Kryptologie (ENC-K)

Projektová dokumentace PEF_K_proj_stego

Martin Kmenta (`qqkmenta`)

29. února 2024

1 Úvod

Projekt PEF_K_proj_stego využívá steganografii k vkládání zpráv do obrázků. Tento dokument popisuje jeho fungování, použití, teoretické základy a možná vylepšení.

2 Vstup do problematiky

Aplikace je založena na teoretických principech steganografie a zajišťuje, že zprávy jsou vloženy způsobem, který zabraňuje jejich odhalení. To zahrnuje manipulaci s nejméně významnými bity (LSB) barevných kanálů každého pixelu obrázku, což je technika, která umožňuje uložit informace bez znatelných změn v obrázku.

Tato metoda využívá binární povahy digitálních obrazů, kde je každý pixel reprezentován kombinací bitů. Změnou LSB lze vložit informace přímo do obrazu, aniž by došlo k výrazným změnám jeho vnímatelných vlastností, protože tyto bity mají nejmenší vliv na barvu, kterou vnímá lidské oko.

Složitost do tohoto procesu lze vnést šifrováním. Před vložením vlastní zprávy do obrázku lze text zašifrovat pomocí kryptografického algoritmu, který poskytuje další vrstvu zabezpečení. To znamená, že i když je steganografická zpráva odhalena, bez správného dešifrovacího klíče zůstane zpráva nesrozumitelná. Použitý šifrovací algoritmus se může pohybovat od jednoduchých šifer, jako je Caesar, Vigenèrova šifra, až po pokročilejší, jako je AES nebo RSA, v závislosti na požadované úrovni zabezpečení.

Při dekódování probíhá opačný proces. Data LSB jsou extrahována a poté dešifrována, pokud bylo použito šifrování. Úspěch tohoto procesu závisí do značné míry na přesnosti extrakčního algoritmu, který dokáže z pozic LSB v rámci hodnot pixelů přesně rekonstruovat původní zprávu bit po bitu.

Některé formáty, které využívají kompresi, jako například JPEG, mohou v kontextu steganografie představovat problém, zejména při manipulaci s LSB. Kompresní algoritmus může změnit LSB, aby zmenšil velikost souboru, což může narušit skrytá data.

3 Instalace

Požadovaná verze Pythonu: 3.10+. Je potřeba nainstalovat závislosti pomocí pip:

```
pip install -r requirements.txt
```

Závislosti:

- `opencv-python` pro zpracování obrázků
- `numpy` pro numerické výpočty
- `Pillow` pro manipulaci s obrázky
- `tqdm` pro progress bar

4 Použití

Spuštění aplikace pomocí argumentů příkazového řádku.

```
main.py [-h] [-m MESSAGE] [-e] [-d] [-i IMAGE] [-o OUTPUT] [-t] [-g]
```

- `-h`: Zobrazí nápovědu
- `-e`: Zakóduje zprávu
- `-d`: Dekóduje zprávu
- `-i`: Cesta ke vstupnímu obrázku
- `-o`: Cesta pro výstup (obrázek)
- `-t`: Spuštění testů
- `-g`: Spuštění grafického rozhraní

Program umí zakódovat a dekódovat zprávu do binární podoby. Dokáže načíst a uložit obrázek, do kterého může zakódovat zprávu, nebo ji dekódovat. Aktuálně jsou podporovány obrázky ve formátech `.bmp` a `.png`.

Pro zakódování je potřeba zadat parametr `-e`, pro dekódování pak parametr `-d`.

Pokud při kódování není zadán parametr `-i`, bude zpráva pouze kódována do binární podoby. V opačném případě bude bude kódována zpráva v obrázku a je nutné v případě zakódování zadat i výstupní cestu pomocí parametru `-o`.

Byly napsány základní testy pro testování funkcionality programu, které je možné spustit pomocí parametru `-t`.

V grafickém rozhraní (GUI) jsou k dispozici tlačítka pro načtení obrázku, zahájení procesu kódování nebo dekódování spolu s poli pro tajnou zprávu a log, usnadňující práci s nástrojem a eliminující potřebu používat příkazovou řádku. GUI lze otevřít buď pomocí parametru `-g`, nebo spuštěním programu bez parametrů. Ukázka GUI je na obrázku 1.

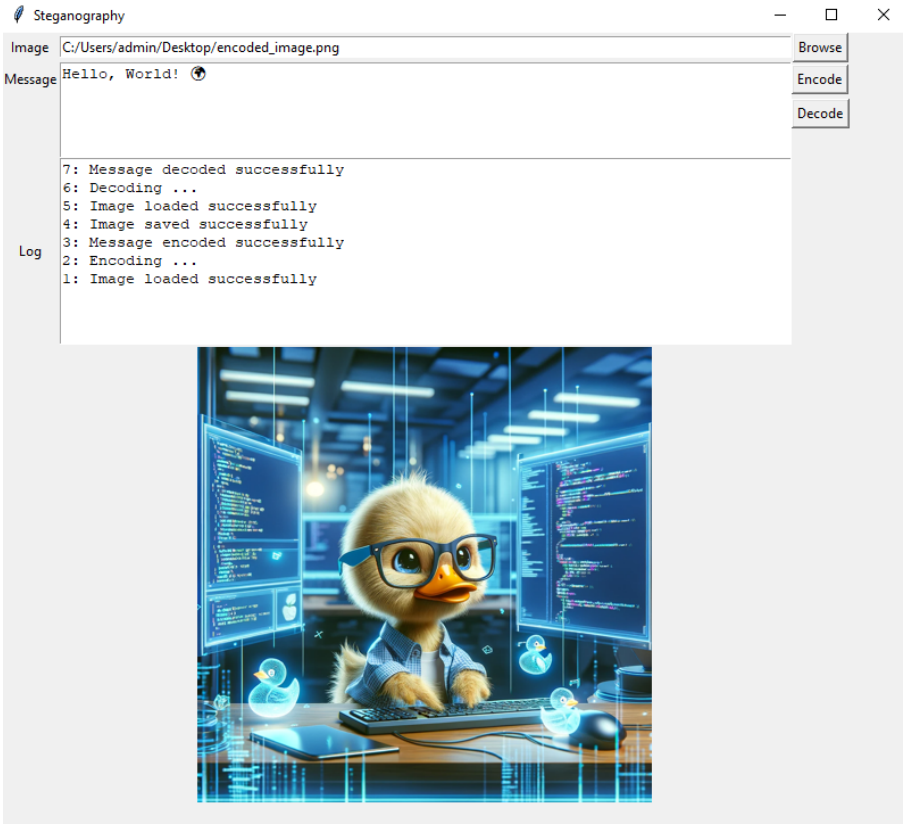
5 Možná vylepšení

Budoucí vylepšení by mohly zahrnovat:

1. Pokročilé metody šifrování zprávy pro zvýšení bezpečnosti.
2. Podpora dalších formátů obrázků pro zvýšení použitelnosti.
3. Vylepšení grafického uživatelského rozhraní pro více intuitivní ovládání.
4. Optimalizace efektivity pro rychlejší zpracování velkých obrázků nebo dlouhých zpráv.
5. Rozšíření programu o možnosti kódování do dalších typů médií, jako jsou například videa a audio.

6 Závěr

PEF_K_proj_stego nabízí bezpečnou metodu vkládání zpráv do obrázků. Tato dokumentace poskytuje základní informace pro pochopení, používání a případné možná vylepšování aplikace.



Obrázek 1: Snímek obrazovky grafického rozhraní