Programiranje v Pythonu

Izdelava programa za steganografijo slik

Matej Marinko

februar 2017

Kazalo

Povzetek

Namen naloge je ugotoviti, ...

1 Uvod

2 Steganografija

Steganografija je znanost, ki omogoča skrivanje podatkov v navidezno nepomembnem prenosnem mediju. Beseda izhaja iz grščine, in pomeni *zakrito pisanje*. Predstavlja skupek metod za skrivanje informacij v neke druge informacije. Za razliko od kriptografije oz. šifriranja, ki želi podatke narediti neberljive, steganografija poskuša prikriti, da ti podatki sploh obstajajo [1].

Šibkost kriptografije je, da je sporočilo sumljivo že na prvi pogled. Šibkost steganografije pa je, da ko nekdo enkrat odkrije, kje je sporočilo skrito, ga lahko enostavno prebere. V praksi se zato pogosto uporabljata obe metodi skupaj, saj druga drugi odpravita slabosti.

2.1 Tehnike

Primeri steganografije so znani že od Antike, različne tehnike pa so se ohranile vse do danes. Z razvojem računalništva se je steganografija razvila tudi na digitalnem področju.

Primeri fizičnih tehnik:

- V Stari Grčiji so sporočila skrivali v voščene tablice. Na les so napisali sporočilo, ki so ga nato prekrili z voskom. Na vosek pa so napisali nedolžno in nepomembno sporočilo.
- Drugi postopek, ki so ga uporabljali v Antični Grčiji je bil približno takšen: Sužnju so pobrili glavo in mu vtetovirali sporočilo. Ko so lasje zrasli sporočilo ni bilo več vidno. Očitna pomankljivost te motode je, da moramo počakati, da osebi lasje zrastejo nazaj.
- Sporočilo, ki je napisano z nevidnim črnilom, na nepopisanem delu pisma.
- Sporočilo je v Morsejevi abecedi, napisani na prejo, ki so jo potem vtkali kurirju v blago.
- Del črk v besedilu je napisan z drugačno pisavo kot druge črke (npr. ležeče). Te črke so tvorile skrivno sporočilo. [3]
- Nemci so med drugo svetovno vojno uporabljali mikropike (microdots). Podatke so skrivali v znakih, ki jih je bilo mogoče prebrati samo pod veliko povečavo. [1]
- Cardanovo rešeto - mreža z odprtinami, s katero prekrijemo besedilo, da se prikaže skrito sporočilo.

- Ameriški pilot Jeremiah Denton, ki ga je ujela vietnamska vojska, je bil med televizijsko konferenco prisiljen pričati, da z njim v ujetništvu ravnajo dobro. Hkrati pa je z mežikanjem v morsejevi abecedi črkoval besedo T-O-R-T-U-R-E (mučenje).[2]

Primeri digitalnih tehnik:

- Skrivanje podatkov v najnižje bite slikovnih datotek, z neopaznimi spremembami barv.
- Skrivanje podatkov v zvočni zapis, s spremembami, neslišnimi za človeško uho.
- Tehnika *pletja in presejanja* (chaffing and winnowing), kjer gre za to da paketkom, ki gredo čez nezavarovano povezavo dodamo lažne paketke, v katere lahko skrijemo sporočilo.
- Dodajanje podatkov v neuporabljene dele datoteke, npr. na konec.
- Skrivanje z uporabo unicode znakov, ki izgledajo enako kot ASCII znaki.
- Nekateri moderni tiskalniki z težko vidnimi svetlo rumenimi pikami na vsakem listu označijo serijsko številko tiskalnika in čas tiska. [3]

2.2 Steganografija digitalnih fotografij

Večja kot je datoteka, v katero nameravamo skriti naše sporočilo, v primerjavi z tem sporočilom, lažje jo je skriti. Zato so slike primerne za steganografijo, saj vsebujejo velike količine podatkov. Tako lahko skrijemo podatke npr. na Internetu. Slika je vsem na očeh, venar se nihče ne zaveda, da so v njej skrite še dodatne informacije. Ni znano, kako pogosta je ta praksa, vendar vemo da obstaja.

