Steganografia imaginii

Autor: Duțulescu Darius-Mihail, 333AA

An: al III-lea

Cuprins

[1. Introducere 3](#_Toc135568631)

[1.2 Prezentarea temei 4](#_Toc135568632)

[1.3 Prezentarea obiectivelor 4](#_Toc135568633)

[1.4 Terminologii ale steganografiei imaginii 5](#_Toc135568634)

[2. Prezentarea tehnică a etapei de implementare 6](#_Toc135568635)

[2.2 Algoritm folosit pentru ascunderea mesajului ascuns 7](#_Toc135568636)

[2.3 Biblioteci utilizate in cadrul proiectului 8](#_Toc135568637)

[3. Prezentarea modului de utilizare a proiectului 9](#_Toc135568638)

[4. Concluzii 12](#_Toc135568639)

[5. Bibliografie 14](#_Toc135568640)

**Cuvânt înainte**

Steganografia este una dintre acele metode folosite pentru schimbul ascuns de informații și poate fi definită că studiul comunicației "invizibile". În acest fel, dacă se realizează cu succes, mesajul nu atrage atenția interceptorilor și atacatorilor. Folosind steganografia, informațiile pot fi ascunse în diferite medii de încorporare, cunoscute sub numele de purtători (en. carriers).

Acești purtători pot fi imagini, fișiere audio, fișiere video și fișiere text. Accentul în această lucrare este utilizarea unui fișier imagine ca purtător, folosind metoda celui mai nesemnificativ bit (en. LSB).

# Introducere

Cuvântul steganografie provine din cuvintele grecești steganos (care înseamnă "ascuns") și graphia (care înseamnă "scris"), care, practic, înseamnă scriere ascunsă. În termeni generali, steganografia este cunoscută ca o comunicație "invizibilă". Steganografia înseamnă ascunderea unor mesaje existente în alt mediu, precum audio, video, imagini, comunicații. Sistemele steganografice de astăzi folosesc obiecte multimedia, cum ar fi imagini, audio, video ca suport, deoarece oamenii, de obicei, transmit imagini digitale prin e‑mail sau le distribuie prin alte aplicații de comunicare pe internet. Există diferențe între steganografie și protejarea conținutului actual al unui mesaj. În cuvinte simple ar fi ascunderea unei informații în altă informație.

Steganografia diferă și de criptografie. Criptografia are ca scop securizarea informațiilor prin schimbarea datelor într-o forma pe care un interceptor nu ar putea-o descifra. Pe de alta parte, tehnicile de steganografie au tendință de a ascunde existența mesajului în sine, lucru ce îl face pe un observator să își dea greu seama unde este mesajul. În unele cazuri, trimiterea informațiilor criptate poate atrage atenția, pe când, cele invizibile, nu. În consecință, criptografia nu este cea mai buna soluție pentru o comunicare sigură, este doar o parte a soluției. Ambele științe pot fi folosite împreună pentru o protectie mai buna a informației. În acest caz, daca steganografia dă greș, mesajul nu poate fi recuperat pentru că este folosită și o tehnica de criptare.

Watermarking-ul și fingerprinting-ul, printre alte tehnologii, legate de steganografie, sunt folosite pentru protecția proprietății intelectuale. Watermark-ul digital este un semnal încorporat permanent în date digitale (audio, video, imagini și text) și poate fi detectat sau extras ulterior, după ce este confirmată autenticitatea datelor. Watermark-ul este ascuns în fișierele gazda în așa fel încât acesta nu poate fi eliminat fară a degrada mediul gazda. Deși această metodă păstrează datele accesibile, acesta este un marcaj permanent. Informația ascunsă în cadrul unui obiect watermark este o semnătură care se referă la originea sau adevăratul autor al datei, pentru a asigura protecția împotrivă copywriting-ului. În cazul fingerprinting-ului, diferite și specifice semne sunt incluse în copii ale lucrării pe care diferiți clienți ar trebui să le primească. În acest caz, devine foarte ușor pentru proprietar să identifice clienții care încalcă dreptul cu privire la licență produsului atunci când transmit ilegal produsul altor grupuri. (1)

Performanța unui sistem steganografic poate fi măsurat folosind mai multe proprietăți. Cea mai importanta proprietate este nedetectabilitatea (imperceptibilitatea), statistică a datelor care arată cât de dificil este să determine existența unui mesaj ascuns. Alta măsură asociată este capacitatea stegaongrafica, care reprezintă cantitatea maximă de informație care poate fi în siguranță inclusa într-un mediu, fară a putea fi detectabilă. Cea din urma proprietate, robustețea, care se refera la cât de bine rezista sistemele steganografice la extragerea datelor ascunse.

