CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

Faculdade de Tecnologia de Jundiaí – "Deputado Ary Fossen"

Curso Superior de Tecnologia em Gestão da Tecnologia da Informação

RICHARD MARTINS BASTOS

SILAS RAFAEL S FERREIRA

PERICIA FORENSE – A UTILIZAÇÃO DA ESTEGANOGRAFIA EM MIDIAS DIGITAIS NO CRIME ORGANIZADO

Jundiaí
2021
RICHARD MARTINS BASTOS
SILAS RAFAEL S FERREIRA

PERICIA FORENSE – A UTILIZAÇÃO DA ESTEGANOGRAFIA EM MIDIAS DIGITAIS NO CRIME ORGANIZADO

Trabalho de Graduação apresentado à Faculdade de Tecnologia de Jundiaí - “Deputado Ary Fossen” como requisito parcial para a obtenção do título de Tecnólogo em Gestão da Tecnologia da

Informação, sob a orientação do Professor Mestre Rafael Gross

Fatec Jundiaí — Centro Paula Souza

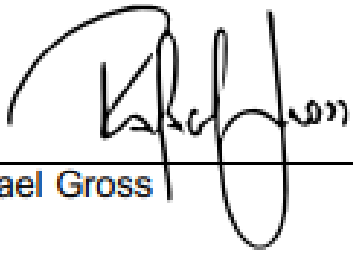
Faculdade de Tecnologia de Jundiaí - "Deputado Ary Fossen"

TCC-T1 - TERMO DE ACEITE DO PROFESSOR ORIENTADOR

Eu, Mestre Rafael Gross, docente do Curso de Gestão da Tecnologia da Informação da Faculdade de Tecnologia de Jundiaí - "Deputado Ary Fossen", declaro para os devidos fins que aceito a orientação do Trabalho de Conclusão de Curso que tem por tema principal: Esteganografia e que será elaborado pelo(s) estudante(s), nomeado(s) a seguir.

Nome Completo	**RA**
Richard Martins Bastos	1140781823034
Silas Rafael Silva Ferreira	1140781823037

Jundiaí, 28 de Agosto de 2020



Me. Rafael Gross

CopySpider Scholar | Apoiar o CopySpider

Exportar relatório | Exportar relatório PDF | Visualizar | Gerador de Referência Bibliográfica (ABNT, Vancouver)

TCC.docx (28/05/2021):

Documentos candidatos

fatecjd.edu.br/intra... [1,73%]

fatecjd.edu.br/intra... [1,17%]

fatecjd.edu.br/moodl... [0,53%]

sans.org/reading-roo... [0,23%]

profs.sci.univr.it/~... [0,22%]

ijarcsse.com/Before_... [0,17%]

en.wikipedia.org/wik... [0,07%]

datahide.org/BPCSe/a... [0,00%]

cps.sp.gov.br [0,00%]

tecmundo.com.br/crip... [0,00%]

Arquivo de entrada: TCC.docx (2629 termos)

Arquivo encontrado	Total de termos	Termos comuns	Similaridade (%)	
fatecjd.edu.br/intranetAlunos/wp-content...	1352	68	1,73	Visualizar
fatecjd.edu.br/intranetAlunos/wp-content...	4419	82	1,17	Visualizar
fatecjd.edu.br/moodle	352	16	0,53	Visualizar
sans.org/reading-room/whitepapers/stenga...	6868	22	0,23	Visualizar
profs.sci.univr.it/~giaco/download/Water...	6836	21	0,22	Visualizar
ijarcsse.com/Before_August_2017/docs/pap...	2654	9	0,17	Visualizar
en.wikipedia.org/wiki/Steganography	6521	7	0,07	Visualizar
datahide.org/BPCSe/applications-e.html	1370	0	0,00	Visualizar
cps.sp.gov.br	402	0	0,00	Visualizar
tecmundo.com.br/criptografia/22938-como-...	164	0	0,00	Visualizar

Dedico este trabalho aos
meus familiares por ter
adiado a realização de
muitos de seus sonhos,
em benefício da realização
dos meus.

AGRADECIMENTOS

Todo trabalho, por mais simples que seja, não é elaborado sem o auxílio de outras pessoas. Durante o desenvolvimento desta pesquisa tivemos muita ajuda. Desta forma, gostaríamos de agradecer aos meus familiares pelo apoio nesta jornada, mesmo com as dificuldades ocasionadas pela pandemia, e sem eles não teríamos conseguidos ter finalizados.

“Gênio não é aquele que enxerga o óbvio, como disse o filósofo. É quem percebe a incerteza perdida nos consensos.
Uma simples folha torta com a qual ele explique toda a floresta.”
Stefan Schweitzer

BASTOS , Richard Martins e FERREIRA, Silas Rafael S. (**Pericia forense – A utilização da esteganografia em mídias digitais no crime organizado**). XX f. (XX: número de páginas) Trabalho de Conclusão de Curso de Tecnólogo em Gestão em Tecnologia da Informação. Faculdade de Tecnologia de Jundiaí - “Deputado Ary Fossen”. Centro Estadual de Educação Tecnológica Paula Souza. Jundiaí. 2021.

RESUMO

Esteganografia deriva do grego *steganographia*, onde stegano significa esconder, mascarar e graphia significa escrita. Logo, esteganografia é a arte da escrita oculta. Durante toda a história, as pessoas buscam inúmeras formas de ocultar informações dentro de outros meios, para, de alguma forma, obter mais privacidade para seus meios de comunicação. Na antiguidade, as mensagens eram passadas escritas no couro cabeludo de um escravo fiel, raspando a cabeça e tatuando a mensagem, aguardava o cabelo crescer novamente e assim enviando o escravo com a mensagem. Com o passar dos anos, novas formas foram de ocultar mensagens, para fins de direitos autorais, maior privacidade, ou compartilhamento de arquivos e documentos ilícitos. Utilizando a esteganografia, junto a criptografia, conseguimos mascarar e ocultar textos e imagens escondidos em diversos arquivos digitais, podendo conter arquivos que irão passar desapercebidas para a maioria das pessoas e o crime organizado está aproveitando da dificuldade em identificar esses arquivos.

Palavras-chave: Esteganografia; Criptografia; Mídias digitais; Terrorismo; Crime Organizado.

