Aplicații Multimedia

Laborator 6

Watermarking. Steganografie

Cuprins

Watermarking

Watermarkingul digital este un marcaj transparent (scris sau imagini/ logo-uri) care se aplică pe imagini sau documente, funcția sa principală fiind aceea de a proteja proprietatea intelectuală asupra respectivelor documente. În mod normal, un watermark este dificil sau chiar imposibil de eliminat, prevenind astfel utilizarea neautorizată a fișierului.

Deși dorim să protejăm documentul, este important ca informația propriu-zisă din acesta să nu devină dificil de recunoscut ca urmare a aplicării watermark-ului. Următoarele aspecte sunt câteva reguli generale pentru aplicarea unui watermark:

- Să fie mic și monocromatic – sau cu foarte puțină culoare. Watermark-urile prea mari sau în multe culori pot distrage atenția de la imagine sau conținutul documentului.
- Să fie plasat într-o zonă discretă a imaginii/documentului, care nu interferează cu vizualizarea, dar care face totuși mai dificilă eliminarea sau clonarea.
- Să aibă puțin text.

Exemplu watermark [sursă]

Steganografie

Steganografia este o tehnică de a trimite mesaje considerate secrete folosindu-se ca mediu purtător un conținut obișnuit, care nu este secret. De fapt, ceea ce se dorește de fapt este să se ascundă faptul că se trimite un mesajul secret.

Tehnicile steganografice variază de la metode clasice, precum scrierea cu cerneală invizibilă sau puncte minuscule perforate printre rândurile unei scrisori, ascunderea unui mesaj în prima/ a doua/ ultima literă din cuvintele unui text, la metode digitale, precum mascarea informațiilor în pagini web, ascunderea unor fișiere cu nume aparent importante în directoare ale sistemului de operare, sau chiar în fișiere audio sau video.

De cele mai multe ori, în cazul metodelor digitale, fie că este vorba despre text, audio sau imagini, informația este mai întâi criptată, pentru a asigura o dublă protecție. Astfel, pentru a descoperi mesajul ascuns, trebuie ca o terță parte mai întâi să își dea seama de existența lui, să îl extragă și apoi să îl decripteze.

Formula de mai jos reprezintă o descriere generală ale componentelor unui proces steganografic:

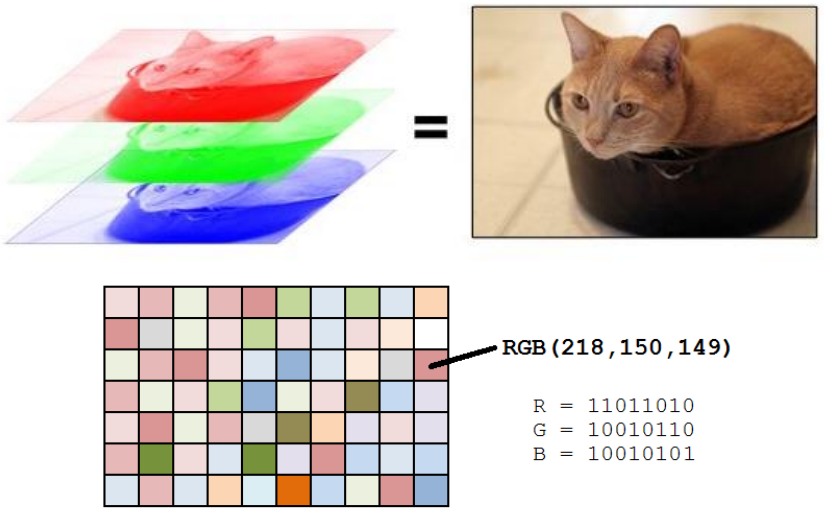
În mediul purtător vor fi incluse datele ascunse, ambele putând fi criptate cu cheia steganografică. Este necesar ca rezultatul, mediul steganografic menționat mai sus să fie de același tip cu mediul purtător. Cel mai frecvent, acestea sunt reprezentate de text, imagini sau fișiere audio.