V RGBA zapisu uporabimo 32 bitov za vsak piksel, to pomeni 8 bitov za vsako komponento. Samo rdeča barva ima 2^8 različnih intenzivnosti. (Glej poglavje: Zapis slik v računalniku) Razliko med $10111111_{(2)}$ in $10111110_{(2)}$ v inteziteti barve človeško oko zelo težko prepozna. Zato lahko najnižje bite (least significant bits) spremenimo in v njih skrijemo svoje podatke. Če v vsakem pikslu v vseh štirih komponentah spremenimo 2 najmanj pomembna bita, lahko v en piksel skrijemo 1 bajt (8 bitov) podatkov. V celotni sliki lahko, če je dovolj velika, skrijemo tudi več MB podatkov.

Pri tem je pomembno, da slika, v katero želimo skriti podatke ni enobarvna, oziroma sestavljena iz večjih enobarvnih ploskev. Če je slika takšna,

obstaja večja možnost, da kdo opazi različne odtenke sosednjih pikslov na sliki. Zato so slike, ki se uporabljajo za steganografijo pogosto slike narave, živali, ipd.

3 Zapis slik v računalniku

Slika je v računalniku zapisana tako, da je razdeljena na drobne kvadratke, imenovane piksli. Vsak piksel ima podatke kako močno in v katerih barvah žari. Za zapis se uporablja več različnih formatov, med katerimi so najbolj znani JPEG, PNG, BMP, GIF... Med seboj se razlikujejo v različnih lastnostih, kot so način zgoščevanja, število možnih barv posameznega piksla...

Osnovna zgradba vsakega formata sestoji iz:

glave, ki vsebuje glavne podatke, kot so velikost, barvna globina in kompresijska tehnika.

slikovnih podatkov oziroma niza pikslov. Podatki so lahko kompresirani ali nekompresirani.

polj za metapodatke (metadata), kot so datum posnetka, avtor slike...

3.1 Format PNG

PNG (Portable Network Graphics) je razmeroma nov slikovni format, ki je popularen predvsem na spletu.

Format PNG uporablja brezizgubno kompresijo, kar nujno potrebujemo pri steganografiji, saj se zanašamo da bomo podatke skrili tako, da jih človeško oko ne bo zaznalo. Izgubna kompresija pa izpušča podatke, ki jih človeško oko ne more zaznati, ter tako onemogoča pridobivanje skritega sporočila nazaj iz slike.

Ena izmed prednosti formata PNG pred drugimi slikovnimi formati je podpora več različnih barvnih tabel. Poleg standardnega RGB (Red Blue Green) zapisa podpira tudi RGBA (Red Green Blue Alpha) zapis, katerega bistvena razlika je dodaten alpha kanal. Le-ta se navadno uporablja za prosojnost slik. Če je vrednost kanala 0% je piksel popolnoma prosojen, če pa je vrednost 100% pa je piksel enak običajnim pikslom.

V primeru steganografije dodaten kanal veliko pripomore, saj lahko v sliko skrijemo kar $\frac{1}{4}$ več informacij, kot v rapisu RGB (Glej poglavje: Steganografija digitalnih fotografij).

4 Python

Python je moderen programski jezik, ki je nastal ...

4.1 Bitne operacije

5 AES kriptiranje

6 Program

```
def hide_core(image_data, secret, size):
    new_image = Image.new('RGBA', size)
    new_image_data = new_image.getdata()

    index = 0
    for y in range(size[1]):
        for x in range(size[0]):
            r, g, b, a = image_data.getpixel((x, y))

            if index < len(secret):
                r &= ~3
                g &= ~3
                b &= ~3
                a &= ~3
                r |= secret[index] & 3
                g |= (secret[index] & 12) >> 2
                b |= (secret[index] & 48) >> 4
                a |= (secret[index] & 192) >> 6
                index += 1

            new_image_data.putpixel((x,y), (r, g, b, a))

    return new_image
```

Literatura

[1] Marko Hölbl, Skrivanje podatkov - steganografija. *Monitor*, Oktober 2008. Pridobljeno iz `www.monitor.si/clanek/skrivanje-podatkov-steganografija`.

[2] Mojca Kumerdej, Doma sem nikjer in hkrati povsod. Moja identiteta je steganografska. *DELO*, 11. 2. 2017

[3] Steganography (2017). Wikipedija The Free Encyclopedia. Pridobljeno iz `en.wikipedia.org/wiki/Steganography`