Bastos, Richard Martins e Ferreira, Silas Rafael S. (**Digital forensics – The use of steganography in digital media in organized crime**). XX p. End-of-course paper in Technologist Degree in Technologist in Information Technology Management. Faculdade de Tecnologia de Jundiaí - “Deputado Ary Fossen”. Centro Estadual de Educação Tecnológica Paula Souza. Jundiaí. 2021

ABSTRACT

The word *steganography* is derived from the Greek words *steganos* (meaning *hidden* or c*overed*) and the Greek root *graph* (meaning *to write*). Therefore, it is practiced by those wishing to convey a secret message or code. Throughout the history, people searched many ways from hidden information in other media to somehow get more privacy for their media. In the past, the secret message was tattooed on the slave’s head, waited for his hair to grow back, and then send him off to destination. Over the years, new ways have been to hide messages, for purposes of copyright, greater privacy or sharing illegal files and documents. If is used Steganography and cryptography together, to conceal almost any type of digital content, including text, image and another type of social and digital media. Because of the difficulty for the most of people identifying or detect this process inside some media, the organized criminal and terrorist groups can take advantage of this technique.

Keywords: *steganography; cryptography; social media, Terrorism; organized crime;*

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A elaboração e estudo deste projeto, tem como foco os conceitos e exemplos de Esteganografia em utilização no crime organizado, buscando conscientizar sobre um dos métodos utilizados para a comunicação das organizações criminosas, de forma oculta, passando desapercebido pela sociedade.

A incrível expansão de sistemas multimidias interligadas nas redes de computadores nos últimos anos, tem se tornando um enorme desafio nos aspectos de propriedade, direito autoral, integridade e autenticação de dados digitais. O crescimento de técnicas inovadoras para a proteção das informações aumenta na proporção da crescente disponibilidade de sistemas de comunicação, estes cada vez mais sofisticados.

Um dos métodos mais utilizados e eficientes para a transferência de informações, sem que haja a possibilidade de comprometimento da privacidade, é através da codificação das informações, conhecida como criptografia.

A implementação da esteganografia junto a criptografia potencializa sua segurança, dificultando a identificação, transformando o trabalho do perito em um grande desafio.

A criptografia estuda os princípios, meios e métodos de assegurar a integridade e confidencialidade das informações através da codificação ou cifração e que permite a recuperação da informação através de um processo de decifração. Esta ciência utiliza-se de algoritmos matemáticos e criptoanálise para conferir o nível de complexidade da criptografia.

Outro método utilizado, a esteganografia, é uma antiga técnica utilizada para introduzir mensagens secretas em mensagens aparentemente inocentes, a qual visa dificultar a detecção por parte de terceiros.

A esteganografia inclui uma ampla disponibilidade de técnicas para ocultar mensagens, podendo ser combinado com a criptografia. Entre esses métodos estão tintas invisíveis, micropontos, assinaturas digitais, canais escondidos e comunicação de espectro espelhado.

Atualmente, graças ao avanço da tecnologia, a esteganografia pode ser utilizada em textos, sons, sinais, imagens, vídeos e outros.

O objetivo desse trabalho é instruir métodos para identificar arquivos que possivelmente sofreram alterações através das técnicas de esteganografia em conjunto com métodos de criptografia. Mostrando técnicas e softwares utilizados para esteganografia e análise de Esteganografia.

Os objetivos específicos do trabalho são:

a) Esconder um arquivo de imagem comprimindo em um arquivo de áudio utilizando o site https://rxrichard.github.io/spectrum/
b) Visualizar a imagem utilizando análise de espectrograma com o software Sonic Visualizer
c) Adicionar um arquivo de texto dentro do arquivo de áudio utilizando o software OpenPuff, utilizando 2 camadas de segurança, adicionando um arquivo falso e outro verdadeiro
d) Descriptografar e descompactar o texto original, e o arquivo falso

2 REFERENCIAL TEORICO

Para embasar a proposta deste artigo faz-se um levantamento teórico de aspectos relevantes sobre o tema, os quais são descritos nesta seção, começando pela explicação básica de perícia forense digital e esteganografia

2.1 PERÍCIA FORENSE DIGITAL

Perícia forense digital é a área que tem como especialização na investigação e restauração de informações encontradas em vários dispositivos digitais, esta ligada principalmente a crimes relacionados na área de informática. Tem como base o uso de métodos para fazer a identificação, coleta, preservação, análise, interpretação, documentação e apresentação de provas que são validas perante a lei.

Aplicabilidade dos métodos nem sempre acorre de forma metódica e simples, porque as vezes para encontrar ou rastrear evidências no meio digital pode sem um processo muito difícil. Com a tecnologia atual sempre evoluindo e a capacidade de armazenamento dos meios digitais vem aumentando, a quantidade de arquivos para serem armazenados acaba aumentando. Com isso em mente temos que usar métodos e técnicas de Computação Forense para que possamos encontrar as provas para que os crimes tenham uma solução ou condenar um criminoso.

2.2 ESTEGANOGRAFIA

Esteganografia é o estudo que usa técnicas de forma para ocultar mensagens dentro de outras mensagens, de forma segura.

Esteganografia é uma parte particular da criptologia que tem como objetivo que é uma mensagem escondida(camuflada) em outra mensagem com a finalidade de disfarçar a sua verdadeira intenção. É importante lembrar que tem diferença entre

criptografia e esteganografia. Criptografia oculta a mensagem enquanto esteganografia oculta a existência da mensagem.

Um bom exemplo de uma técnica moderna de esteganografia é a alteração do bit menos significativo de cada pixel de uma imagem colorida para que ele corresponder a um bit da mensagem. Esta técnica, não é ideal de se fazer, porém afeta bem pouco a imagem.

Analisando os fatores envolvidos no reconhecimento de um estego-arquivo dificulta bastante a análise da perícia, visto que a as organizações criminosas utilizam esta técnica para envio de dados.

Atualmente existem softwares especializados para o auxílio na identificação de arquivos com esteganografia, porém com alto valor de investimento, o modo mais seguro para identificação é através de identificação por hash, onde através de uma sequencia numérica única, baseada no arquivo original conseguimos identificar se houve alguma alteração no arquivo, sendo o único inconveniente sendo necessitar do arquivo original para comparação com o arquivo suspeito.

3 ESTEGANÁLISE

A esteganálise é a forma de identificar a mensagem oculta podendo destruir, alterar ou ser decodificada.

Segundo Coelho (2004, apud Johnson, 1998, p.13), “a esteganálise visa descobrir e tornar inúteis mensagens secretas ocultas em um recipiente”. Coelho (2004, apud Kurak, 1992, p.13), também completa que “ao utilizar a esteganografia, a qualidade do objeto é degradada e tal degradação pode ser perceptível aos sentidos dos seres humanos e demonstra certas características semelhantes, o que torna possível padronizar uma espécie de assinatura, permitindo a detecção dos métodos e dos softwares utilizados”.