Steganografia în imagini

Imaginile reprezintă un mediu purtător bun pentru ascunderea de date, fiind de dimensiuni mari (de ordinul MB), ceea ce înseamnă că datele adăugate suplimentar pot fi de asemenea de ordinul MB. Totuși, cu cât se adaugă mai multe date într-o imagine, cu atât este mai facil să se descopere prin metode statistice că pe respectiva imagine au fost folosite tehnici steganografice.

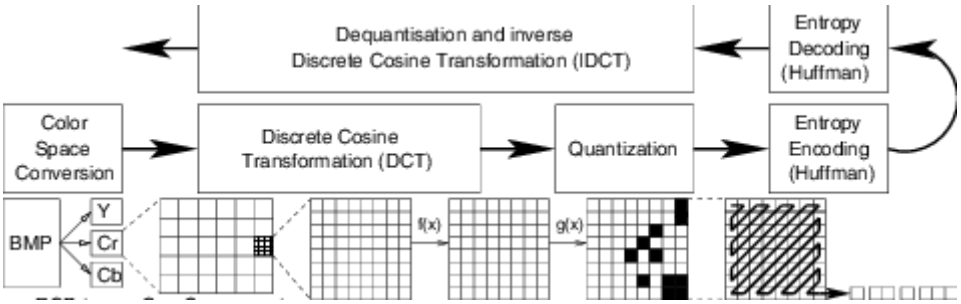
Cea mai simplă modalitate de realizare a steganografiei pe imagini este metoda celui mai puțin semnificativ bit (LSB), în care cei mai mici biți din reprezentarea culorilor într-o imagine se modifică cu biți mesajului dorit.

Așa cum a fost discutat deja, imaginile sunt cel mai des reprezentare în spectrul de culoare RGB (roșu, verde, albastru), ceea ce înseamnă că un pixel roșu poate fi exprimat ca o pereche (255, 0, 0), cu valoarea maximă pe canalul de roșu și valoare minimă pe canalul de verde și de albastru. De asemenea, există mai multe formate în care se pot stoca imagini, în care se stochează valorile pixelilor, fie ca atare, fie cu modificări.



Dimensiunea unei imagini va depinde, bineînțeles, de numărul de pixeli din aceasta, dar și de numărul de biți pe care se reprezintă fiecare canal de culoare.

Spre exemplu, dimensiunea unei imagini de 640x480 de pixel cu 3 canale ar fi de aproximativ 900KB necomprimată. Pentru a reduce dimensiunea imaginilor, există mai multe tipuri de compresii (PNG, GIF, JPEG). PNG folosește o compresie lossless, iar JPEG o compresie lossy, ceea ce înseamnă ca imaginea stocată este foarte asemănătoare cu cea originală, dar nu identică.

