



UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI
TEHNOLOGIE POLITEHNICA BUCUREȘTI
FACULTATEA DE ȘTIINȚE APLICATE



Programul de studii:
Teoria Codării și Stocării Informației

Algoritm de recunoaștere facială

Disciplină: Proiectarea traficului informațional în rețelele
de calculatoare

STUDENT

Becheru Alexandru

București
2025

Cuprins

Introducere	1
Analiza soluțiilor	2
Proiectarea și implementarea soluției	3
Concluzie	7
Bibliografie	8

Introducere

Recunoașterea facială este o tehnologie emergentă care transformă modul în care interacționăm cu lumea digitală. Utilizată în diverse domenii, de la securitate și sănătate până la marketing și divertisment, recunoașterea facială implică utilizarea algoritmilor pentru identificarea și verificarea identității unei persoane pe baza trăsăturilor faciale. În acest proiect, vom explora principalele metode și tehnici utilizate în recunoașterea facială, precum și aplicațiile și provocările acesteia.

Algoritmii de recunoaștere facială reprezintă un domeniu fascinant la intersecția dintre inteligența artificială, procesarea imaginilor și biometrie. Acești algoritmi permit calculatoarelor să identifice sau să verifice identitatea unei persoane analizând caracteristicile unice ale feței. De la filmele SF la utilizări practice în viața cotidiană, recunoașterea facială a devenit o realitate omniprezentă.

Recunoașterea facială constă în preluarea unei imagini a unei fețe, prelucrarea acesteia și compararea datelor returnate cu o bază de date preexistentă. Algoritmii examinează anumite aspecte ale feței, cum ar fi distanța dintre ochi, forma nasului, lungimea maxilarului și curbele feței. Pentru a învăța și a recunoaște modelele unice ale fiecărei fețe, algoritmi moderni utilizează rețele neuronale profunde.

Procesul implică mai multe etape: detectarea feței într-o imagine sau video, analiza trăsăturilor faciale și compararea acestora cu o bază de date. Printre metodele utilizate se numără algoritmi tradiționali, cum ar fi Viola-Jones pentru detectarea feței, și soluții avansate bazate pe rețele neuronale profunde, precum FaceNet sau DeepFace, care oferă rezultate de o acuratețe impresionantă.

Una dintre cele mai răspândite aplicații pentru recunoașterea facială este securitatea. Tehnologia este utilizată pentru aplicații, precum: deblocarea dispozitivelor mobile, restricționarea accesului în clădiri, monitorizarea zonelor publice etc.. În domeniul financiar, aceasta este utilizată pentru autentificarea tranzacțiilor și reducerea riscului de fraudă. În plus, spitalele și unitățile medicale folosesc această tehnologie pentru a îmbunătăți îngrijirea pacienților și pentru a localiza persoanele dispărute. În marketing, recunoașterea facială permite întreprinderilor să evalueze reacțiile emoționale ale clienților la produse și servicii.

În ciuda avantajelor clare, recunoașterea facială generează preocupări etice și juridice. Una dintre principalele preocupări este legată de confidențialitatea datelor și de supravegherea invazivă (ex. cazurile mediatizate despre companiile Hik-Vision și Dahua). Există posibilitatea ca aceste tehnologii să fie exploatare, punând în pericol libertatea individuală. De asemenea, s-a descoperit că unele sisteme au o precizie scăzută pentru anumite grupuri etnice, ceea ce poate duce la prejudecăți neintenționate.

Analiza soluțiilor

Biometria, este un termen compus din cuvintele grecești “bios”(viață) și “metrikos” (măsură), ce se referă la un ansamblu de metode și tehnici automate, utilizate pentru identificarea unei persoane folosind diverse caracteristici biometrice, precum geometria palmelor, amprenta digitală, irisul, retina, geometria feței sau caracteristici comportamentale, precum timbrul vocal, configurarea ADN-ului, structura scrisului de mână, dinamica tastării. Este bine cunoscut, faptul că unele dintre aceste caracteristici biometrice, cum ar fi amprentele digitale sau irisul, pot identifica în mod unic o persoană. Având în vedere această unicitate, datele biometrice pot fi utilizate pentru dezvoltarea și implementarea tehnologiilor, echipamentelor și sistemelor care permit o identificare cu performanțe semnificativ îmbunătățite față de cele existente.