## Prezentarea temei

Creșterea rapidă în dezvoltarea tehnologiei moderne de comunicații a făcut transmiterea datelor mai ușoară și mai rapidă. Cu toate acestea, acest lucru a făcut ca datele transmise să fie mai ușor de copiat, modificat sau distrus de către utilizatorii neautorizați sau atacatori. Astfel, protejarea secretă a datelor a devenit o problemă critică. Criptarea datelor și ascunderea datelor sunt două tehnici majore de securitate a informațiilor pentru a menține protecția datelor.

Steganografia imaginii este este cea mai comună și mai des folosită tehnică pe scară largă prin compararea cu alte metode de steganografie. Această popularitate se datorează faptului că imaginile au o cantitate mare de date redundante care pot fi folosite pentru a ascunde cu ușurință date secrete și pentru că imaginile iau în considerare avantajul puterii limitate a sistemului vizual uman. În steganografia imaginii, imaginea orignala este numită imagine copertă, pe când, imaginea stego este cea care rezultă în urmă incorporării datelor în interiorul imaginii originale. Imaginea originală și stego imaginea ar trebui să fie asemănătoare, așa că vă fi greu pentru o persoană normală să cunoască diferență dintre cele două. (2)

Există multe abordări steganografice pentru ascunderea datelor. Cea mai faimoasa abordare steganografica este metodă bitului celui mai nesemificativ(LSB), unde LSB se referă la ultimul bit sau bitul cel mai din dreapta dintr-un număr binar. Această abordare înlocuiește ultimii/ultimul bit al unui octet al imaginii originale cu biții de date ai mesajului ascuns. Metodă LSB este ușoară și simplu de calculat, dar capacitate acesteia este scăzută. Simplă abordare a metodei bitului celui mai nesemnificativ nu este nici robustă din cauza ușurinței de a prelua mesajul secret prin preluare ultimilor biți al fiecărui octet. (3)

## Prezentarea obiectivelor

În cadrul acestei lucrări despre steganografie în care am utilizat metoda bitului celui mai nesemnificativ, se dorește urmărirea următoarelor obiective:

1.     Studierea teoriei și principiilor steganografiei: înțelegerea conceptelor fundamentale, înțelegerea metodei bitului celui mai nesemnificativ, modul de funcționare și impactul asupra imaginilor.

2.     Dezvoltarea unei aplicații software care să permită ascunderea și extragerea mesajelor secrete în cadrul unor imagini, folosind metoda prezentată anterior. Aplicația ar trebui să ofere și o interfață utilizator intuitivă și ușor de folosit.

3.     Evaluarea impactului și relevanței metodei: analiză impactului metodei bitului celui mai nesemnificativ în ceea ce privește eficientă, performanță și posibilele aplicații în societatea actuală prin testarea diferențelor între imaginea originală și imaginea purtătoare de mesaj ascuns prin cadrul metodei PSNR.

Realizări similare ale steganografiei:

            În procesul de dezvoltare al proiectului am consultat și studiat mai multe realizări în domeniul steganografiei, care au condus la o mai bună înțelegere a subiectului. Astfel, câteva dintre aceste cercetări includ:

1.     Proiectul „Image Steganography Method for Securing Multiple Images using LSB – GA”: În cadrul acestui studiu sunt prezentate două tehnici de steganografie utilizate pentru ascunderea datelor în imagini, GA(Genetic Algorithm) și cea a celui mai nesemnificativ bit(LSB). (4)

2.     Articolul „ An efficient steganographic technique for hiding dată”: Acest articol exploreza o tehnică inovatoare de steganografie bazată pe metodă celui mai nesemnificativ bit și propune o abordare eficientă pentru ascunderea mesajelor secrete în imagini. (5)

3.     Lucrarea „A New Image Steganography Tehnique Based on Bit Plane Complexity Segmentation” publicată în IEEEXplore. Această lucrare prezintă o tehnică inovatoare de steganografie care se bazează pe segmentarea complexității planului de biți al imaginii. (6)

## Terminologii ale steganografiei imaginii

Terminologiile steganografiei imaginii sunt următoarele:

·       Imaginea de copertă: imaginea originală care este folosită ca suport pentru informații ascunse.

·       Mesajul: Informațiile care sunt folosite pentru a fi ascunse în imagine. Mesajul ar putea fi un simplu text sau o altă imagine.

·       Stego-imaginea: După încorporarea mesajului în imaginea de coperta, aceasta poartă numele de stego-imagine.

·       Stego-cheie: O cheie ce este folosită pentru încorporarea sau extragerea mesajelor din imaginile de coperta și stego-imaginile.