A esteganálise ativa, é a manipulação dos dados, de mais alto nível de complexidade, pois além de ter que ter o conhecimento sobre esteganografia, muitas vezes as mensagens esta criptografada

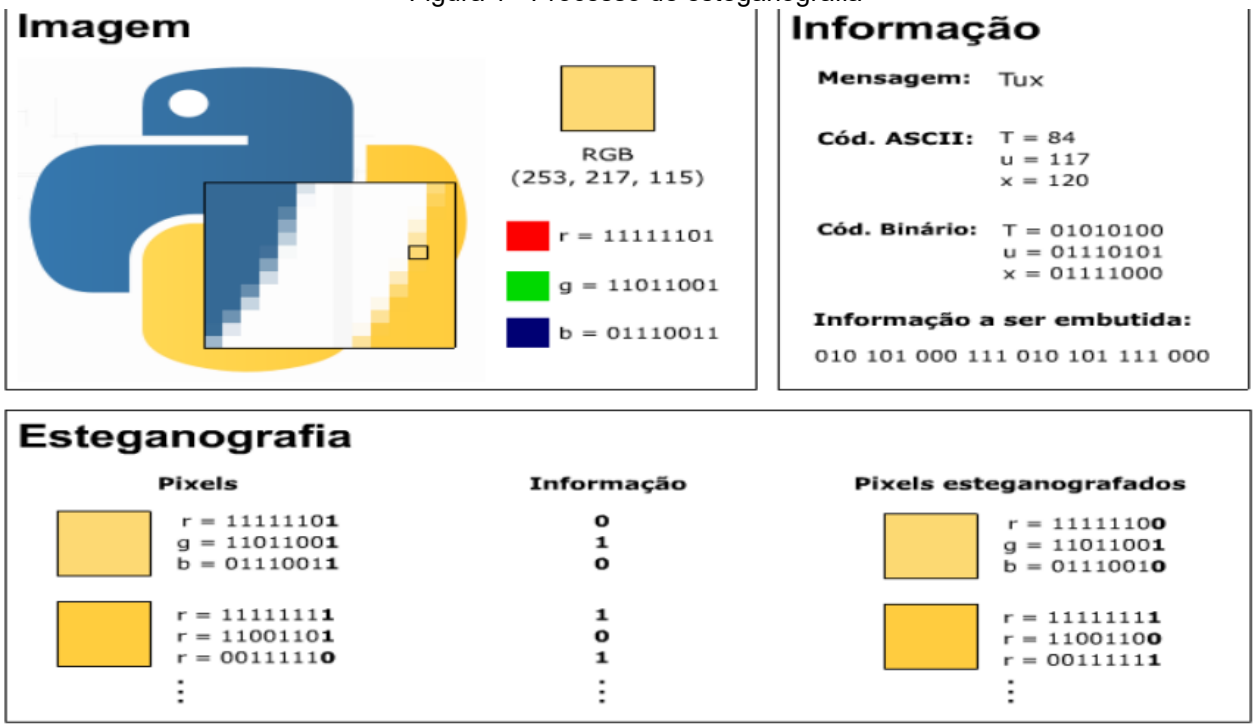
Para fazer a destruição da mensagem, existe várias formas. Umas dessas formas é comprimir o arquivo, que retira as informações extras. Também pode ser alterado o formato, que acaba dando conflito pois cada formato tem uma forma diferente de armazenar a informação.

As técnicas usadas para identificar tem três ramos principais, que são: Estruturais, Visuais (Aurais) e estatísticas.

3.1.1 VISUAIS

Ataques Aurais consistem em substituir os bits menos significativos, dificultando a identificação aos olhos humanos por alguma anomalia, substituindo os valores padrões (RGB – Red (Vermelho), Green (Verde) e Blue (Azul)

Figura 1 - Processo de esteganografia



Fonte: Rev. Cienc. Exatas Tecnol., v. 10 1

3.1.2 ESTRUTURAIS

Para explicar o método de ataque estrutural, consiste em analisar padrões estruturais, “muitas vezes ao inserir novas mensagens acaba revelando mensagens ocultas”. Um bom exemplo disso é que as vezes quando se altera a cor ou a luminosidade de uma imagem podemos descobrir mensagens que antes não davam para ver. As vezes também comprimir uma imagem e comparar a compressão com a imagem anterior, isso pode acabar revelando a mensagem oculta na imagem.

3.1.3 ESTATÍSTICAS

O método de ataque estatístico, segundo Rocha (2003, apud Wayner, 2002), “os padrões dos pixels e seus bits menos significativos freqüentemente revelam a existência de uma mensagem secreta nos perfis estatísticos”. Esta técnica

serve para analisar e determinar a probabilidade de que se exista algum arquivo escondido, baseado em que a maioria das vezes, os dados esteganografados se tornam mais aleatórios que os dados nativos.

4 TÉCNICAS DE OCULTAÇÃO DE DADOS

Quando se trata de ocultação de dados, podemos considerar inúmeras possibilidades, desde métodos físicos, com a utilização de cofres secretos, caixas enterradas, a métodos convencionais, fundo falso, cofres, senhas, cadeados. Nos últimos anos, para dificultar além de todas essas camadas, podemos utilizar sistema de esteganografia para dificultar a percepção, e caso encontrado o arquivo, não compreensão.

Com isso, nos subcapítulos abaixo, será mostrado duas técnicas que podem ser combinadas, dificultando em muito a identificação.

4.1 PROCESSO DE CODIFICAÇÃO DE IMAGEM EM AUDIO

O processo de codificação e transformação de imagem em áudio se encontra em um projeto desenvolvido em código aberto, onde será descrito de forma simples como transformar qualquer imagem em um áudio, podendo ser visualizado através de análise de espectrograma.

