Universidade Federal de Pernambuco (UFPE)

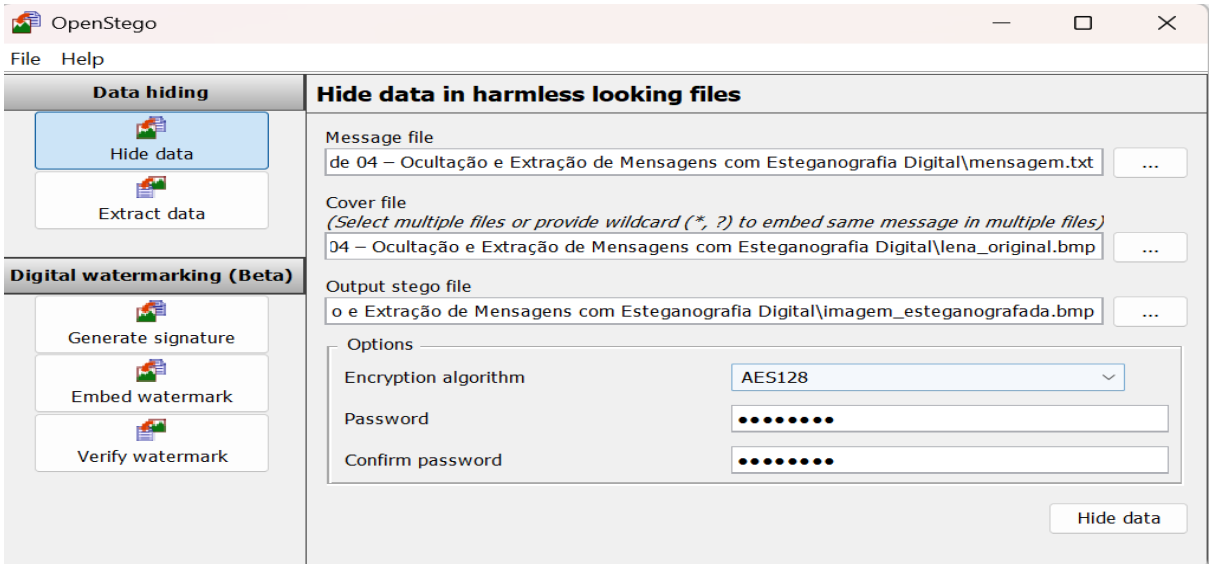
Pós-Graduação em Inteligência Cibernética e Segurança Ofensiva