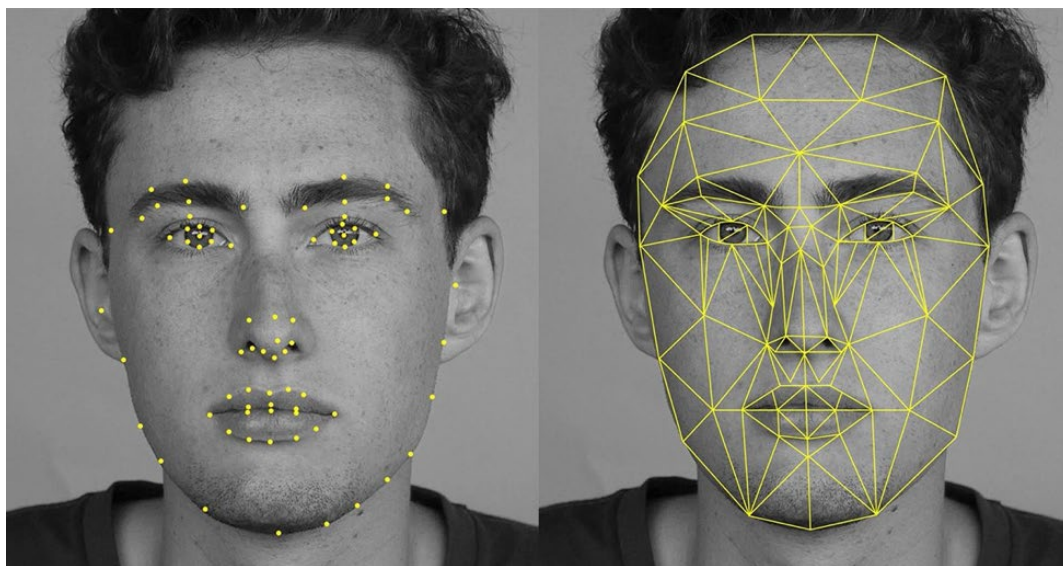


Fig. 1.1 – Algoritm de recunoaștere facială

Implementarea cu succes a unui sistem de recunoaștere depinde de selectarea celui mai potrivit sistem de recunoaștere, astfel încât să se ofere o soluție unică, personalizată în conformitate cu nivelul de securitate impus. Tehnologia biometrică, are proprietatea de a realiza conexiunea dintre individ și acțiunea sau tranzacția efectuată, oferind avantajul prevenirii utilizării de către persoane neautorizate și eliminând posibile fraude în sistem.

Implementarea unui sistem de verificare este mai simplă decât cea a unui sistem de recunoaștere a identității. Într-un sistem de verificare, se autentifică identitatea pretinsă a unei persoane, prin comparația trăsăturilor biologice specifice, furnizate de acesta într-un anumit moment, cu trăsăturile memorate anterior în sistem și asociate identității pretinse de persoană.

În contrast cu sistemul de verificare, sistemul de recunoaștere are o procedură mai complexă, unde trăsăturile biometrice furnizate de o persoană sunt comparate cu măsurile tuturor trăsăturilor biometrice similare stocate într-o bază de date sau într-o rețea neuronală.

De asemenea, recunoașterea irisului este o metodă avansată și automatizată, de identificare biometrică, care se bazează pe tehnici matematice, pentru a recunoaște și analiza modelele din imagini sau materiale video, ale unuia sau ambilor iriși ai ochilor unei persoane. Aceste modele complexe ale irisului, sunt unice pentru fiecare individ, sunt stabile în timp și pot fi observate de la o anumită distanță. Utilizând algoritmi specializați, această metodă permite extragerea și compararea caracteristicilor specifice alea irisului, facilitând identificarea precisă și securizată a persoanelor în cauză.

Proiectarea și implementarea soluției

Metoda propusă utilizează tehnologii moderne precum OpenCV și MediaPipe pentru a aborda dificultatea detectării automate a fețelor umane din fotografii statice. Acest sistem este destinat să ofere o metodă rapidă, eficientă și avantajoasă pentru localizarea trăsăturilor faciale într-o serie de medii vizuale.