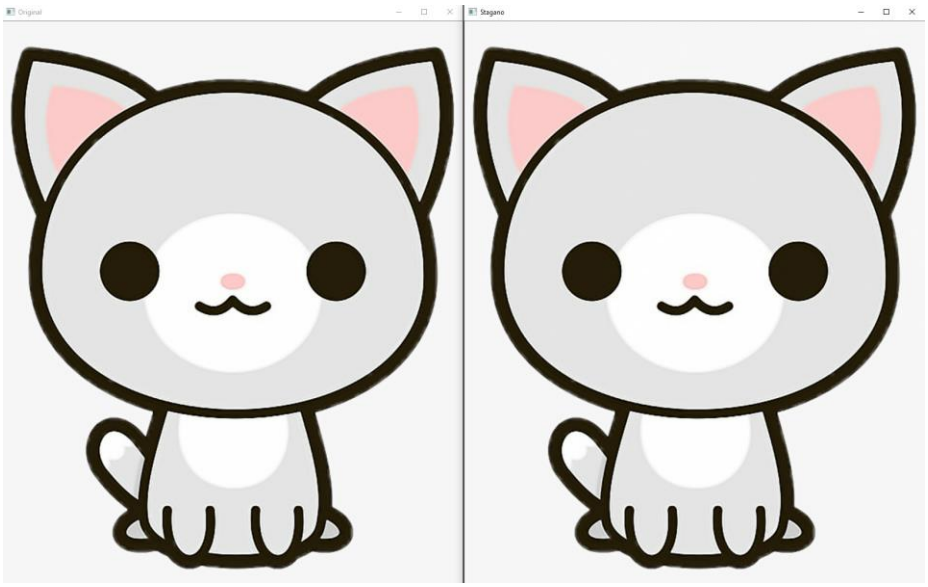


Pentru steganografie, mai potrivite sunt tipurile de compresie și formatele lossless, în care se păstrează integritatea imaginii inițiale. Totuși, există și tehnici pentru steganografia pe imagini JPEG.

Metoda LSB

Este asemănătoare cu metoda folosită în steganografia audio și se folosește de faptul că ochiul uman nu este suficient de sensibil pentru a repera schimbări minore în intensitățile pixelilor. Astfel, metoda LSB presupune că se va lua reprezentarea binară a mesajului ascuns și se vor suprascrie ultimul sau ultimii 2 cei mai puțini semnificativi biți ai imaginii purtătoare.

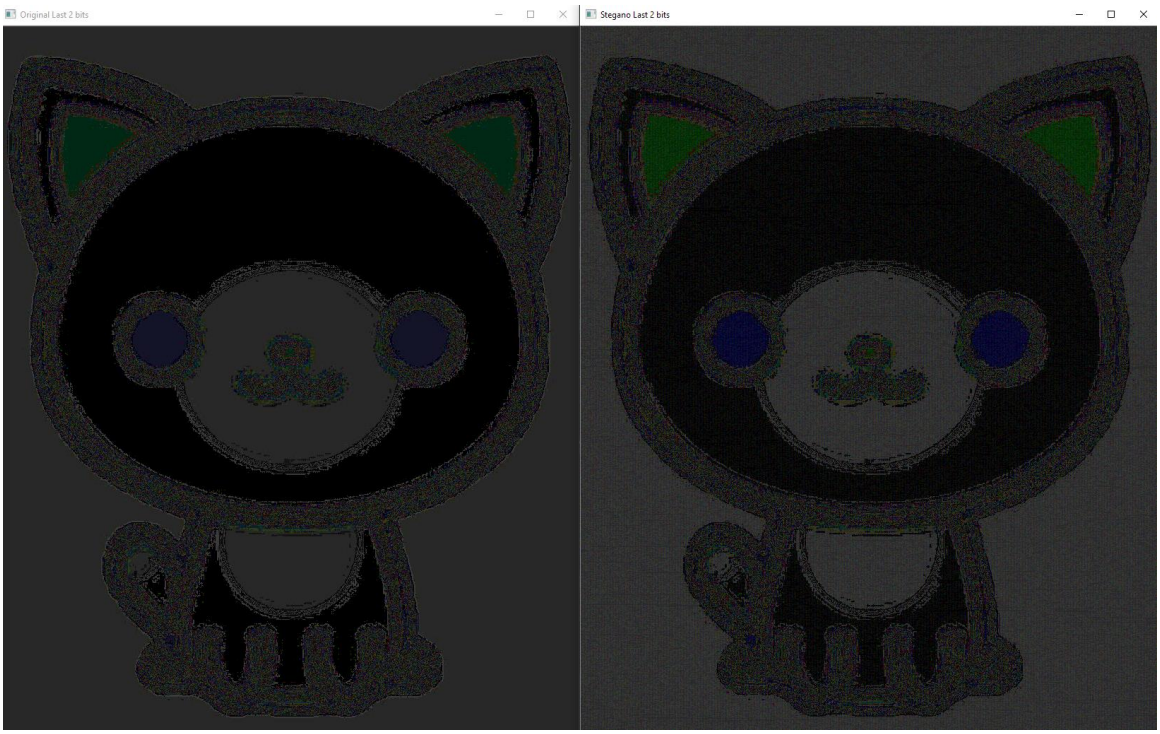
Imaginile de mai jos reprezintă originalul și imaginea steganografică obținută prin adăugarea unui text care are aproximativ 600KB. După cum se poate vedea, cu ochiul liber nu se observă nicio diferență.