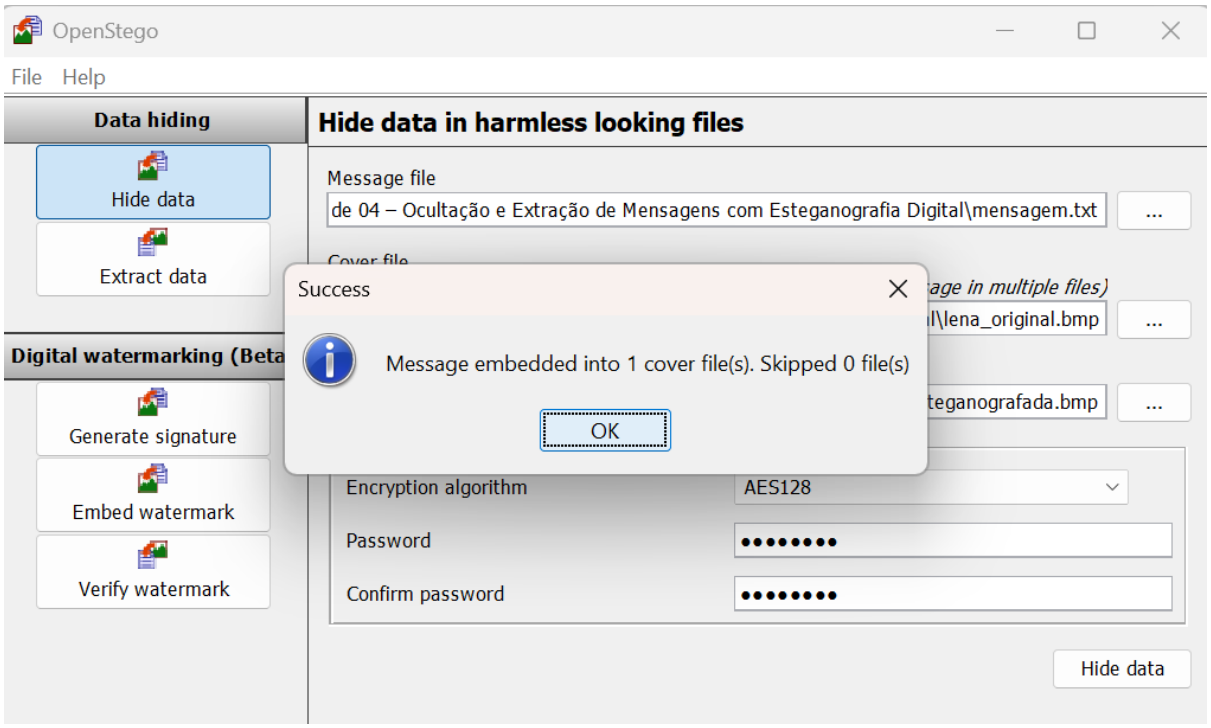
Disciplina: Ocultação de Dados

Professor: Juliano Bandeira Lima

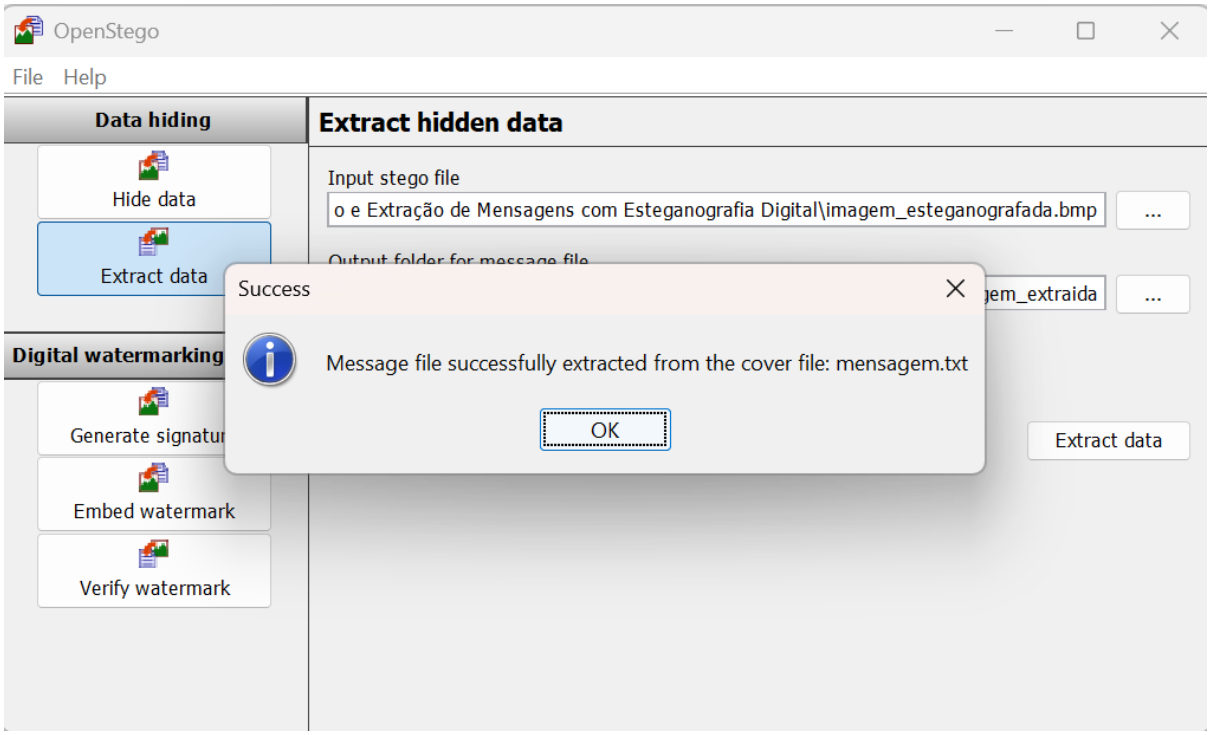
Alunos: Rafael Matos, Anderson Cesar e Mateus Guerra

