MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___" _____ 2025

ANALIZA VULNERABILITĂȚILOR ALGORITMILOR DE RECUNOAȘTERE FACIALĂ

Teză de master

Student: _____ **Vechiu Ana-Maria, TI-231M**

Coordonator: _____ **Istrati Daniela, lect. univ., dr**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

Lucrarea de față analizează tehnologia de recunoaștere facială, punând accent pe aplicabilitatea acesteia în diverse domenii, precum securitatea, monitorizarea prezenței în educație și utilizarea în sectorul juridic. Scopul principal al cercetării a fost de a explora algoritmii utilizați în recunoașterea facială, de a analiza vulnerabilitățile și atacurile la care sunt expuși aceștia, precum și măsurile necesare pentru a le contracara.

În cadrul lucrării, au fost examinate tipurile de algoritmi de recunoaștere facială, atât cei care se bazează pe trăsături geometrice ale feței, cât și cei care utilizează învățarea profundă. S-a realizat o comparație între aceștia, evidențiind punctele forte și limitările fiecărei abordări. De asemenea, au fost identificate vulnerabilitățile majore, cum ar fi atacurile de tip spoofing, atacurile adversariale și problemele legate de confidențialitate, care pot afecta performanța și fiabilitatea sistemelor de recunoaștere facială.

Un alt punct important al cercetării a fost analiza prejudecăților introduse în seturile de date utilizate pentru antrenarea algoritmilor, ceea ce poate duce la discriminare și inegalități în performanțele sistemelor. S-au propus soluții pentru reducerea acestor prejudecăți, cum ar fi diversificarea și augmentarea seturilor de date, precum și utilizarea tehnologiilor de criptare și anonimizare a datelor pentru a proteja confidențialitatea utilizatorilor.

În concluzie, recunoașterea facială reprezintă o tehnologie cu un mare potențial, dar care trebuie implementată cu precauție, având în vedere riscurile legate de securitate, etică și protecția datelor. Studiile de caz din educație și domeniul juridic au demonstrat beneficiile acestei tehnologii, dar și necesitatea reglementărilor stricte pentru a asigura utilizarea responsabilă și echitabilă a acesteia. Cercetările viitoare în domeniu ar trebui să se concentreze pe îmbunătățirea acurateței algoritmilor și pe dezvoltarea unor soluții inovative pentru combaterea atacurilor și protejarea drepturilor fundamentale ale persoanelor.

ABSTRACT

This paper analyzes facial recognition technology, focusing on its applicability in various fields such as security, attendance monitoring in education, and its use in the legal sector. The main objective of the research was to explore the algorithms used in facial recognition, analyze the vulnerabilities and attacks to which they are exposed, and propose measures to mitigate them.

The paper examines different types of facial recognition algorithms, including those based on facial geometric features and those utilizing deep learning. A comparison between these approaches was made, highlighting the strengths and limitations of each. Major vulnerabilities, such as spoofing attacks, adversarial attacks, and privacy concerns, were identified as factors that can affect the performance and reliability of facial recognition systems.

Another key aspect of the research was the analysis of biases introduced in the datasets used to train the algorithms, which can lead to discrimination and inequalities in the system's performance. Solutions were proposed to address these biases, such as diversifying and augmenting datasets, as well as employing encryption and data anonymization technologies to protect user privacy.

In conclusion, facial recognition represents a technology with great potential but must be implemented with caution due to the security, ethical, and data protection risks. Case studies from education and the legal sector demonstrated the benefits of this technology, but also highlighted the need for strict regulations to ensure its responsible and equitable use. Future research in this field should focus on improving algorithm accuracy and developing innovative solutions to combat attacks and protect individuals' fundamental rights.

Cuprins

INTRODUCERE

Fața reprezintă o componentă esențială a corpului uman, fiind elementul care ne permite să identificăm rapid o persoană într-un grup numeros. Din perspectiva istorică, fața a fost mereu un simbol al individualității și al identității personale, încă din cele mai vechi civilizații, fiind folosită pentru a distinge oamenii între ei. Datorită caracteristicilor sale unice și variate, fața a devenit una dintre cele mai eficiente și recunoscute metode biometrice.

De-a lungul timpului, domeniul recunoașterii faciale a captat interesul oamenilor de știință și a devenit un standard de referință în recunoașterea umană. În ultimele patru decenii, recunoașterea facială a fost unul dintre cele mai studiate domenii din viziunea computerizată, datorită numeroaselor sale aplicații practice: monitorizarea securității, sistemele automate de supraveghere, identificarea victimelor și a persoanelor dispărute, printre altele.

Acest studiu explorează o gamă extinsă de tehnici utilizate în recunoașterea facială, analizând avantajele și dezavantajele fiecărei metode. În prima parte, sunt prezentate bazele tehnologice ale recunoașterii faciale, fluxul său de lucru standard, contextul de utilizare și provocările întâmpinate, precum și aplicațiile sale potențiale. În continuare, sunt discutate tehnologiile specifice recunoașterii faciale, cu punctele lor forte și limitările aferente. Secțiunea finală analizează oportunitățile viitoare de dezvoltare și implicațiile acestora pentru evoluția domeniului.