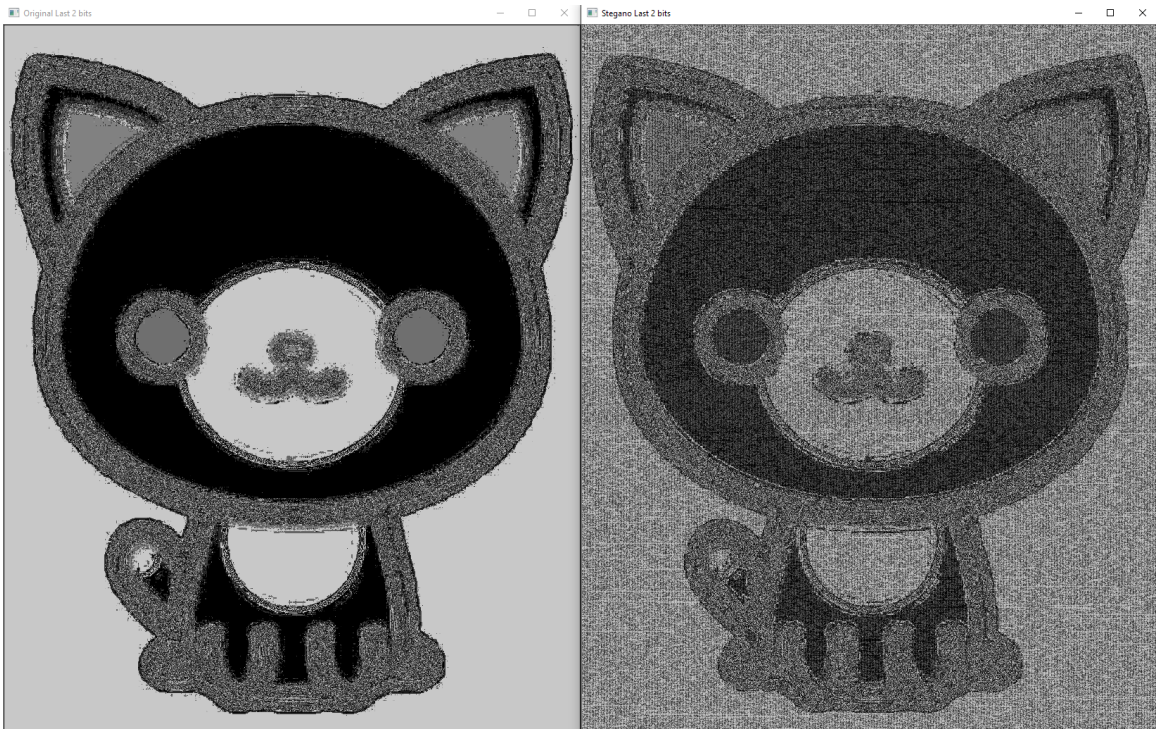
Totuși, imaginea aleasă pentru ascunderea textului nu este potrivită din 2 motive:

1. Este ușor de găsit online. Este de preferat ca atunci când se aplică tehnici steganografice pe o imagine purtătoare, sursa să nu fie disponibilă. În caz contrar, imaginea steganografică și cea inițială pot fi comparate și mesajul poate fi descoperit mai facil.
2. Are multe zone în care culorile sunt constante. Cele mai bune imagini pentru steganografie sunt acelea în care intensitățile pixelilor se schimbă și variază în vecinătăți adiacente. Acest aspect mai este cunoscut și ca textură.