1. Ocultação da mensagem em imagem .bmp

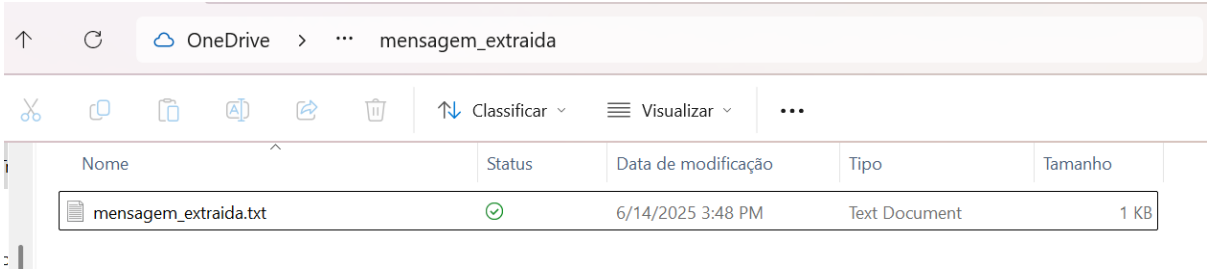




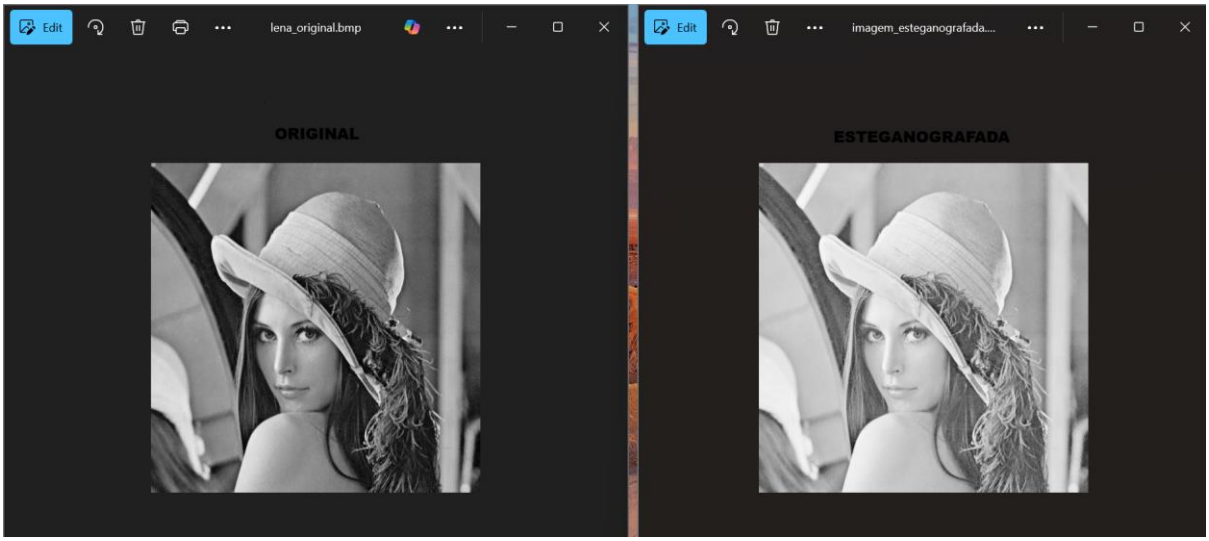
2. Extração da mensagem



3.1 Mensagem extraída

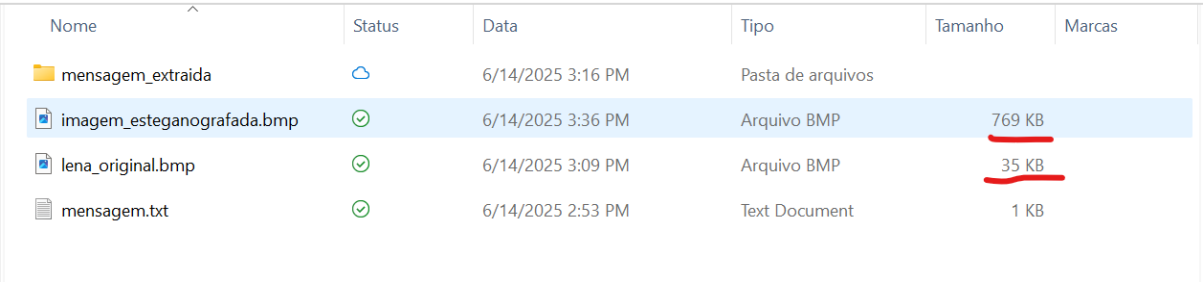


1. **A imagem marcada é perceptivelmente diferente da original?**



Sim, é visível que ao realizar a ocultação na imagem de formato .bmp ela se apresentou com tonalidade mais clara.