În general, steganografia imaginii este o metodă de ascundere a informațiilor în imaginea de copertă și generează o stego-imagine. Această stego-imagine este trimisă unei părți prin intermediul unui mediu cunoscut, o persoană terță nu știe de existența mesajului ascuns. După primirea mesajului ascuns în stego-imagine, mesajul poate fi extras cu ajutorul stego-cheii (în funcție de algoritmul de încorporare). Schemă de baza a unei steganografii de imagine este prezentată în *Figure 1.* Algoritmul de încorporare a textului are nevoie de imaginea de copertă și textul pentru procedura de încorporare. Ieșirea algoritmului de încorporare este o stego-imagine, care pur și simplu poate fi transmisă la algoritmul de extragere, unde se va afișa mesajul ascuns. (4)

Diagram

Description automatically generated

Figure 1

# Prezentarea tehnică a etapei de implementare

Imaginile sunt ideale pentru ascunderea informațiilor datorită cantității mare de spațiu redundant care este creat în stocarea imaginilor. Deoarece acest lucru poate fi făcut în mai multe moduri, steganografia imaginii este studiată și una dintre metodele care se poate folosi pentru reprezentarea acestei ipoteze este metodă celui mai nesemnificativ bit (LSB), tehnică în care bitul cel mai nesemnificativ al fiecărui byte este modificat pentru a formă șirul de biți reprezentând textul încorporat.

Alterarea tehnicii LSB va cauza doar modificări minore în culoarea imaginii, această schimbare nefiind vizibilă de ochiul uman. În timp ce această tehnică merge foarte bine pentru imaginile color de 24 de biți, steganografia nu are un succes la fel de bun atunci când se folosește o culoare pe 8 biți a imaginii, din cauza limitării în variația culorilor. În timpul acestei implementări, un mesaj text este ascuns în imagine. Aceste informații ascunse pot fi descoperite doar printr-o tehnică de decodare adecvată. (8)

## Algoritm folosit pentru ascunderea mesajului ascuns

Când se aplică metoda LSB la fiecare octect al unei imagini pe 24 de biți, trei biți pot fi codificați la fiecare pixel.

Pixeli: (00110010 10011001 11001000)

(00101011 01011100 11001001)

(11011010 01100111 10111001)

a: 01100001

Rezultat: (00110010 10011001 11001001)

(00101010 01011100 11001001)

(11011010 01100111 10111001)

Inserarea metodei LSB este ușor de aplicat, dar în acelși timp, ușor de atacat. În ziua de astăzi, steganografia, este încorporată in tehnologia digitală.

**A.**    **Pașii algoritmul de criptare folosit în cadrul acestui proiect:**

1)     Mai întâi convertim mesajul secret în cod ASCII, luând fiecare caracter în parte.

2)     După ce am obținut codul ascii al fiecărui caracter, convertim codul ASCII în binar, astefel încât să obținem un flux de 8 biți per caracter.

3)     Pasul următor constă în includerea câte unui caracter pe rând, în image, după ce imaginea este și ea procesată după cum urmează.

4)     Se copiază imaginea originală, se extrage fiecare pixel, obțînându-se pentru fiecare setul de culori.

5)     Cu ajutorul funcțiilor din cadrul bibliotecilor puse la dispoziție, culoarea fiecărui pixel este tranformată în spațiul de culori RGB, unde fiecare componente va fi reprezentată în binar, tot pe 8 biți, pentru a se putea realiza ascunderea mesajului secret.

6)     În acest pas, regula generală de ascundere a mesajului este următoarea: în cadrul fiecărei componente R, G, B al unui pixel, înlocuim ultimul bit, al optulea, cu fiecare bit, luați în ordine consecutivă,  al unui caracter din mesajul ascuns pe care dorim să îl introducem. Astfel, pentru a ascunde un caracter scris în binar vor fi necesari 3 biți din cadrul unei imagini, astfel încât valorea ultimului bit din cadrul componentei B, al celui de-al treilea pixel va fi folosit ca metodă de oprire sau continuare a criptării.

7)     Din moment ce componentele fiecărui pixel au fost modificate și s-a realizat ascunderea mesajului secret, se folosesc metode inverse celor prezentate anterior pentru a recrea imaginea inițială, dar modificată, astfel:  prin combinarea valorilor R, G și B al fiecărui pixel, se va obține o culoare, ulterior, suma acestora va formă imaginea modificată.

**B.**    **Pașii algoritmului de decriptare:**

1)     Se descompune imaginea modificată în pixeli, fiecărei pixel fiind caracterizat de două coordonate, x și y, și o culoare.

2)     Din fiecare pixeli, culoarea este tranformată în spațiul de culori de R, G, B iar pentru fiecare culoare se face conversia în binar.

3)     Ulterior, sunt luați pe rând, câte 3 pixeli din care se va extrage câte un caratcer din mesajul modificat până se ajunge la valoarea de stop „0”, astfel: se extrage ultimul bit din cadrul fiecărei componete al unui pixel, până se ajunge la 8 biți. Acești 8 biți reprezintă codul ASCII al unui caracter, iar al noulea bit este folosit că indicator de stop. Dacă al noulea bit are valorea „1”, atunci decriptarea va continuă, în sensul că mai sunt caractere ascunse, iar dacă valoarea este „0”, decriptarea se va opri.