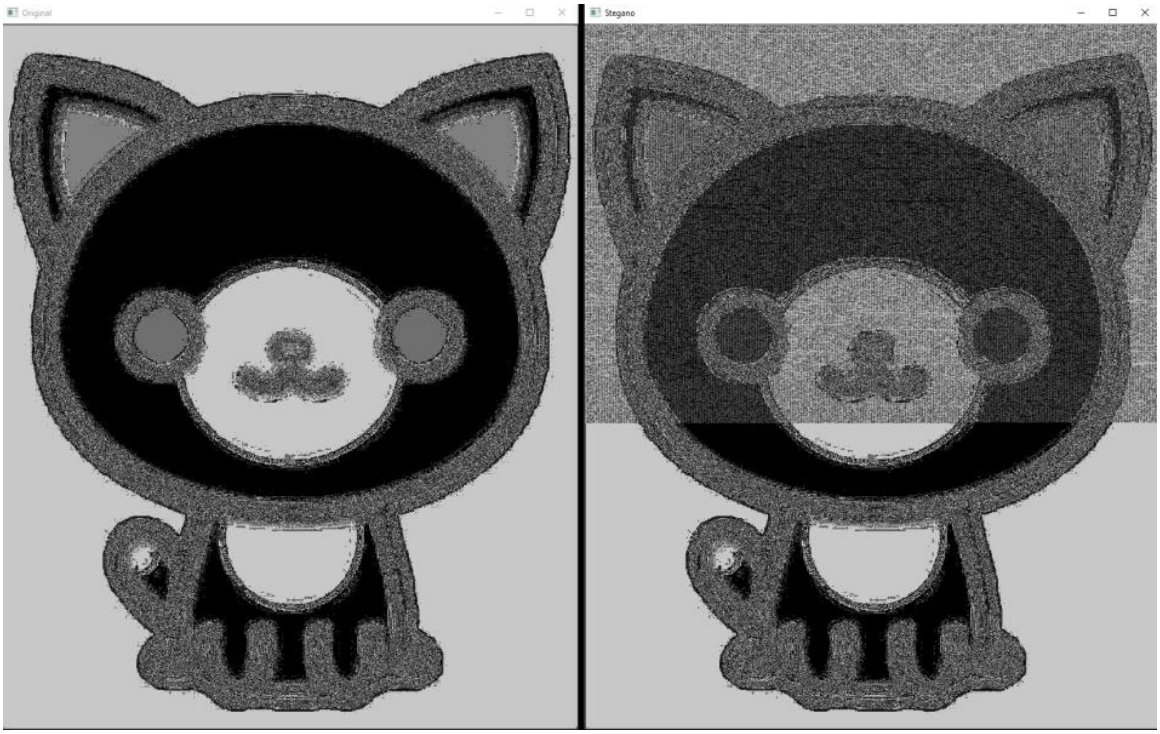
În imaginea de mai jos au fost reprezentați doar ultimii 2 biți din reprezentarea pe 8 biți a imaginilor, atât înainte, cât și după ascunderea textului. Se poate observa că imaginea steganografică este caracterizată de mult mai mult zgomot decât cea inițială. Pentru evidențiere, în imaginea de mai jos, valoarea ultimilor 2 biți a fost amplificate de 20 de ori.



Imaginea de mai jos este tot o reprezentare a ultimilor 2 biți, multiplicați de 100 de ori, iar imaginile rezultate transformate în grayscale din RGB.