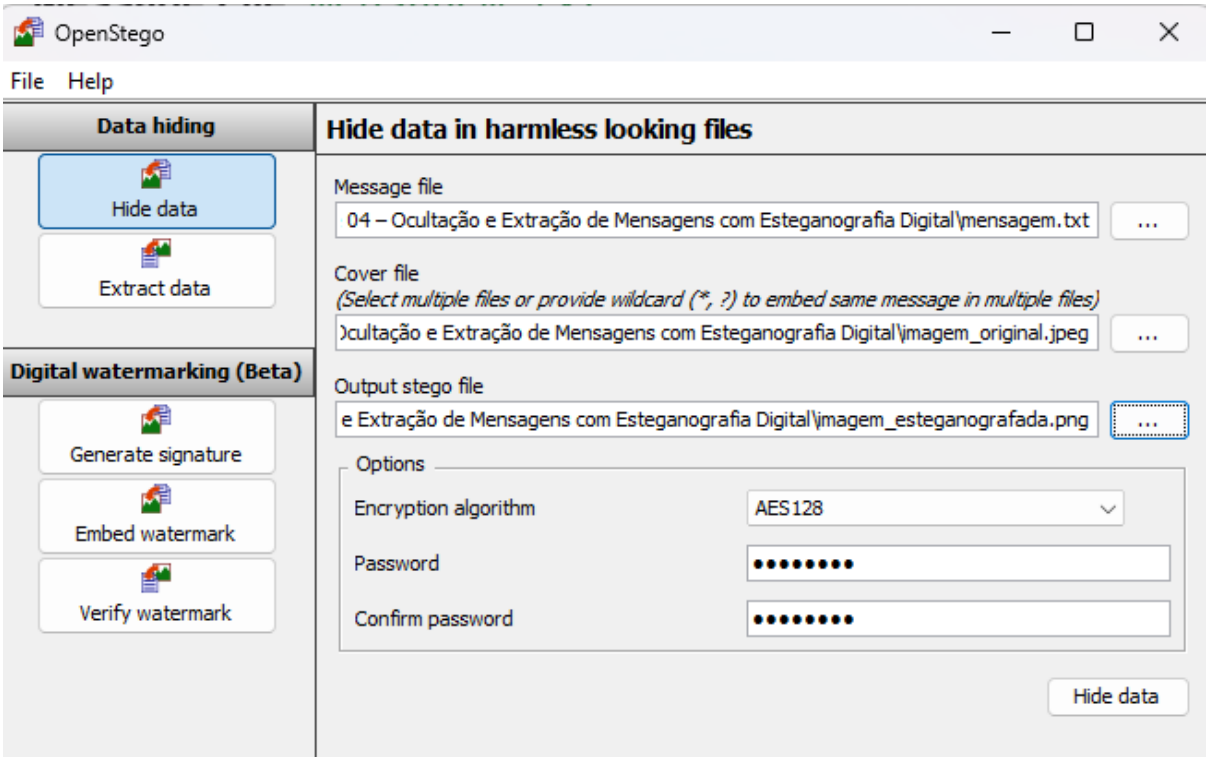
2. **O tamanho do arquivo foi significativamente alterado?**