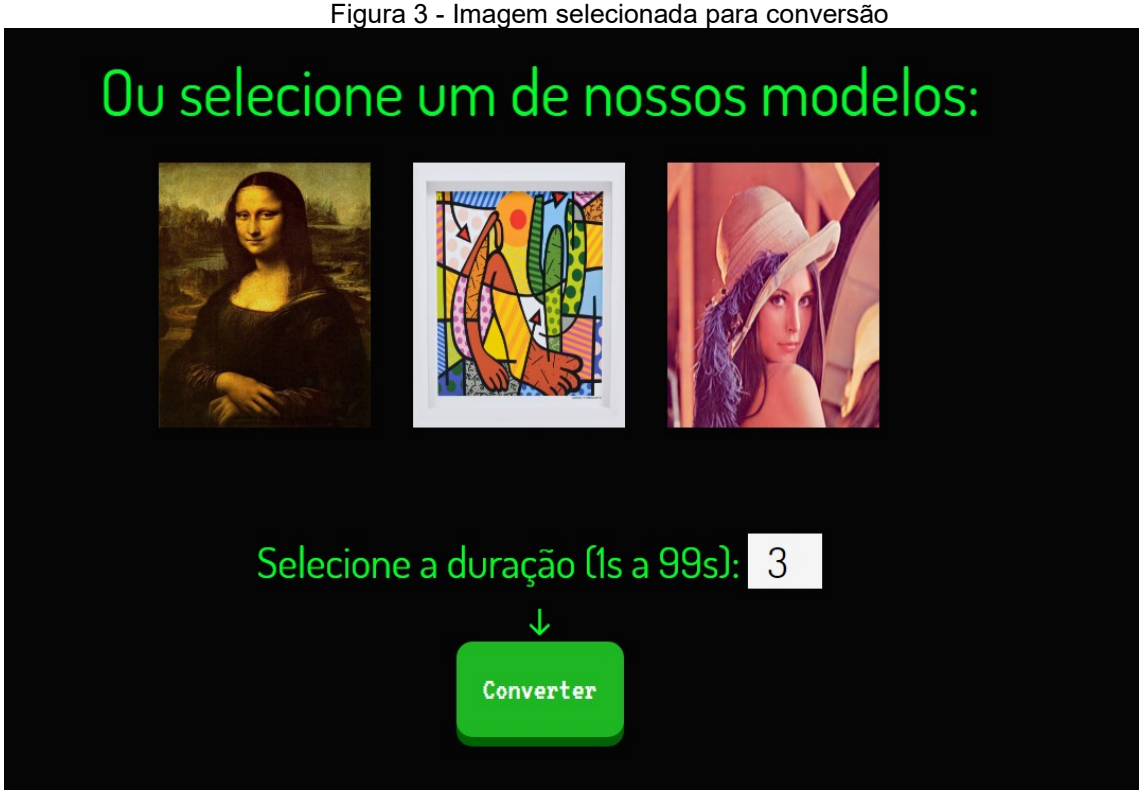
Utilizaremos para transformar a imagem em áudio o site: rxrichard.github.io/spectrum e para a análise de espectrograma iremos utilizar o software Sonic Visualiser.

Figura 2 - Pagina principal do site Spectrum

Fonte: O Autor

Após acessar o site, será necessário escolher uma imagem já disponibilizada, ou poderá selecionar a imagem que poderá ser enviada.

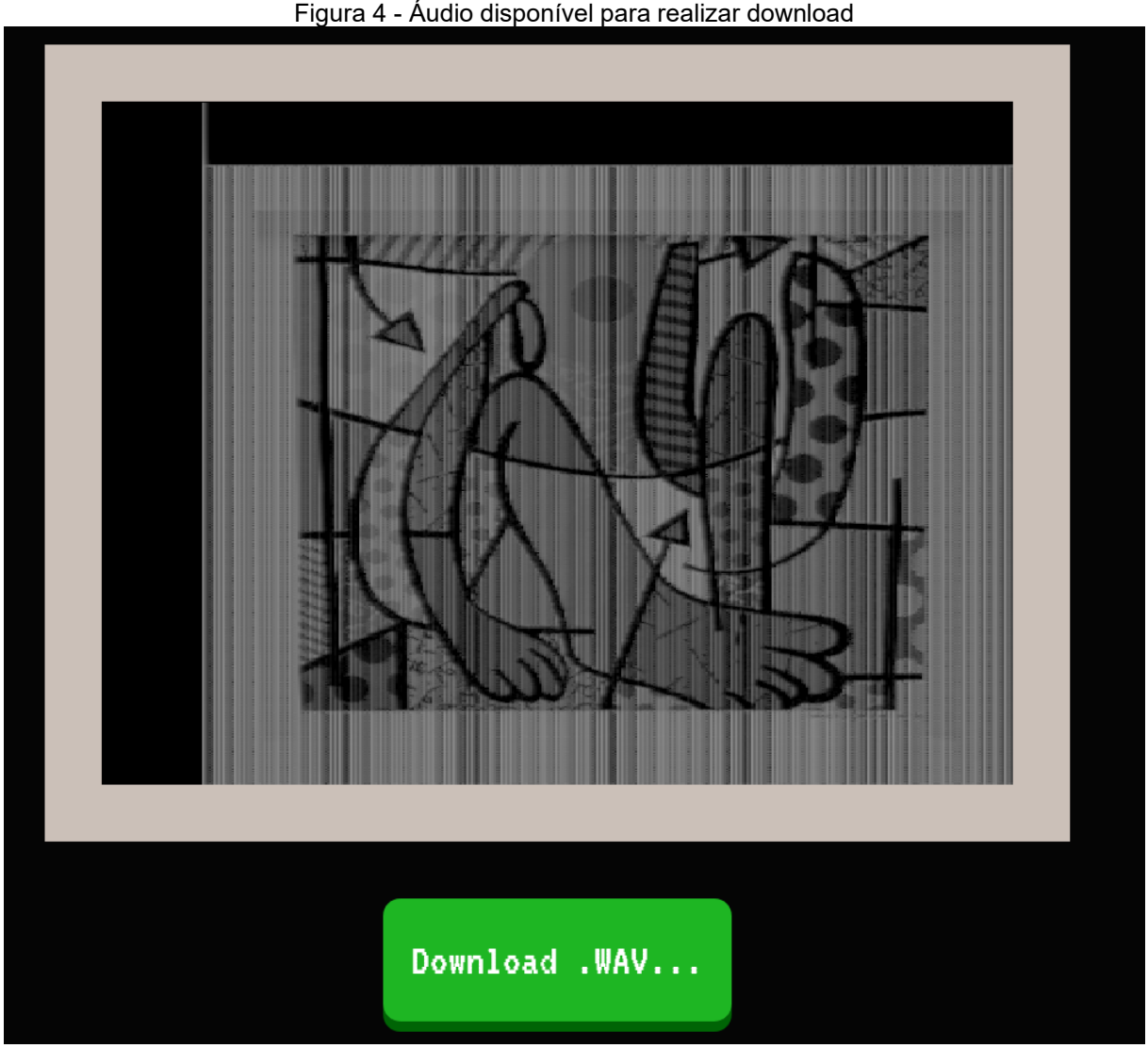
Figura 3 - Imagem selecionada para conversão



Fonte: O Autor

Após a imagem ser selecionada, irá habilitar o tempo responsável pela duração do áudio, podendo ser de 1 a 99 segundos. Após definir o tempo do áudio, deverá clicar no botão converter para iniciar o processo de transformação.

