Studiu comparativ al metodelor de blurring al imaginior si al eficientei acestora in combaterea recunoasterii faciale

Rizoiu Alexandra-Elena, 343C2

January 9, 2024

1 Introducere

Într-o lume în care algoritmii de recunoaștere facială au devenit din ce în ce mai comuni, un subiect îngrijorător a devenit protejarea vieții private. În acest sens, o arie de studiu relevantă devine găsirea metodelor optime de modificare a imaginilor pentru a atinge acest scop.

În consecință, proiectul de față studiază eficiența a 4 metode de blurring (average, median, gaussian și bilateral) în a ascunde trăsături recognoscibile de modele de ML.

2 Considerente teoretice

Acest studiu compară 4 metode specifice: average, median, gaussian și bilateral filter. Mai jos sunt descrieri ale fiecăreia și cazurile tipice de utilizare. Elementul comun al tuturor este ca presupun ca imaginea blurata este rezultatul unui prouds de convolutie intre "bucăți" din imaginea inițială și o matrice special aleasă numită nucleu.

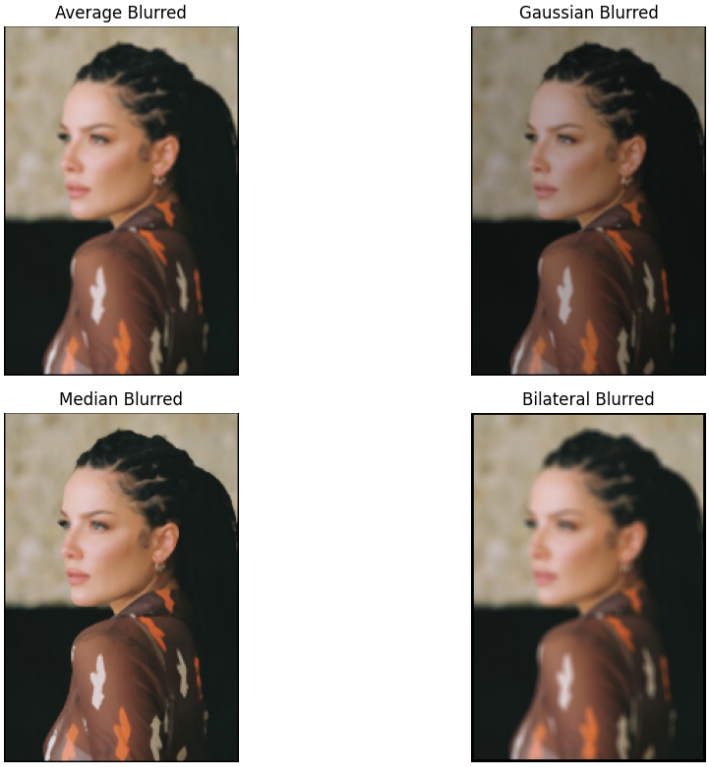

Figure 1: Tehnicile de blur

1. **Average blur:** aplică unui efect de estompare a imaginii prin substituirea fiecărui pixel cu o valoare medie a pixelilor adiacenți. Această tehnică duce la crearea unei umbre uniforme în jurul fiecărui pixel, reducând contrastul și detaliile din imagine. Average blur este una dintre cele mai simple tehnici de blurare și poate fi utilă în diverse situații de prelucrare a imaginilor în care este necesară o reducere generală a detaliilor și a contrastului. Este folosită de obicei pentru a estompa detalii sensibile sau irelevante sau a uniformiza imagini înainte de procesare.

2. **Median blur:** este similar ca mecanism cu average blur, dar folosește mediana în loc de medie. În consecința, elimina anumite valori extreme dintr-o imagine, reducând astfel zgomotul și detaliile nedorite si pastrand contururile. Acesta se folosește in situații similare cu cel mediu, dar dă rezultate mai bune în cazul în care imaginea inițiala are un contrast mare (are mulți pixeli extremi).

3. **Gaussian blur:** este o tehnică de estompare a imaginii folosind o distribuție gaussiană pentru calcularea ponderilor pixelilor dintr-o zonă vecină. Astfel, fiecare pixel adiacent celui pe care îl înlocuim are o contribuție diferită în calcularea valorii noi. Rezultatul este o metodă mai fină de a reduce zgomotul care aplică un filtru uniform care pastreaza detaliile relevante.

4. **Bilateral filter:** este o tehnică de estompare a imaginii care reduce zgomotul și estompează detaliile nedorite menținând în același timp anumite margini clare ale obiectelor din imagine. Acest filtru utilizează două componente principale: o componentă spațială și o componentă de intensitate (valorile pixelilor).

3 Metodă

Metoda folosită în acest studiu este simplă: pornind de la o imagine cu o celebritate, o blurez folosind una dintre cele 4 metode, apoi o uploadez cu ajutorul imgur pentru a o putea da ca parametru unui API pentru google lens. Acesta returnează titlurile rezultatelor obținute, în care caut numele celebrității pentru a vedea dacă o recunoaște. Pentru fiecare metodă țin evidența numărului de aplicări succesive ale acesteia pentru a nu mai fi recognoscibilă, ținând cont și de latura nucleului necesar.