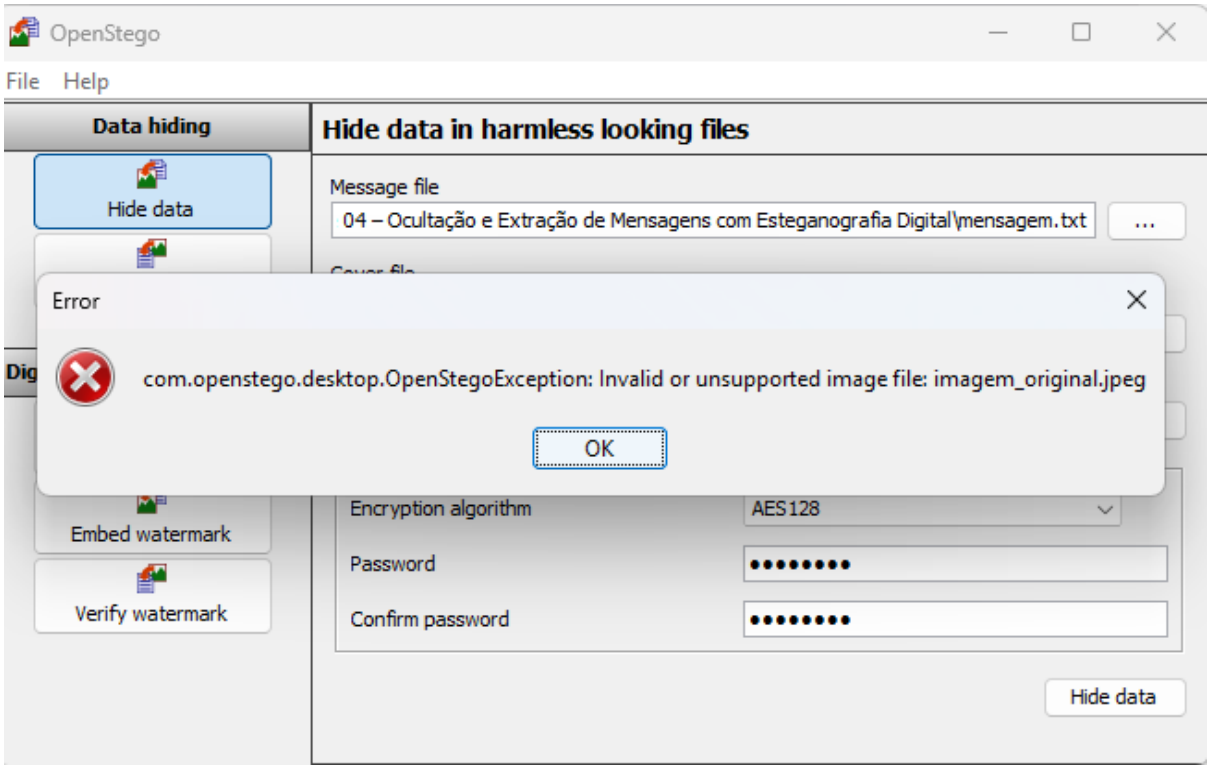


Sim, foi identificado que a imagem esteganográfica possui um tamanho mais elevado do que a original.

4. Tarefas Adicionais

1. **Realize a mesma ocultação em uma imagem JPEG e observe as diferenças.**





Infelizmente não foi possível fazer o experimento com o OpenStego pois ele não aceita esse formato jpeg.

2. **Utilize um software como StegExpose (linha de comando) para tentar detectar a presença da esteganografia.**