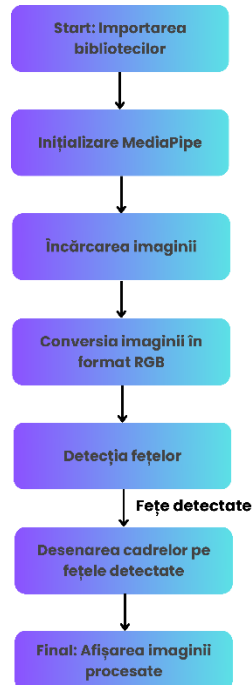


Fig. 2.1. – Diagramă Flux

Scopul principal este asigurarea funcționării programului de recunoaștere facială, aceasta fiind prima condiție în asigurarea a numeroase aplicații uzuale, inclusiv:

- **Securitatea biometrică:** Utilizează recunoașterea facială în scopul autentificării.
- **Asistența medicală:** Examinarea expresiilor faciale pentru a evalua emoțiile sau starea de sănătate.
- **Interacțiunea om-mașină:** Controlul dispozitivelor bazat pe mișcările și expresiile faciale
- **Divertisment și realitate augmentată:** Integrarea elementelor digitale în funcție de poziția feței utilizatorului.

Limitări în detecția facială:

- Sunt prevăzute mai multe condiții de iluminare.
- Diferențe în poziționarea feței (unghiuri diferite).
- Detectarea multiplă a fețelor în fotografii aglomerate.

Sistemul abordează aceste provocări prin utilizarea simultană a **MediaPipe**, o platformă optimizată de procesare vizuală, cu **OpenCV**, un pachet bine cunoscut de procesare a imaginilor. Spre deosebire de crearea de la zero a unui model de identificare a feței, soluția propusă utilizează algoritmi pre-antrenați, ceea ce prezintă avantaje importante:

- **Reducerea complexității de dezvoltare:** Utilizarea soluțiilor existente economisește timp și resurse.
- **Performanță ridicată:** **MediaPipe** detectează obiectele rapid și precis, ceea ce îl face ideal pentru implementările în timp real.
- **Accesibilitate:** Tehnologiile utilizate sunt documentate și disponibile open source.

Fluxul conceptual al detectării fețelor:

Metoda propusă are o abordare structurată, în trei componente majore: colectarea datelor, prelucrarea imaginilor și generarea rezultatelor. Acest flux optimizează detecția fețelor prin integrarea tehnicilor de procesare a imaginilor cu modele de învățare automată pre-antrenate.

1. Prelucrarea datelor de intrare:

Etapa inițială constă în accesarea datelor vizuale de intrare, care pot fi imagini statice salvate local sau obținute din surse externe.

Încărcarea imaginii: Pentru a introduce în sistem o imagine care cuprinde una sau mai multe fețe, utilizatorul specifică locația fișierului.

Validarea formatului: Sistemul se asigură că imaginea respectă formatele acceptate (JPEG, PNG). Această validare previne erorile de procesare ulterioară.

Pregătirea datelor pentru prelucrare: Imaginea este plasată în memorie și pregătită pentru utilizare de către algoritmi de detectare.

2. Procesarea imaginii:

A doua etapă reprezintă partea centrală funcțională a sistemului, în care datele brute sunt analizate pentru a identifica fețele. Aceasta include:

- **Conversia imaginii în format RGB:** deoarece algoritmi **MediaPipe** funcționează optim cu imagini în format **RGB** (în loc de BGR, utilizat de OpenCV), această conversie este esențială. Aceasta face ca imaginea să fie compatibilă cu motorul de detectare a fețelor.

- **Analiza cu MediaPipe Face Detection:**

- Programul MediaPipe analizează pixelii imaginii cu ajutorul unui model de rețea neuronală pre-antrenat.

- Detecția se bazează pe anumiți factori precum simetria caracteristicilor și curbele faciale pentru a identifica zonele care prezintă caracteristici similare fețelor umane.

- Fiecărei fețe detectate i se atribuie un „bounding box” (o zonă dreptunghiulară) și un scor de încredere care indică probabilitatea ca zona să conțină o față.

3. Generarea și vizualizarea rezultatelor:

Ultima etapă transformă informațiile procesate într-un rezultat vizibil pentru utilizator. Acest proces include:

- **Desenarea zonelor detectate:** OpenCV este utilizat pentru a evidenția fețele detectate pe imagine. De obicei, sunt utilizate cadre dreptunghiulare sau alte marcaje grafice (contururi sau puncte) pentru a indica zonele detectate.

- **Afișarea rezultatului final:** Imaginea procesată este afișată într-o fereastră dedicată sau salvată pentru utilizare ulterioară. Acest pas permite utilizatorului să verifice vizual performanța sistemului.

Implementarea Practică a Detectării Fețelor cu OpenCV și MediaPipe:

1. Configurarea și inițializarea componentei:

- **OpenCV (cv2):** Folosită pentru manipularea imaginii, de la încărcare la afișarea rezultatelor.