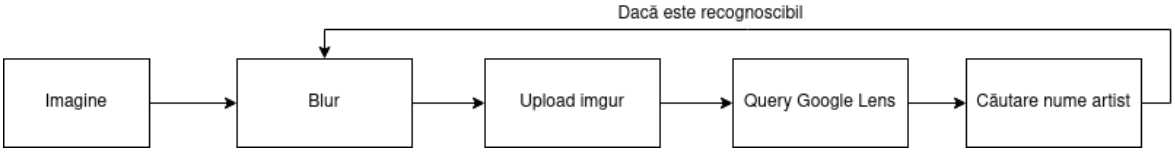

Figure 2: Diagrama care prezintă metoda.

Fiindcă nu toate metodele au aceeași parametri, a trebuit să iau niște decizii aproximativ arbitrare pentru a le putea compara: elementul comun tuturor metodelor este latura nucleului, iar la metodele care au mai mulți parametri aceștia au avut valori statice pe care le-am ales ca valori medii pentru fiecare metodă.

4 Rezultate

Mai jos sunt rezultatele studiului. Menționez ca 10 pe axa verticala este o valoare falsă, în cazul filtrului median. Adevărul este că pentru nucleul de 3 imaginea rămânea recognoscibilă si după 100 de încercări succesive. Concluziile interesante sunt că desi filtrul bilateral este mult mai complex, are acelasi efect in materie de anonimizare ca cel average. De asemenea, am demonstrat folosirea filtrului median ca instrument de blurare care pastrează marginile intacte prin faptul ca are o valoare mare pentru nucleu de 3. Nu in ultimul rand, filtrul gaussian pare ca nu performeaza liniar (un nucleu de 5 functioneaza mai ineficient decat unul de 3, ceea ce e interesant).

La final, concluzia este că pentru anonimizare metodele ideale sunt filtrele agerage si cele bilaterale, dar pentru pastrarea anumitor contururi mai evidente este preferabil un filtru median cu un kernel mai mare.

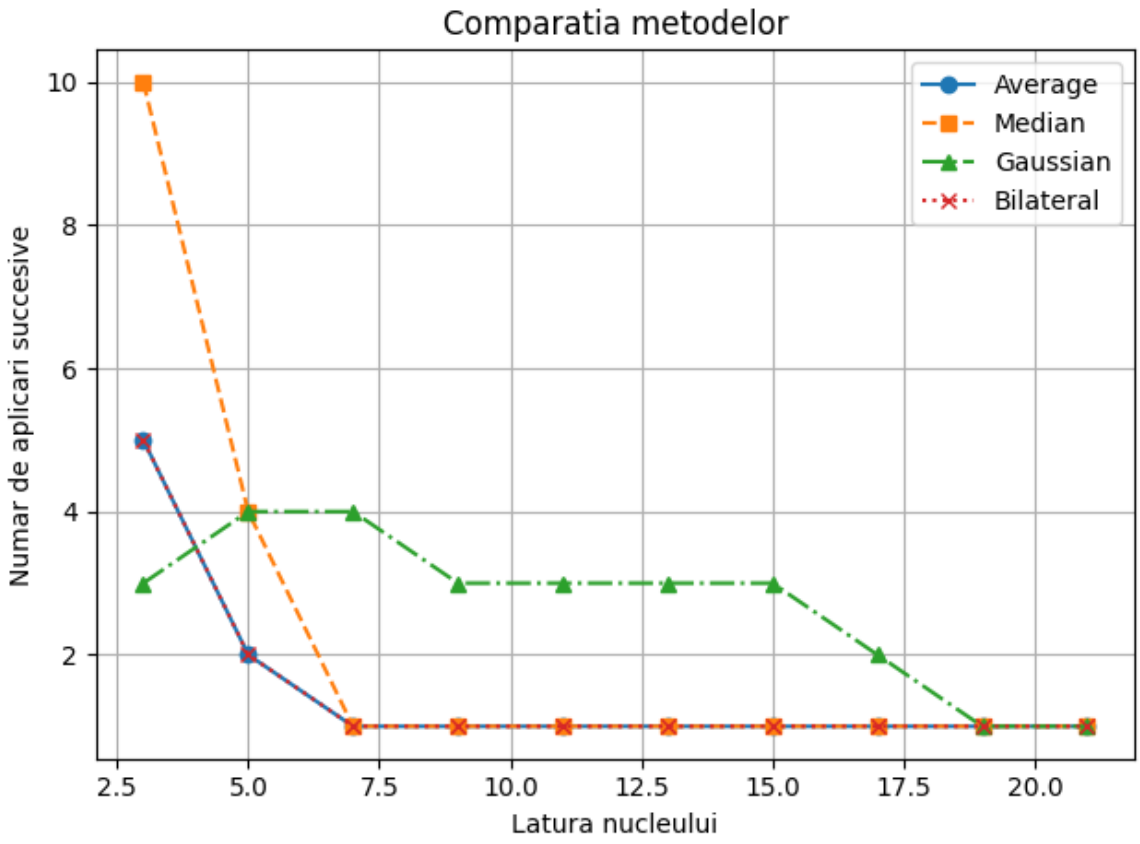

Figure 3: Rezultatele