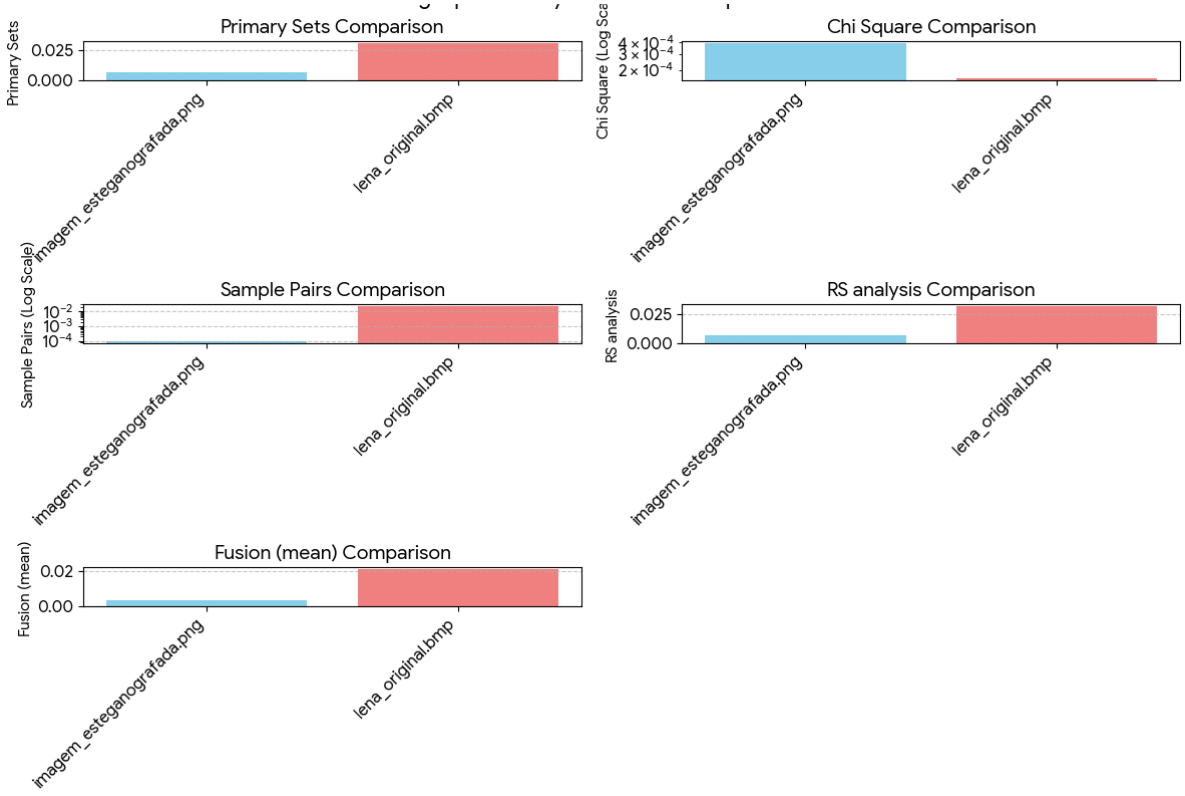
2.1 Execução do StegoExpose

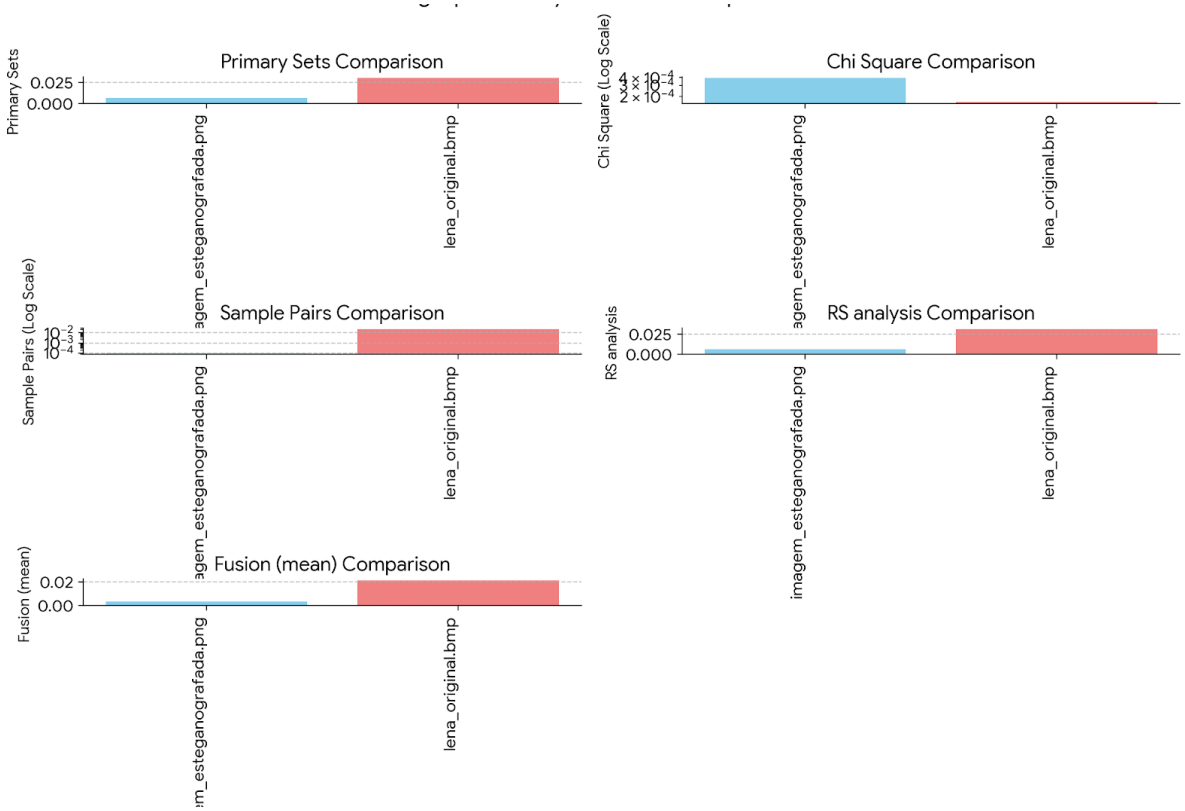
```
devel@LAPTOP-JJMLJ2BJ MINGW64 ~/OneDrive/Area de Trabalho/Atividade 04 - Ocultação e Extração de Mensagens com Esteganografia Digital/stego_expose
$ java -jar StegExpose.jar . default 0.2 resultado.csv

devel@LAPTOP-JJMLJ2BJ MINGW64 ~/OneDrive/Area de Trabalho/Atividade 04 - Ocultação e Extração de Mensagens com Esteganografia Digital/stego_expose
$
```

2.2 Resultado da execução:

Nome	Status	Data de modificação	Tipo	Tamanho
imagem_esteganografada.png	✓	6/15/2025 11:03 AM	Arquivo PNG	303 KB
lena_original.bmp	✓	6/14/2025 3:09 PM	Arquivo BMP	35 KB
mensagem_oculta.txt	↻	6/15/2025 11:01 AM	Text Document	5 KB
resultado.csv	↻	6/15/2025 11:03 AM	Arquivo de Valore...	1 KB
StegExpose.jar	✓	6/15/2025 10:38 AM	Executable Jar File	2,989 KB





Ambas as imagens analisadas (`imagem_esteganografada.png` e `lena_original.bmp`) foram classificadas como **"false"** na coluna "Above steg threshold?", indicando que a ferramenta **não detectou esteganografia** acima do limiar configurado para qualquer uma delas.