Figura 4 - Áudio disponível para realizar download



Fonte: O Autor

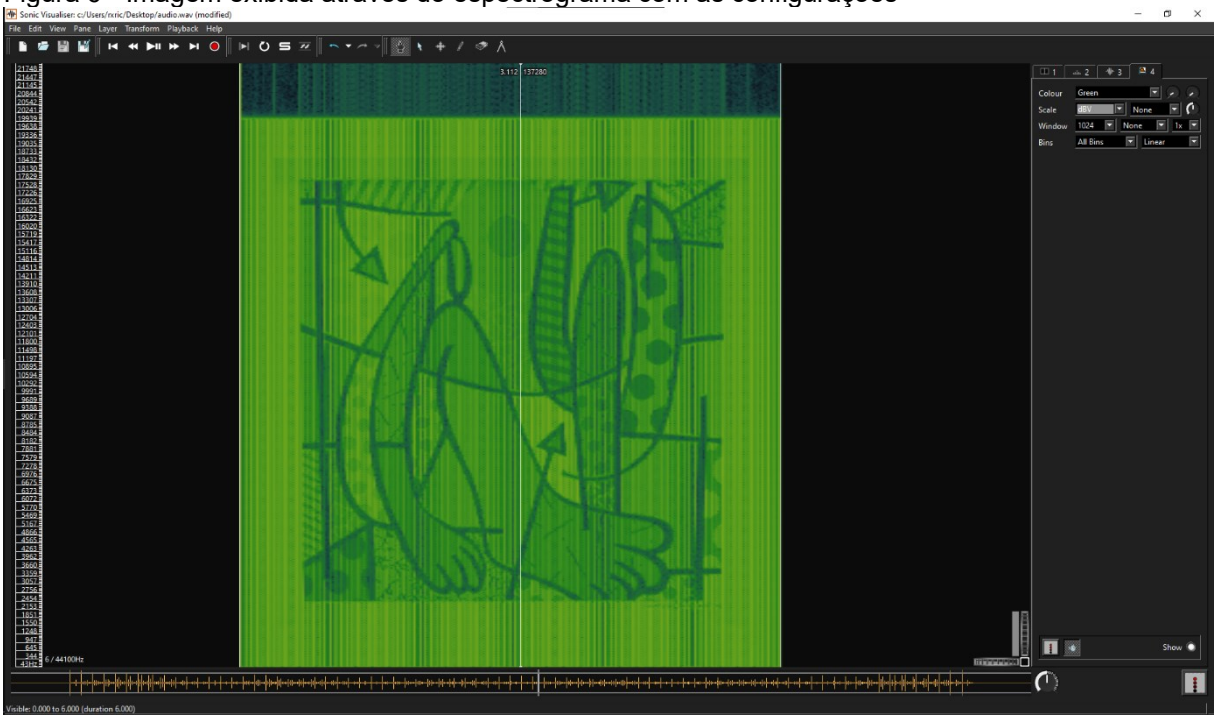
Após realizar o download do áudio, iremos abrir o software Sonic Visualiser e abrir o arquivo de áudio

Figura 5 - Tela inicial do software Sonic Visualiser

Fonte: O Autor

Para importar o áudio, irá em File => Open, ou poderemos utilizar o atalho Ctrl + O. Para podermos visualizar a imagem gerada pelo sistema, iremos acessar Layer => Add Spectogram, ou utilizar o atalho Shift+G

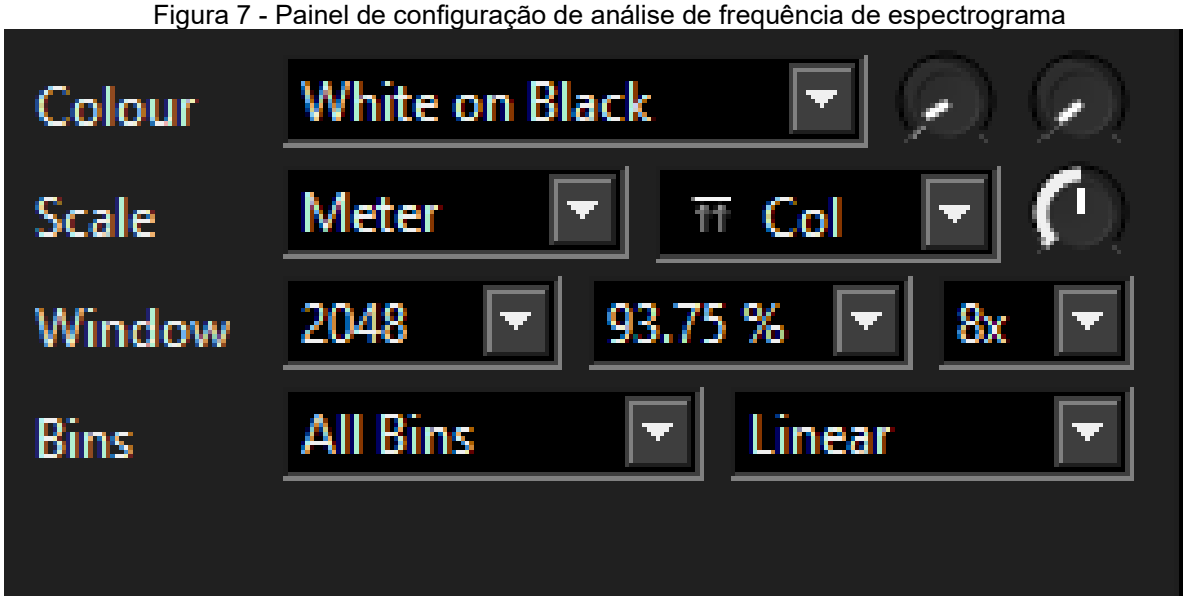
Figura 6 - Imagem exibida através do espectrograma com as configurações



Fonte: O Autor

Após a visualização do espectrograma, um campo de configuração irá ficar disponível, conforme Figura 6, onde dependendo da imagem utilizada, as configurações serão personalizadas.