## Biblioteci utilizate in cadrul proiectului

În cadrul acestui proiect, am beneficiat de o diversitate vastă de biblioteci software care au ajutat la o dezvoltare facilă și complexă a acestui experiment. Prin intermediul acestor biblioteci, am reușit să implementez și să dezvolt funcționalități complexe în mod eficient, având că rezultat un nivel superior de performanță. În continuare, voi prezența o lista a principalelor biblioteci pe care le-mă utilizat în cadrul acestui proiect:

***1.***     ***Color:***

Biblioteca „Color” oferă funcționalități pentru lucrul cu culori. Această biblioteca permite manipularea, crearea și transformarea culorilor în diferite formate, precum RGB și HSL. De exemplu, am utilizat metodele din această biblioteca pentru a obține componente individuale ale unei culori (roșu, verde și albastru), pentru a putea ascunde mesajul text și metode pentru a combină culorile, pentru a obține imaginea modificată.

***2.***     ***BufferedImage:***

Biblioteca „BufferedImage” este utilizată pentru manipularea imaginilor în Java. Aceasta ne pune la dispoziție o multitudine de funcții pentru citirea și scrierea pixelilor, redimensoinarea și aplicarea de filtre, de aceea rolul ei în acest proiect a fost de a copia imaginea originală într-un „bufferedImage” pentru a putea lucra mai ușor cu imaginea.

***3.***     ***File:***

Biblioteca „File” oferă funcționalități pentru lucrul cu fișiere și directoare. De exemplu, cu ajutorul acestei biblioteci, putem crea, citi, accesa și manipula fișiere și directoare din sistemul de fișiere al calculatorului, lucru ce mi-a permis alegerea imaginii pe care doresc să aplic algoritmul bitului celui nesemnificativ pentru a putea ascunde mesajul dorit de mine.

***4.***     ***IOException:***

„IOException” este o clasă din biblioteca standard a limbajului Java care se ocupă de tratarea excepțiilor pentru operații de intrare/ieșire. Această clasa a fost utilizată pentru tratarea erorilor și situațiilor deosebite care ar fi putut apărea în timpul citirii sau scrierii unor fișiere.

***5.***     ***ArrayList:***

„Array List” este o clasă din biblioteca standard a limbajului Java care implementează o lista dinamică. Această biblioteca permite stocarea și manipularea unui număr variabile de obiecte, ceea ce a fost un lucru benefic pentru o gestionare și manipulare mai rapidă în cadrul proiectului.

***6.ImageIO:***

Biblioteca „ImageIO” oferă funcționalități pentru citirea și scrierea imaginilor în diferite formate. În cadrul proiectului, a fost utilizată la salvarea imaginii modificate cu ajutorul algoritmului prezentat.

***7.JfileChooser:***

Biblioteca „JfileChooser” oferă o modalitate convenabilă prin care utilizatorul poate selecta fișiere sau directoare din sistemul de fișiere.

***8.WritableRaster:***

„WritableRaster” este o biblioteca standard în Java care permite accesul și modificarea directă a pixelilor unei imagini și este adesea folosită împreună cu biblioteca „BufferedImage” pentru o mai bună manipulare și efectuare a operațiilor de prelucrare a pixelilor pe imagini.

# Prezentarea modului de utilizare a proiectului

Pentru realizarea proiectului de steganografie bazat pe metodă celui mai nesemnificativ bit am folosit că mediu de dezvoltare Eclipse, limbajul utilizat fiind Java. Pentru a utiliza acest proiect, utilizatorul trebuie să urmeze următorii pași simpli și intuitivi:

1.     Proiectul începe prin rularea fișierului intitulat „MainPage” din cadrul proiectului care va porni și încărca apariția implementării grafice ce facilitează o folosire facilă pentru utilizator:

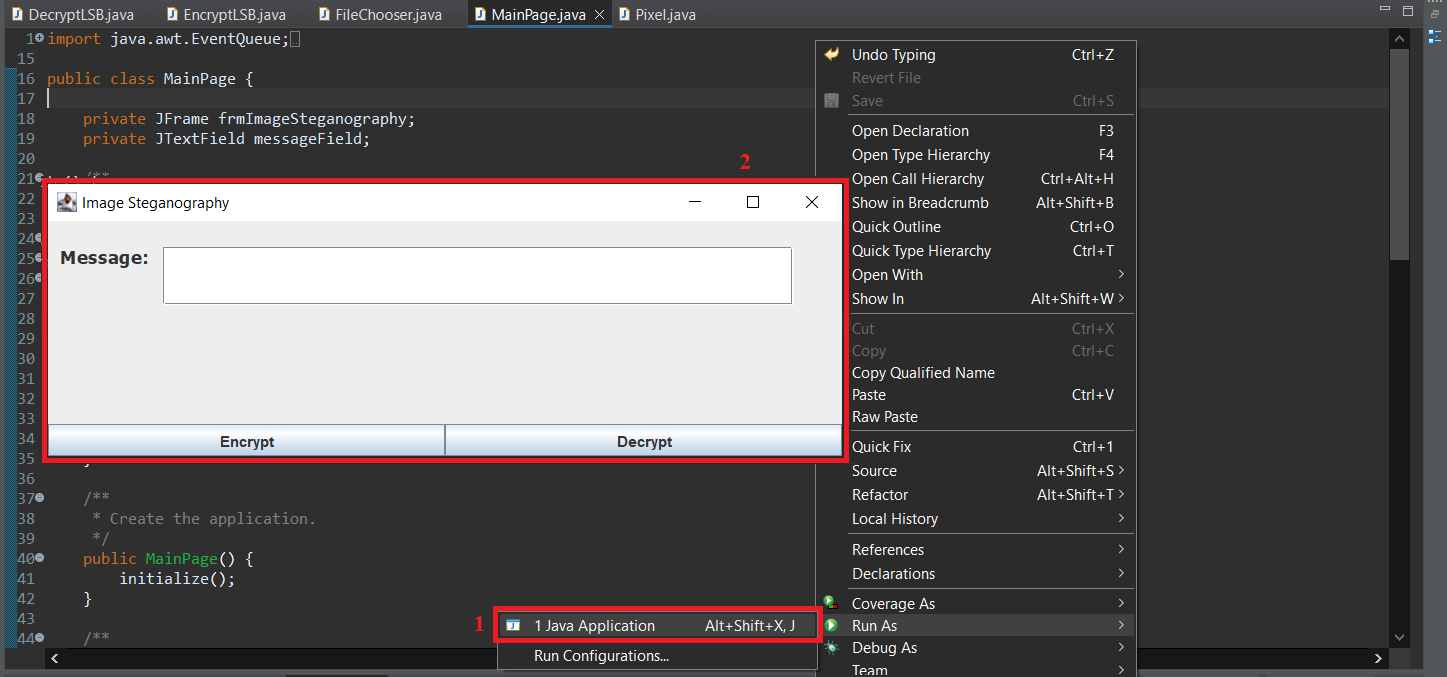


Figure 2

2. Următorul pas este introducere mesajului pe care dorim să-l ascundem in caseta pusă la dispozite din dreapta cuvântului „Message”:

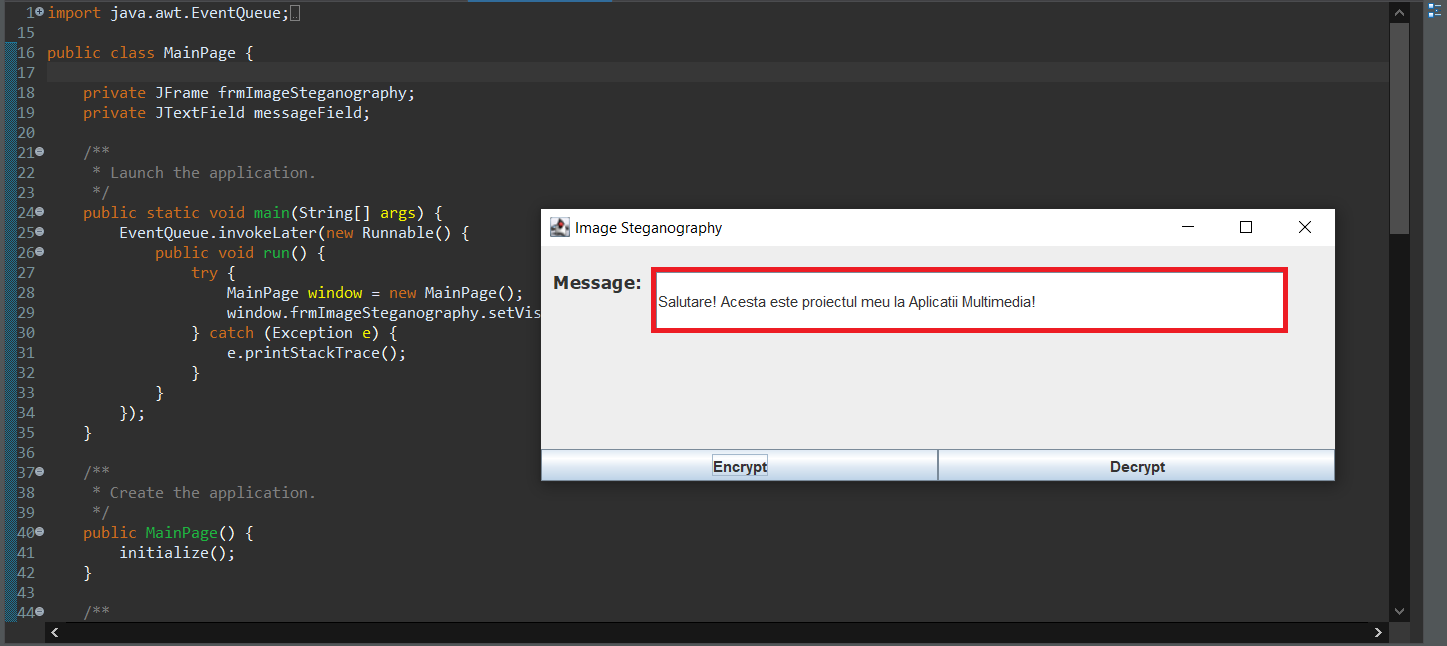


Figure 3

3. Ulterior, după ce textul a fost introdus, se apasă pe butonul „Encrypt” care va deschide o nouă fereastră cu sistemul de fișiere din calculatorul propriu. Se va selecta imaginea în care doriți să ascundeți mesajul ascuns și se apasă pe butonul intitulat „Open”.