Análise Detalhada por Imagem:

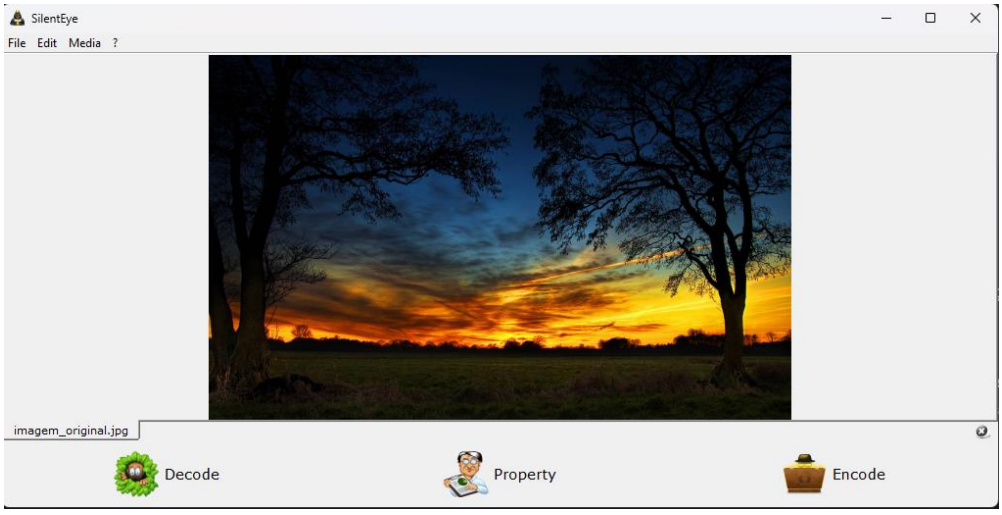
1. `imagem_esteganografada.png`
    a. **"Above steg threshold?":** `false`. Isso significa que, apesar do nome do arquivo sugerir que ele contém esteganografia, a ferramenta não o classificou como tal com base em suas métricas e limiares.
    b. **"Secret message size in bytes (ignore for clean files)":** 358. Um valor de tamanho de mensagem é apresentado, o que pode indicar que a ferramenta estimou que alguns bytes foram alterados, mas não o suficiente para caracterizar esteganografia detectável. Este valor pode ser simplesmente ruído ou alterações mínimas que não cruzaram o limiar de detecção.
    c. **"Primary Sets":** `0.006930109`. Este valor é muito baixo.
    d. **"Chi Square":** `3.9969054489588965E-4`. Um valor extremamente pequeno, próximo de zero, indicando que a distribuição de bits na imagem está muito próxima do que seria esperado para uma imagem limpa, sem esteganografia detectável por este método.
    e. **"Sample Pairs":** `0.00285901318295E-5`. Também um valor extremamente baixo.
    f. **"RS analysis":** `0.006703021`. Este valor é muito baixo. Para detecção de esteganografia LSB, valores significativos na Análise RS geralmente estariam mais próximos de 1.
    g. **"Fusion (mean)":** `0.00347131`. Este valor consolidado é extremamente baixo, corroborando a falta de detecção.
    h. **Conclusão para `imagem_esteganografada.png`:** Apesar do nome sugestivo, a análise estatística da ferramenta não encontrou evidências significativas de esteganografia LSB. Isso pode ocorrer se a esteganografia for muito sutil (poucos dados ocultos), ou se foi utilizada uma técnica que a ferramenta não consegue detectar (ex: uma técnica não LSB, ou uma que é mais resiliente a esse tipo de análise).
2. `lena_original.bmp`
    a. **"Above steg threshold?":** `false`. Como esperado para uma imagem "original" e não modificada.
    b. **"Secret message size in bytes (ignore for clean files)":** 253. Similar à primeira imagem, um pequeno valor é mostrado, mas sem indicar esteganografia. Isso é normal para imagens sem esteganografia real.
    c. **"Primary Sets":** `0.03062402370672454`.
    d. **"Chi Square":** `1.64015429897849795E-4`. Extremamente baixo.
    e. **"Sample Pairs":** `0.0298643831298207016`. Extremamente baixo.
    f. **"RS analysis":** `0.00143477`. Extremamente baixo, confirmando a ausência de esteganografia LSB.

g. **"Fusion (mean)":** `0.02123284988094852`. Muito baixo.
h. **Conclusão para `lena_original.bmp`:** As métricas são consistentemente muito baixas, confirmando que esta imagem é considerada **limpa** e sem esteganografia detectável pela ferramenta. Este resultado serve como um bom ponto de comparação para uma imagem que não deveria conter dados ocultos.