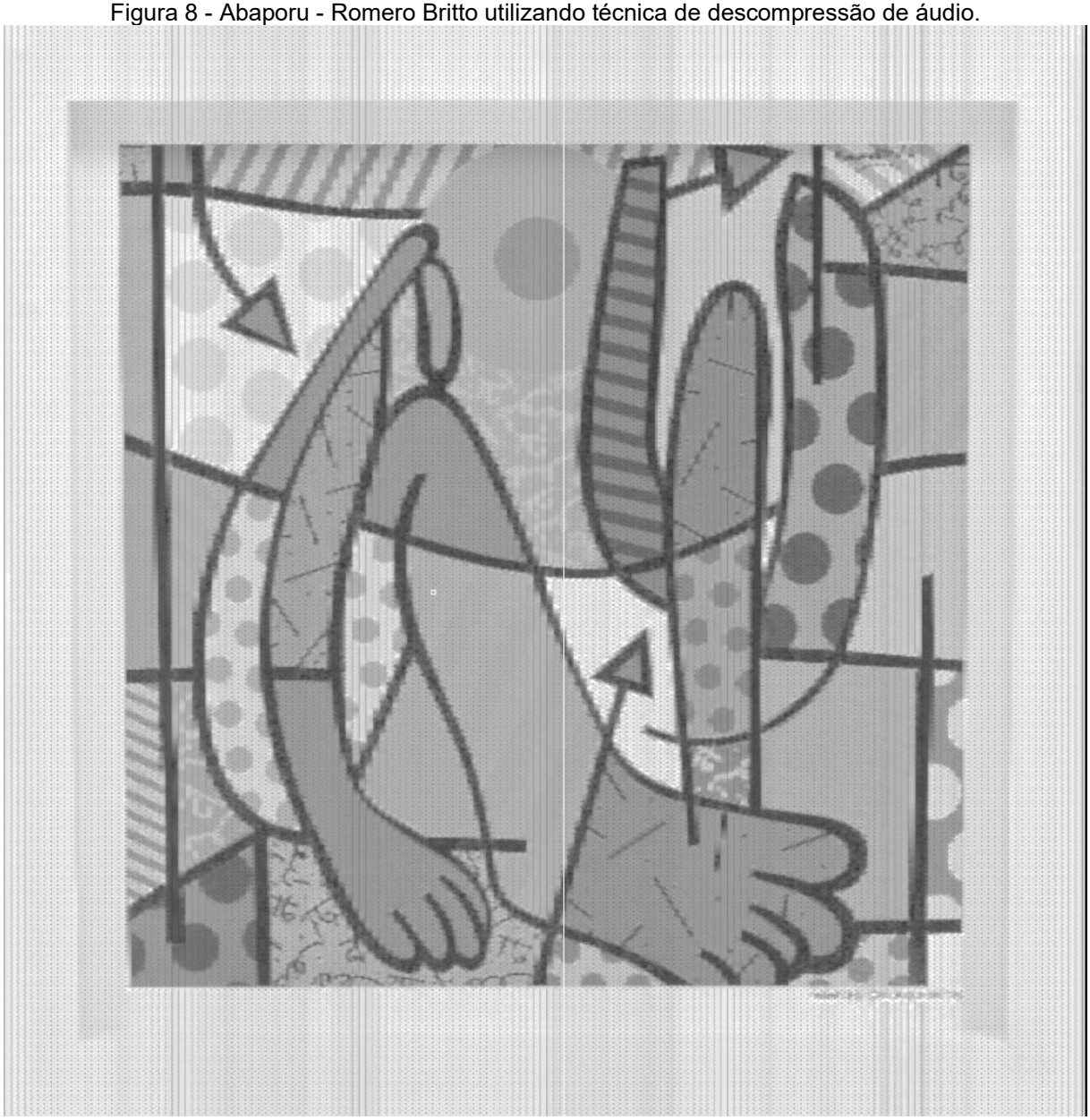
Figura 7 - Painel de configuração de análise de frequência de espectrograma



Fonte: O Autor

Utilizando a imagem disponibilizada no site, Abaporu – Romero Britto, e utilizando as configurações contidas na Figura 6, é possível conseguir o resultado da imagem abaixo:

Figura 8 - Abaporu - Romero Britto utilizando técnica de descompressão de áudio.

