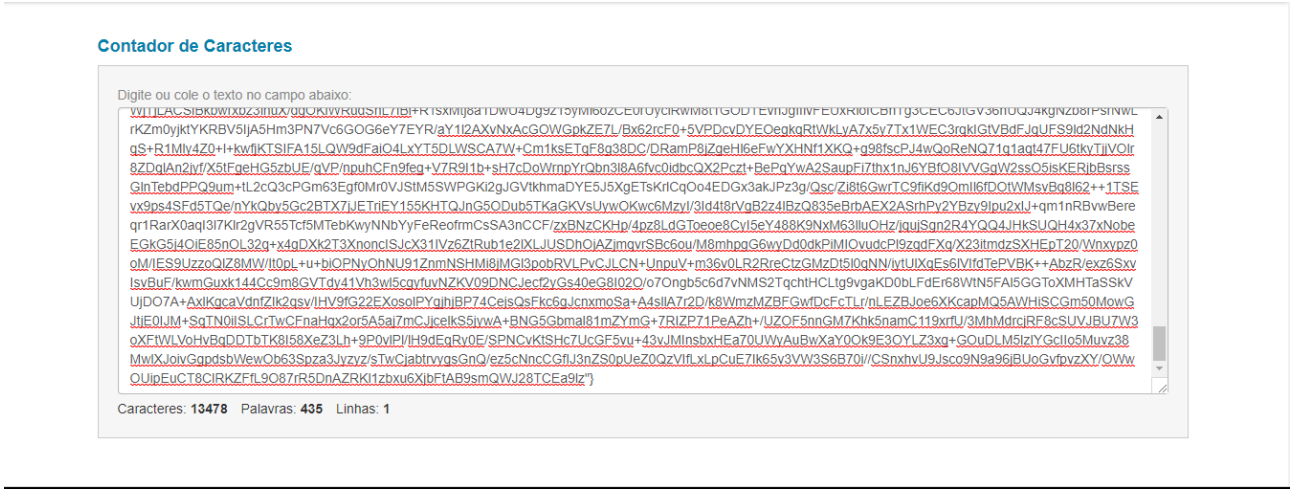

Figura 34: Quantidade de caracteres em uma mensagem.

Fonte: elaborado pelo autor.

5. CONCLUSÃO

Atualmente a Esteganografia não está muito bem difundida entre os usuários da área de computação por não ser um assunto muito discutindo e de fácil acesso, não possuindo muitas aplicações práticas e sim mais específicas, por esse motivo, não atrai a atenção nem o interesse dos usuários, porém ela é muito mais do que apenas esconder uma simples mensagem em uma imagem, e muito mais complexa para se aplicar do que se pode imaginar.

Com o decorrer deste trabalho, pode-se aprender a que nível é necessário chegar na computação para realizar a técnica de Esteganografia para ocultar uma mensagem em uma imagem, tendo a necessidade de chegar a níveis binários, desmantelando um arquivo a ponto de se dividir pixel a pixel, até chegar em seu nível binário e poder “enxergar”, entre 0 e 1 para se realizar a modificação destes dados, juntamente com uma criptografia reforçada para tornar ainda mais impossível a identificação, e muito mais segurança a informação desejada ali a se guardar.

Na aplicação web apresentada, foi encontrada uma limitação de caracteres possíveis a se inserir antes que a própria aplicação, que necessita apenas do navegador, venha a travar e então exigir a necessidade de se reiniciar o navegador. Esta limitação ocorre por não haver nenhum meio de tratamento, um servidor, ou uma aplicação mais potente, exigindo apenas os recursos de um navegador.

Por fim, a aplicação web se encontra em pleno funcionamento, com todas as suas funções sem nenhum erro encontrado. Em todos os testes realizados obtiveram sua resposta as mensagens inseridas funcionando, e retornando a exatidão de caracteres inseridos, sem nenhuma restrição de caractere. Podendo ser utilizada com a limitação de 10000 caracteres em pleno funcionamento, para uso livre e sem o perigo de identificação e de perda de dados.

6. REFERENCIAS

COUTINHO, P.S**. ESTEGANOGRAFIA – TÉCNICAS MODERNAS** (2008). Disponível em <https://www.gta.ufrj.br/grad/08_1/estegano/TcnicasModernas.html>. Acesso em 17/03/2018.

CLAIR, Brian. **Steganography: How to send a secret message** (2001). Disponível em < http://strangehorizons.com/non-fiction/articles/steganography-how-to-send-a-secret-message/>. Acesso em 09/08/2018.

FONSECA, T.C. **Esteganografia** (2007). Disponível em <

http://www.gta.ufrj.br/grad/07_2/thiago_castello/index.html> Acesso em 09/08/2018.

FREITAS, A. R. **Perícia Forense Aplicada à Informática**. Rio de Janeiro: Ed Brasport, 2006.

GIL, Fernando O.; MALANDRIN, Leandro José A. A.; MORIGAKI, Roberto. H.; BARRETO, Paulo. S. L. M. **SEA – Sistema Esteganográfico de Arquivos. Anais do VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, Gramado, p. 401-410, 2008. Disponível em <http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_04_wticg.pdf>. Acesso dia 28/07/2018.

KESSLER, Gary C. **Steganography: Hiding Data Within Data** (2001). Disponível em < https://www.garykessler.net/library/steganography.html>. Acesso em 09/08/2018.

MALAGUTTI, Pedro Luiz. **Atividades de Contagem a partir da Criptografia.** Disponível em <http://server65.obmep.org.br/docs/apostila10.pdf>. Acesso em 29/07/2018.

OAKES, Zach. **STEGANOGRAPHY IN JAVASCRIPT** (2012). Disponível em <https://sekao.net/pixeljihad/about.html>. Acesso em 18/03/2018.

PINHEIRO, José Mauricio Santos. **Esteganografia Digital.** Disponível em < http://www.projetoderedes.com.br/artigos/artigo_esteganografia_digital.php>. Acesso em 30/10/2017.

STARK, Emily; HAMBURG, Michael; BONEH, Dan. **Symmetric Cryptography in Javascript,** Stanford University, CA. Disponível em <https://crypto.stanford.edu/sjcl/acsac.pdf>. Acesso em 28/07/2018.

TECHNOLOGY, COURSE. **Investigating Data & Image Files**. Disponível em < http://ebook.eqbal.ac.ir/Security/Forensics/Computer%20Forensics,%20Investigating%20Data%20and%20Image%20Files.pdf >. Acesso em 30/10/2017.

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