Os resultados indicam que a ferramenta não conseguiu identificar esteganografia acima do seu limiar de confiança em nenhuma das imagens analisadas. Para a `imagem_esteganografada.png`, isso sugere que a esteganografia, se presente, é muito sutil, ou que a técnica utilizada não é facilmente detectável pelos algoritmos estatísticos empregados por ferramentas como o StegExpose (que se focam primariamente em LSB). Para uma análise mais robusta de uma imagem suspeita, seria recomendável:

- Reduzir o limiar de detecção da ferramenta, se possível, para aumentar a sensibilidade.
- Empregar outras ferramentas de detecção de esteganografia que usem diferentes algoritmos ou que sejam mais adequadas para o tipo de arquivo (ex: ferramentas específicas para JPEG, se aplicável, ou para outras técnicas de esteganografia).
- Realizar uma análise manual ou com ferramentas de inspeção de bytes, caso haja suspeita forte.

3. **Gere uma imagem com múltiplas mensagens ocultas usando ferramentas SilentEye.**



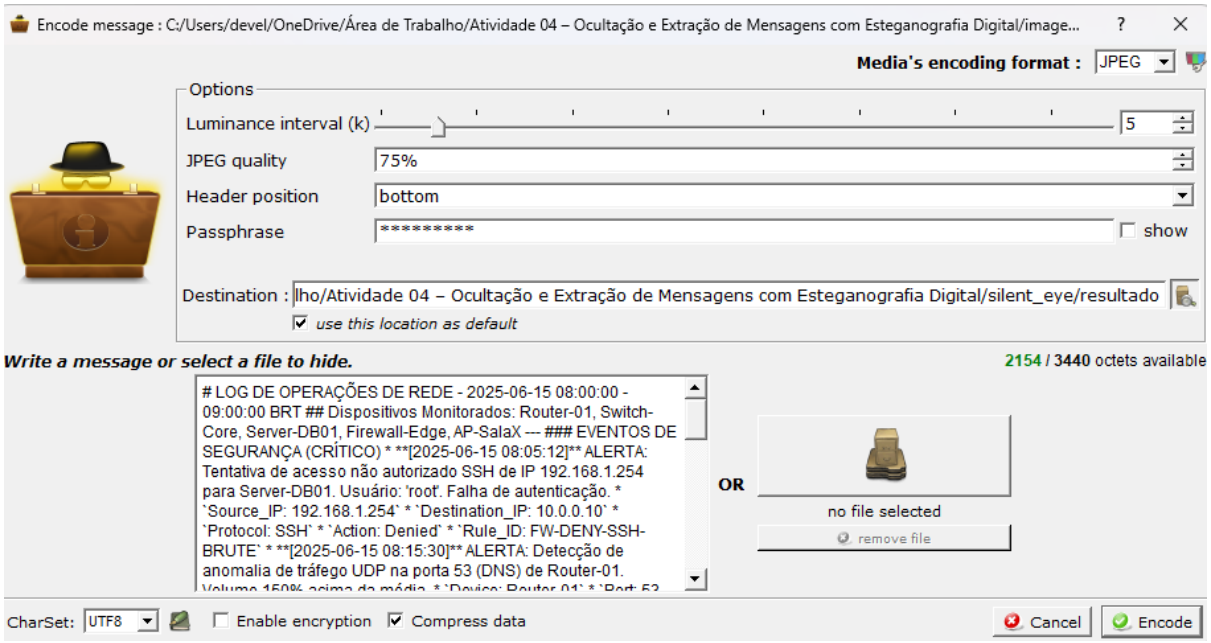


IMAGEM ORIGINAL

IMAGEM ESTEGANOGRAFADA

É possível perceber uma leva alteração de chuvisco na região central da imagem que possui mensagem oculta.

Outro ponto identificado foi um tempo relativamente alto para o processamento de encode na mensagem na ferramenta SilentEye em relação ao OpenStego.