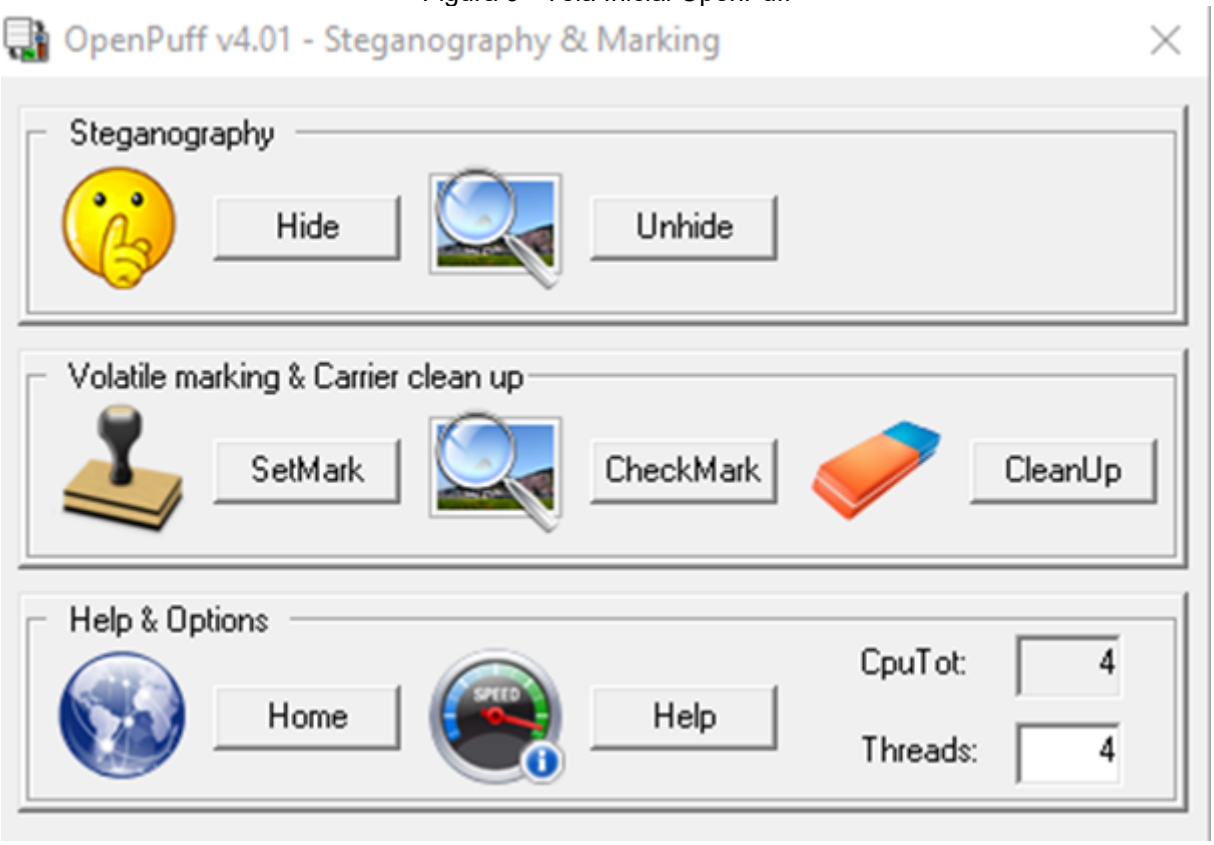


Fonte: O Autor

4.2 OCULTANDO ARQUIVOS COM ESTEGANOGRAFIA

Quando se necessita esconder arquivos, os sistemas de esteganografia serão necessários. Utilizando uma técnica de ocultação por bit menos relevante, conforme descrito no capitulo 2.2, será utilizado para este trabalho o software OpenPuff v4.01 – Steganography & Markin

Figura 9 - Tela Inicial OpenPuff

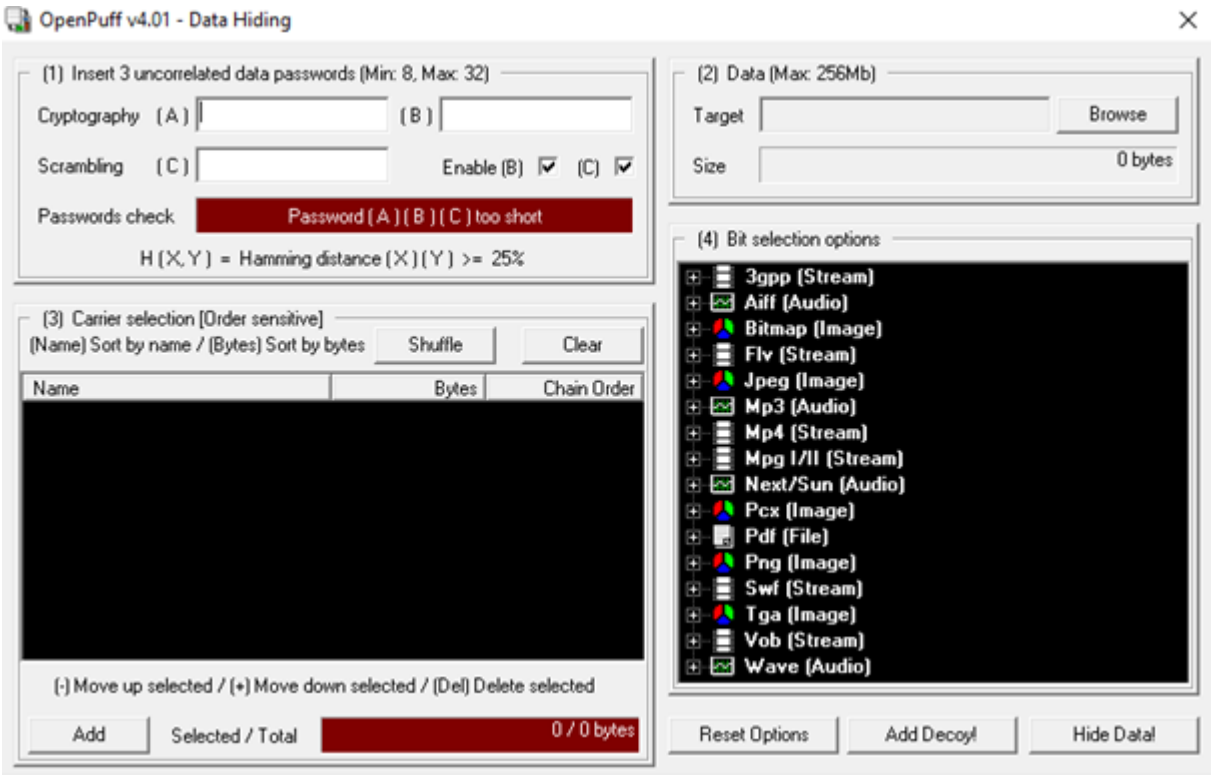


Fonte: O Autor

O software OpenPuff tem uma tela simples e intuitiva, para esteganografia temos a opção Hide(ocultar em português) e Unhide(desocultar em Portugues), para realizar a esteganografia, clique sobre a opção hide, onde irá abrir uma nova tela onde poderá ser realizada a escolha dos arquivos a serem ocultados, a criação de senhas

e de métodos de criptografia, além de quais camadas de segurança será aplicada.