- **MediaPipe (mp.solutions.face_detection):** Un API optimizat pentru detectarea trăsăturilor faciale, care include modele pre-antrenate.

Inițializarea componentei MediaPipe pentru detectarea fețelor:

```
mp_face_detection = mp.solutions.face_detection
mp_drawing = mp.solutions.drawing_utils
```

- **mp.solutions.face_detection:** Configurează detectorul facial cu un prag de încredere minim (`min_detection_confidence`).
- **mp.solutions.drawing_utils:** Oferă funcționalități pentru a desena grafic fețele detectate.

2. Încărcarea și pregătirea imaginii:

Imaginea de intrare este încărcată și pregătită pentru analiză. Acest pas include conversia imaginii în format RGB:

```
image_path = r'C:\Users\alexa\PycharmProjects\PythonProject4\Images\.....jpg'
image = cv2.imread(image_path)
rgb_image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
```

- **cv2.imread():** Încarcă imaginea dintr-o locație specificată.
- **cv2.cvtColor():** Transformă imaginea din format BGR (folosit implicit de OpenCV) în RGB, necesar pentru MediaPipe.

3. Detectarea fețelor:

Componenta MediaPipe procesează imaginea și identifică fețele, returnând coordonatele zonei detectate:

```
with mp_face_detection.FaceDetection(min_detection_confidence=0.2) as face_detection:
    results = face_detection.process(rgb_image)
```

- **FaceDetection():** Inițializează detectorul, iar parametrul **min_detection_confidence** setează pragul minim de încredere (0.2).
- **face_detection.process(rgb_image):** Analizează imaginea RGB și returnează un obiect **results**, care conține toate detecțiile.

4. Evidențierea fețelor detectate:

Dacă există fețe detectate, acestea sunt marcate grafic pe imagine:

```
if results.detections:
    for detection in results.detections:
        mp_drawing.draw_detection(image, detection)
```

- **results.detections:** Listează toate fețele detectate, fiecare cu coordonate precise și scoruri de încredere.
- **mp_drawing.draw_detection():** Desenează un contur sau un cadru dreptunghiular peste fiecare față detectată.