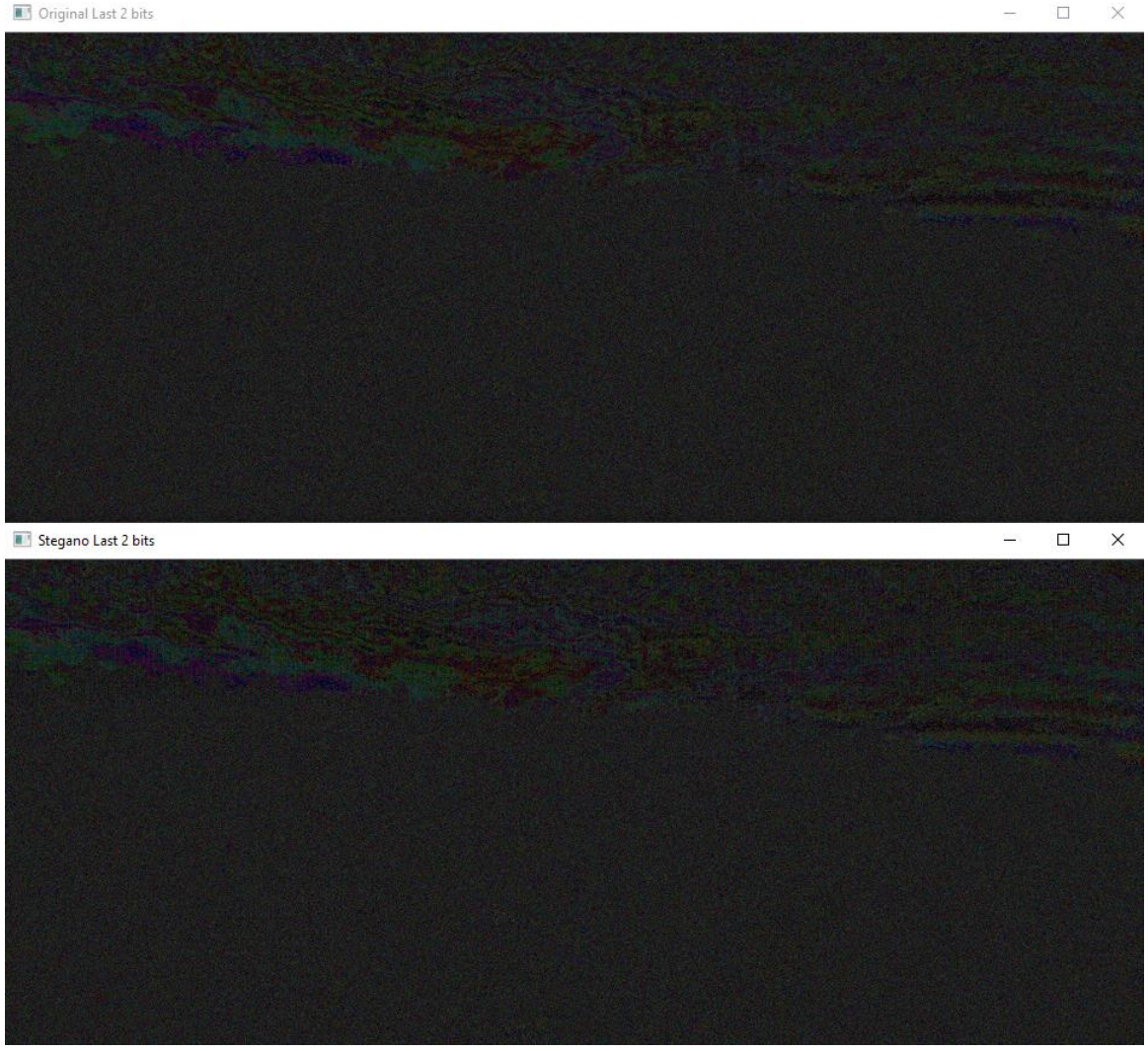


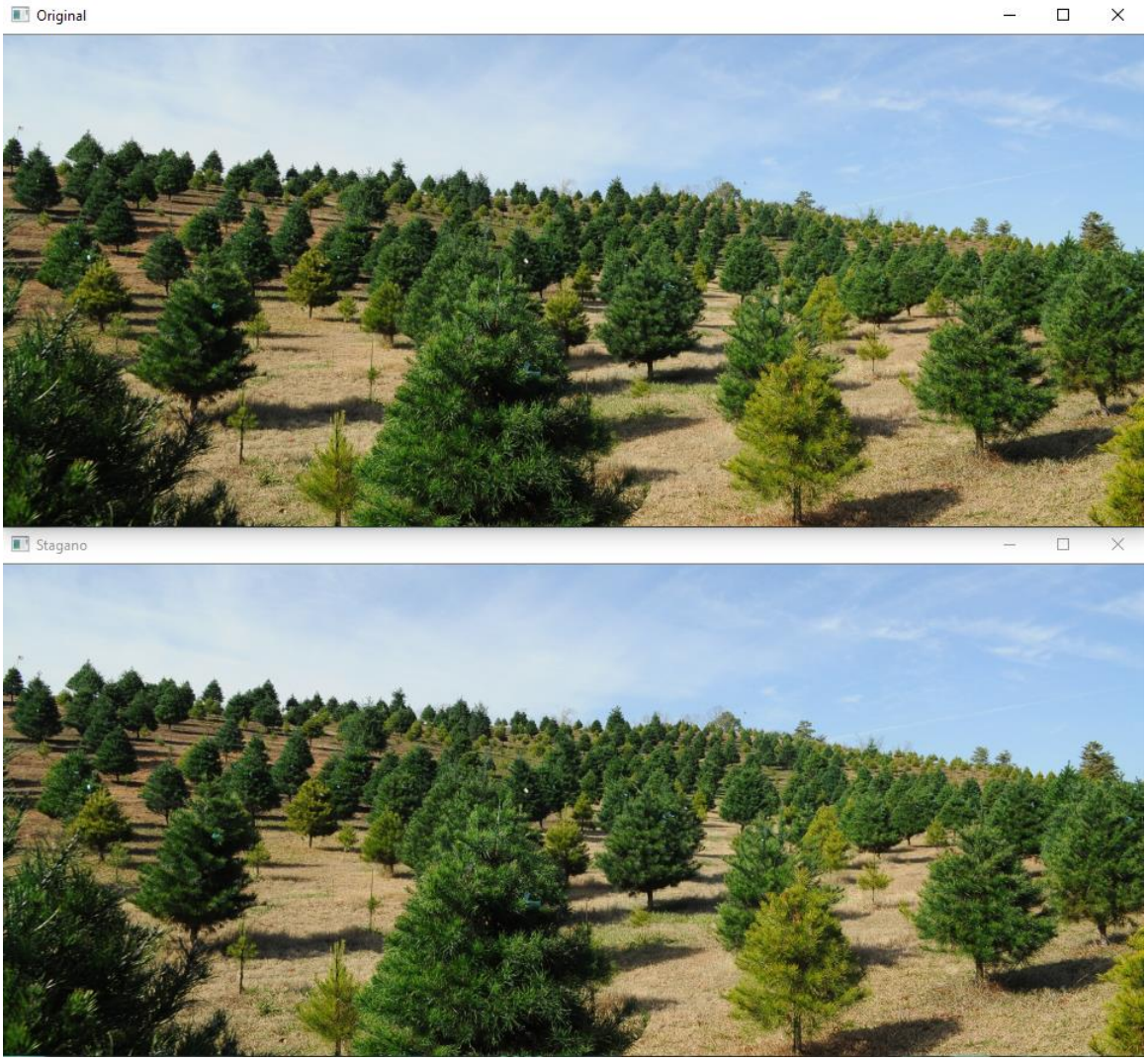
De asemenea, detecția poate fi mult mai simplă dacă dimensiunea textului este cu mult mai mică decât dimensiunea maximă dată de ultimii doi biți ai imaginii. Exemplul de mai jos arată introducerea unui text de aproximativ 150KB într-o imagine de aproximativ 820KB.



Imaginile afișate sunt de asemenea în tonuri de gri, iar ultimii 2 biți multiplicați cu 100.

Exemplele de mai jos arată ascunderea aceleiași cantități de text, dar într-o imagine cu variații mai mari ale intensității:




Original
Stagano