Figura 10 - Tela de ocultação OpenPuff

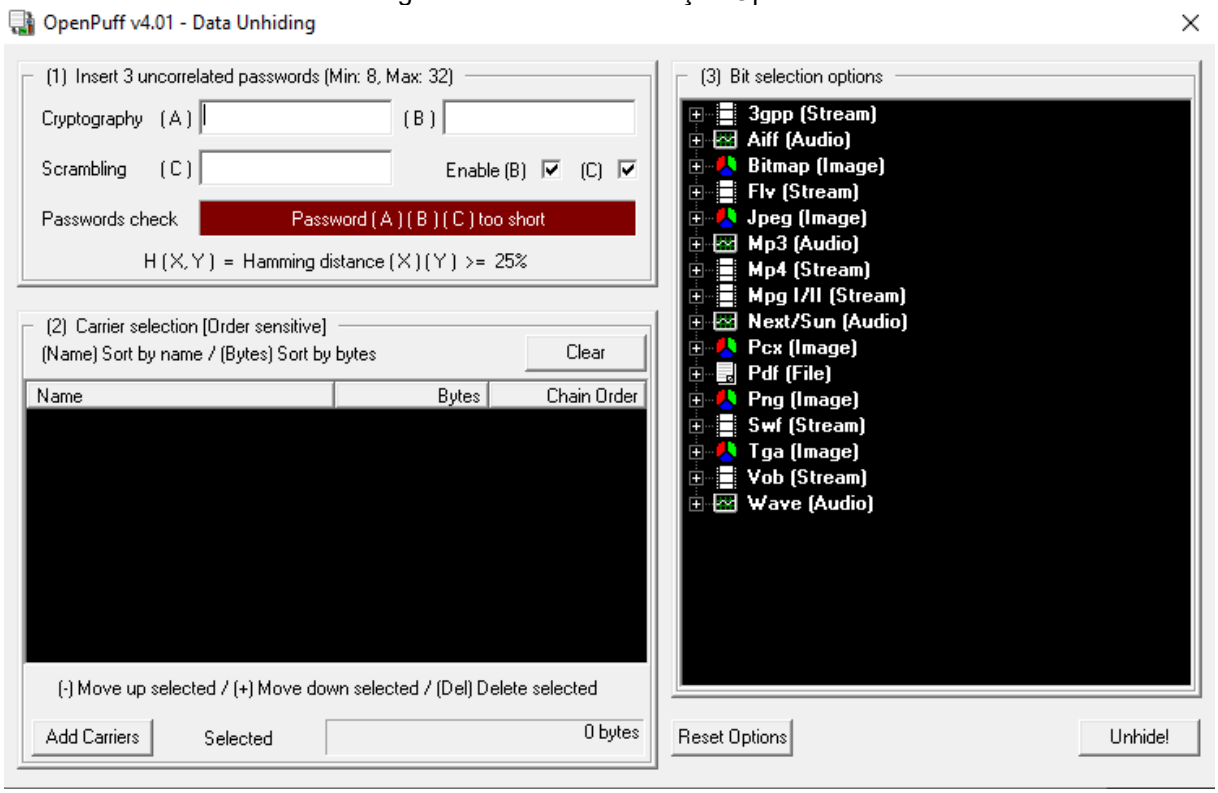


Fonte: O Autor

A configuração padrão, sugere que utilizemos três senhas, referidas como A,B e C, sendo que devem ter uma diferença de padrão entre cada uma delas.

Após definido as senhas, deve-se utilizar o campo 2 na escolha do item a ser ocultado, no campo 3, qual item será utilizado como receptáculo, no campo 4 escolhemos qual será o método de criptografia e a intensidade da compressão. Ao final das quatro etapas, clica-se no botão Hide Data para concluir a compressão dos arquivos, onde o software irá apresentar a opção do local para salvar os arquivos.

Figura 11 - Tela de revelação OpenPuff



Fonte: O Autor

Para a descompressão, na tela inicial do OpenPuff, clica-se no botão Unhide e teremos acesso a tela referente a figura 10, onde será replicado a(s) senha(s) no arquivo criptografado no campo 1, a dicionar o arquivo com esteganografia através do botão Add Carriers no campo 2 e no campo 3 será escolhido a forma de compactação e criptografia selecionada, após finalizado esse processo, clique em Unhide, caso todos os campos foram preenchidos e selecionados corretamente, será descompactado e irá revelar o arquivo oculto.

5 ESTEGANOGRAFIA NO MUNDO DO CRIME

O crime organizado, organizações terroristas e outros meios ilícitos sempre buscam meios de se comunicar e não ser percebido pelas autoridades, e buscam meios cada vez mais audaciosos de se comunicar, como quando utilizam a esteganografia, pois o arquivo pode passar desapercebido na maioria das vezes, mesmo durante uma apreensão ou perícia técnica nos meios digitais, como foi o caso de uma rede de tráfico de drogas e ordens de execução descobertas após encontrar-se mais de 200 imagens da Hello Kitty, no computador do traficante internacional Juan Carlos Ramirez Abadia, contendo informações de texto e áudio esteganografadas.

Em 2011, um homem austríaco, foi preso em Berlim, suspeito de participar da organização terrorista Al-Qaeda, a BKA(Policia Criminal Federal Alemã) encontrou junto as suas roupas intimas, um cartão de memória. Levando para a perícia forense este cartão, constatou que dentro de alguns documentos avulsos, sendo eles alguns vídeos eróticos, continham senha e criptografia. Conseguiram realizar a esteganálise e encontraram 141 documentos de texto inseridos no vídeo, utilizando-o como um arquivo camuflado, funcionando como se fosse um arquivo ZIP ou RAR.

6 CONCLUSÃO

A esteganografia é uma área de estudo inebriante, porém pode ser considerada uma faca de dois gumes, visto que, baseado no seu princípio de ocultação de informações, a sua utilização é de extrema preciosidade para fins ilícitos.

As técnicas de esteganografia existentes, apresentam uma grande fragilidade, onde uma simples compressão pode destruir grande parte da informação oculta, mas extremamente discretas quanto a segurança da informação, uma vez que devido a complexidade e o alto custo computacional para o desenvolvimento de algoritmos de esteganálise que conseguisse extrair a mensagem, quanto identificar sua existência se tornaram inviáveis.

O objetivo deste trabalho de conclusão de curso foi estudar as principais técnicas de esteganografia e suas aplicações em imagens e texto, que foram alcançados de forma satisfatória, visto que foi possível demonstrar os dois principais métodos de esteganografia.

7 BIBLIOGRAFIA

PETRI, Marcelo. Esteganografia. SOCIEDADE EDUCACIONAL DE SANTA CATARINA - SOCIESC, 2004. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_petri_esteganografia.pdf. Acesso em: 3 nov. 2020.

BAGNALL, R. J. Reversing the steganography myth in terrorist operations: The asymmetrical threat of simple intelligence dissemination techniques using common tools. The SANS Institute, 19 de agosto de 2002. Disponível em https://www.sans.org/reading-room/whitepapers/stenganography/reversing-steganography-myth-terrorist-operations-asymmetrical-threat-simple-intellig-556, Acesso em: 4 dez. 2020

HAMANN, Renan. Como a al-Qaeda escondeu documentos terroristas em vídeos pornográficos? TecMundo. 2012. Disponível em: https://www.tecmundo.com.br/criptografia/22938-como-a-al-qaeda-escondeu-documentos-terroristas-em-videos-pornograficos-.htm. Acesso em: 2 mai. 2021.

Reis, Flávio Alexandre; Quintão, Patrícia Lima. - "Esteganografia, a Arte de Ocultar", Revista Eletrônica da Faculdade Metodista Granbery - Juiz de Fora, MG, Minas Gerais, Brasil. Disponível em: http://re.granbery.edu.br/artigos/NDM0.pdf. Acesso em 3 fev 2021

PETITCOLAS, F. A. et al. Information hiding - a survey. In Proceedings of IEEE. Special issue on Protection on multimedia content, 1999.

COELHO, Laura C. M.; BENTO, Ricardo J. Ferramentas de Esteganografia e seu uso na Infowar. Evidência Digital Magazine, Rio de Janeiro, Edição-3, Ano 1, p.09-15, jul/ago/set 2004.