5. Afișarea rezultatului final:

Rezultatul este afișat într-o fereastră grafică, utilizatorul având opțiunea să închidă programul prin apăsarea unei taste:

```
cv2.imshow('Face Detection', image)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

- **cv2.imshow():** Deschide o fereastră cu imaginea procesată.
- **cv2.waitKey(0):** Așteaptă o comandă de la tastatură înainte de a închide fereastra.
- **cv2.destroyAllWindows():** Închide toate ferestrele deschise de OpenCV.



Fig. 2.2. – Detecția a mai multor fețe apropiate dintr-o imagine



Fig. 2.3. – Detecția unei singure fețe

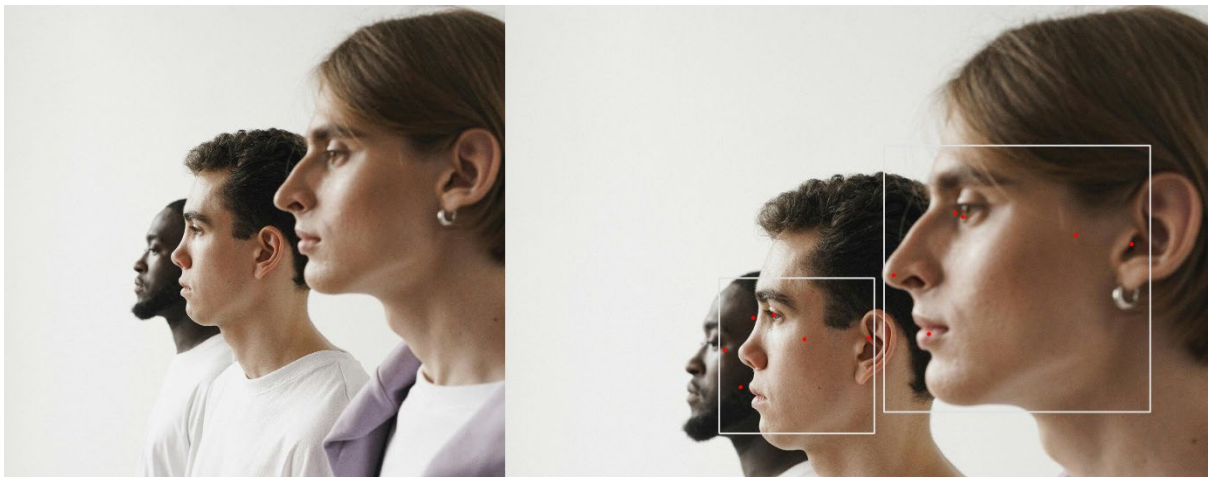


Fig. 2.4. – Detecția fețelor din lateral



Fig. 2.5. – Detecția feței într-o imagine distorsionată de lumină și umbră

Concluzie

Software-ul de recunoaștere facială devine din ce în ce mai popular datorită numeroaselor sale aplicații practice și a potențialului său pentru viitor. Rezultatele obținute cu programul de recunoaștere facială, aflat la stadiul prezent, sunt unele mulțumitoare, raportat la limitările hardware care au fost întâmpinate pe parcurs. Cu toate acestea, reușita cea mai interesantă o reprezintă capacitatea programului de a identifica punctele cheie faciale dintr-o imagine căreia i-au fost aplicate filtre și efecte distorsionate, lucru care adesea se poate întâmpla și în viața reală. Acest lucru indică versatilitatea și capacitatea software-ului de a aborda cu succes și sarcini mult mai complexe decât cele simple/de bază.

Următorul pas îl reprezintă dezvoltarea unui astfel de software, ceea ce creează mai multe posibilități de monetizare și extindere, atât comercializate direct, cât și implementate în soluții complicate care acoperă o gamă largă de nevoi. În continuare, vor fi prezentate principalele domenii și posibilități de valorizare/monetizare, precum și viitoarele oportunități de dezvoltare.

Vânzarea de licențe către întreprinderi și organizații interesate să integreze software-ul în infrastructura lor este o modalitate simplă de monetizare. Clienții pot include întreprinderi din domeniul securității, sănătății, comerțului cu amănuntul sau serviciilor financiare.

O altă abordare este furnizarea de software ca serviciu de abonament, în care clienții plătesc pentru accesul la capacitățile programului prin intermediul unei platforme online. Această abordare vă permite să faceți bani recurenți, atrăgând în același timp un număr mai mare de consumatori.

Adaptarea software-ului la cerințele clienților poate fi o sursă semnificativă de bani. Recunoașterea facială, de exemplu, poate fi utilizată pentru a reglementa accesul la spațiile de lucru, autentificarea sistemelor bancare și monitorizarea proceselor industriale.

Dezvoltarea de soluții hardware-software, cum ar fi sistemele de camere inteligente sau terminalele de acces bazate pe recunoașterea facială, poate spori valoarea de piață a programului și atrage noi clienți.

Totodată, o etapă importantă este optimizarea performanțelor programului prin scăderea erorilor și îmbunătățirea preciziei recunoașterii faciale, în special atunci când este vorba de

diversitate etnică, vârstă sau circumstanțe de iluminare. Implementarea algoritmilor de învățare profundă poate produce rezultate mult mai bune.

Extindeți funcționalitatea software-ului pentru a include tehnologii complementare precum detectarea expresiilor faciale, urmărirea ochilor și integrarea cu alte tipuri de identificare biometrică (amprentă digitală, voce).

Pentru a câștiga încrederea consumatorilor și a partenerilor, sunt necesare o criptare puternică și o stocare sigură a datelor. De asemenea, programul trebuie să respecte normele mondiale, cum ar fi GDPR și CCPA.

Extinderea compatibilității programului cu dispozitivele mobile, sistemele IoT și platformele cloud poate spori atractivitatea acestuia pe piață.

De asemenea, adăugarea de funcții predictive bazate pe inteligență artificială, cum ar fi detectarea comportamentelor anormale sau anticiparea acțiunilor, poate ajuta programul să se remarcă pe piață și să atragă consumatori din sectoare precum siguranța publică sau asistența medicală.

Bibliografie

- [1] https://ai.google.dev/edge/mediapipe/solutions/vision/face_detector/python
- [2] <https://www.pexels.com/photo/women-sitting-jeans-shirt-9385084/>
- [3] <https://www.pexels.com/photo/woman-wearing-black-eyeglasses-1239291/>
- [4] <https://www.pexels.com/photo/photo-of-men-9775895/>
- [5] <https://www.pexels.com/photo/portrait-of-a-man-with-photography-effects-6491250/>
- [6] <https://www.techtarget.com/searchenterpriseai/definition/face-detection>
- [7] <https://www.mdpi.com/2079-9292/10/19/2354>
- [8] <https://medium.com/pythons-gurus/what-is-the-best-face-detector-ab650d8c1225>