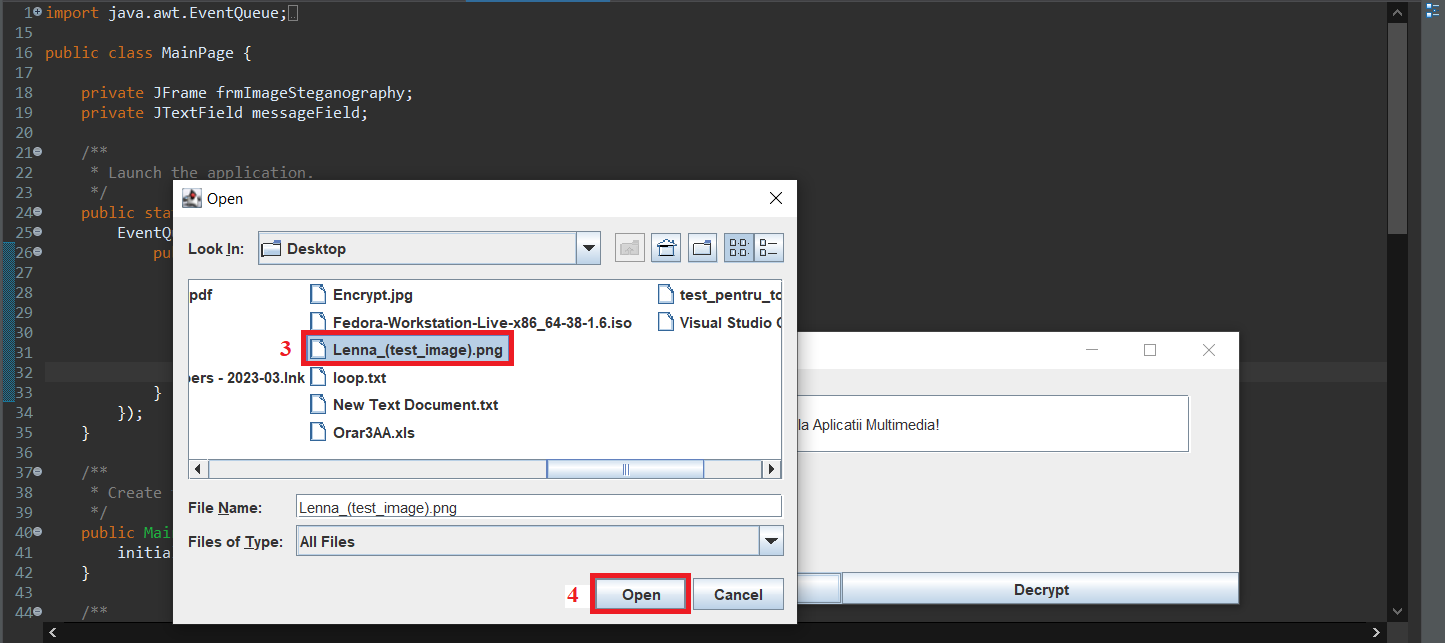


Figure 4

4. Ultimul pas reprezinta decriptarea imaginiii, prin apăsarea butonului „Decrypt”, rezultatul fiind afișat în consolă:

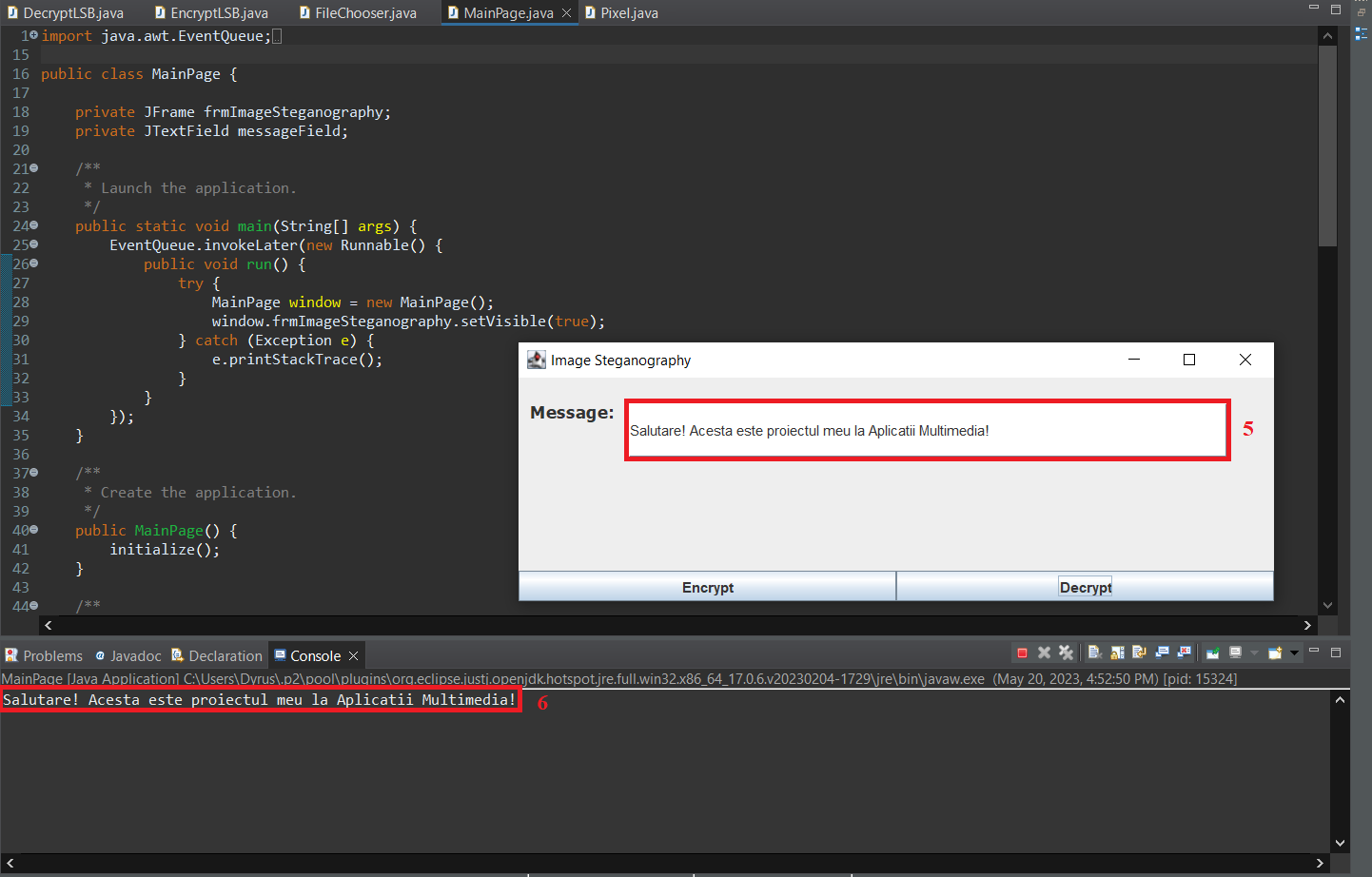


Figure 5

# Concluzii

Proiectul de steganografie bazat pe metoda celui mai nesemnificativ bit a atins obiectivele propuse, de pe urma cărora se pot observa câteva aspecte relevante. Astfel, am observat următoarele concluzii:

1. Proiectul a atins obiectivul principal, acela de a ascunde un mesaj secret în interiorul unei imagini prin utilizarea metodei bitului celui mai nesemnificativ. Acest lucru s-a realizat prin modificarea ultimului bit al fiecărei componente de culori din spațiul RGB al pixelilor imaginii originale.
2. Metoda celui mai nesemnificativ bit reprezintă o modalitate eficientă de a proteja și trimite informații secrete într-un mod aparent inofensiv. Fiind aproape imposibil de detectat diferențele dintre imaginea originală și cea purtătoare de către ochiul uman, aplicația dezvoltată oferă o soluție practică și ușor de utilizat pentru a ascunde informații în imagini.
3. Din punctul de vedere al performanței și eficienței, am realizat 3 teste între imaginea originală și cea purtătoare pentru a observa în ce proporție diferă cele două imagini. Rezultatul este exprimat în procente, iar metodă folosită pentru aceste teste este Peak Signal-to-Noise Ratio (PSNR), o metodă care compară imaginea originală cu cea modificată și oferă o măsură a calității reconstrucției. Am atașat trei imagini cu rezultatele obținute, fiecare test bazându-se pe diferența unei anumite culori, în cazul de față acestea fiind roșu, verde și albastru, iar diferențele obținute sunt de 0.02%, după cum urmează:

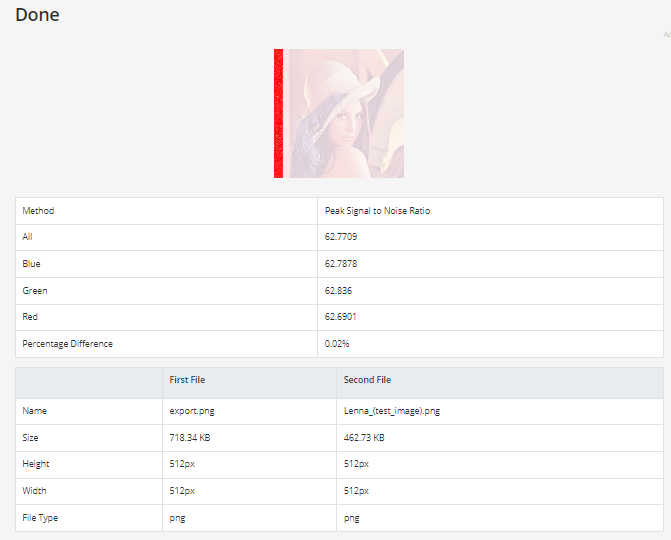


Figure 6

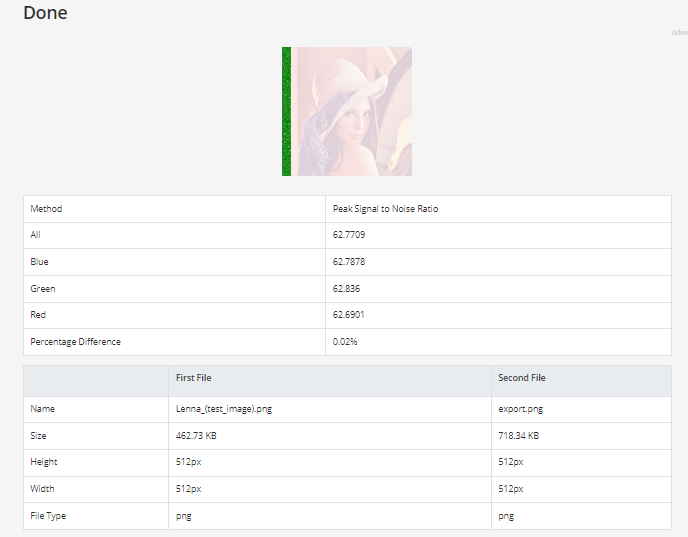


Figure 7

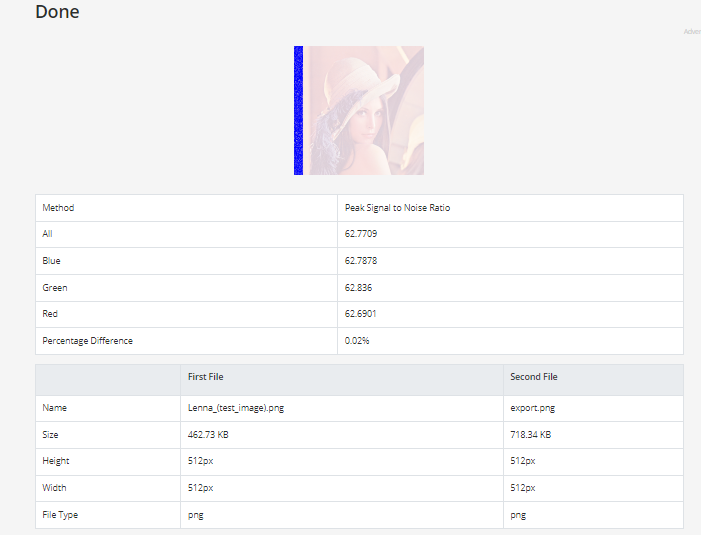


Figure 8

# Bibliografie

1. *Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique .* **SHRIKANT S. KHAIRE, DR. SANJAY L. NALBALWAR.** 2010, International Journal of Engineering Science and Technology, p. 9.

2. *Image Steganography Techniques: An Overview.* **Nagham Hamid, Abid Yahya , R. Badlishah Ahmad , Osamah M. Al-Qershi.** 2012, International Journal of Computer Science and Security (IJCSS), p. 20.

3. *A Survey of Image Steganography Techniques.* **Hussain, Mehdi Hussain and Mureed.** 2013, International Journal of Advanced Science and Technology, p. 13.

4. **Swain, Gandharba.** *Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities.* s.l. : Information Science Reference, 2019. 9781522575160.

5. **Samagh, Randeepika.** *Data Hiding using Image Steganography and LSB Substitution.* s.l. : LAP Lambert Academic Publishing, 2019. 987-659-95957-8.

6. *IMAGE STEGANOGRAPHY USING LSB ALGORITHM.* **Avni Aggarwal, Arpit Sangal, Aditya Varshney.** 2019, International Journal of Information Sciences and Application (IJISA), p. 5.

7. *An efficient steganographic technique for hiding data.* **Mamdouh, Dalia Nashat and Loay.** 2019, Nashat and Mamdouh Journal of the Egyptian Mathematical Society, p. 14.

8. *Image Steganography Method for Securing Multiple.* **Palanichamy Naveen, R Jayaraghavi.** 2022, Research Square, p. 20.