Primii pionieri în domeniul recunoașterii faciale au fost Woody Bledsoe, Helen Chan Wolf și Charles Bisson, care au început să exploreze această tehnologie în anii 1964 și 1965, folosind computere pentru a identifica chipurile umane. [1]

Deși proiectul lor a fost finanțat de o agenție de informații secretă, ceea ce a limitat publicarea rezultatelor, s-a descoperit ulterior că munca lor s-a concentrat pe identificarea manuală a unor repere esențiale ale feței, cum ar fi ochii și gura. Aceste puncte de reper erau apoi manipulate matematic de un computer pentru a ajusta variațiile de expunere. După corectarea acestor factori, distanțele dintre reperele faciale erau calculate automat și comparate între imagini pentru a stabili identitatea persoanelor.

Deși eforturile lui Bledsoe, Wolf și Bisson au fost limitate de tehnologia rudimentară a vremii, contribuțiile lor au reprezentat un pas esențial în demonstrararea faptului că recunoașterea facială poate fi o metodă biometrică viabilă. [1]

După munca lui Bledsoe, în anii 1970, Goldstein, Harmon și Lesk au dus mai departe cercetările în recunoașterea facială. Ei au adăugat 21 de caracteristici specifice, cum ar fi culoarea părului și grosimea buzelor, pentru a face procesul de recunoaștere mai automatizat.[1]

Deși acuratețea s-a îmbunătățit, măsurătorile și localizarea acestor caracteristici trebuiau încă făcute manual, ceea ce era foarte obositor. Cu toate acestea, tehnologia lor reprezenta un pas înainte față de metoda folosită de Bledsoe cu dispozitivul RAND Tablet. [1]

Tehnologia de recunoaștere facială a evoluat rapid în ultimele decenii, devenind una dintre cele mai utilizate forme de autentificare biometrică și identificare personală. Aceasta este aplicată pe scară largă în diverse domenii, de la securitatea națională și sisteme de supraveghere până la dispozitivele mobile și rețelele de socializare. Algoritmii care stau la baza acestor sisteme utilizează caracteristicile unice ale feței umane pentru a identifica sau verifica identitatea unei persoane. Cu toate acestea, în ciuda avantajelor evidente oferite de recunoașterea facială, tehnologia nu este lipsită de vulnerabilități.

Pe măsură ce tehnologia avansează, crește și preocuparea privind securitatea și fiabilitatea algoritmilor de recunoaștere facială. Algoritmii sunt expuși la diverse amenințări și provocări care pot afecta acuratețea, robustețea și integritatea sistemelor. Printre aceste vulnerabilități se numără atacurile de tip "spoofing", unde un utilizator rău intenționat poate folosi fotografii sau modele 3D pentru a păcăli sistemele de recunoaștere facială, precum și probleme legate de prejudecăți algoritmice, care duc la erori semnificative în identificarea persoanelor din anumite grupuri etnice sau de gen. În plus, factorii de mediu, cum ar fi iluminarea slabă sau schimbările de expresie facială, pot afecta performanța algoritmilor.

Analiza vulnerabilităților algoritmilor de recunoaștere facială este crucială pentru înțelegerea limitelor și riscurilor asociate cu utilizarea acestei tehnologii în contexte critice. Un aspect esențial al acestei analize este evaluarea modului în care datele sunt colectate, prelucrate și utilizate de algoritmi. De exemplu, diferențele în calitatea imaginilor sau a datelor de antrenament pot influența rezultatele finale ale procesului de recunoaștere facială. Aceasta ridică întrebări legate de echitatea algoritmilor și de impactul social al utilizării lor.

O altă preocupare majoră este lipsa de transparență a algoritmilor de recunoaștere facială. În multe cazuri, detaliile despre modul în care aceștia funcționează sunt protejate de drepturi de proprietate intelectuală, ceea ce limitează capacitatea publicului și a cercetătorilor de a evalua corect siguranța și etica sistemelor. Această opacitate poate duce la o încredere exagerată în tehnologie, în ciuda vulnerabilităților sale ascunse. În plus, lipsa standardelor uniforme în industrie pentru testarea și evaluarea acestor algoritmi complică și mai mult identificarea și corectarea problemelor de securitate.

O altă sursă de vulnerabilități este legată de evoluția constantă a tehnicilor de atac cibernetic, care devin din ce în ce mai sofisticate. Atacurile de tip adversarial, în care imagini manipulate subtil sunt folosite pentru a păcăli sistemele de recunoaștere facială, reprezintă o amenințare serioasă pentru securitatea datelor. Aceste atacuri exploatează punctele slabe ale algoritmilor, făcându-i să identifice greșit persoanele sau să nu recunoască deloc anumite fețe. În plus, atacurile bazate pe inteligența artificială și învățarea automată devin din ce în ce mai comune, ceea ce adaugă o dimensiune suplimentară de complexitate în apărarea împotriva acestor amenințări.

De asemenea, aspectele etice și legale joacă un rol important în discuțiile despre vulnerabilitățile algoritmilor de recunoaștere facială. Utilizarea necorespunzătoare a acestei tehnologii poate duce la încălcări ale dreptului la intimitate și la utilizarea abuzivă a datelor biometrice. În plus, utilizarea sa în

supravegherea în masă a populației a ridicat îngrijorări semnificative în rândul activiștilor pentru drepturile omului, care avertizează asupra potențialului său de a facilita controlul și abuzurile guvernamentale.

Una dintre cele mai mari îmbunătățiri aduse de algoritmii de recunoaștere facială este în domeniul securității și al prevenirii criminalității. În orașe din întreaga lume, sistemele de supraveghere bazate pe această tehnologie sunt utilizate pentru a monitoriza spațiile publice, identificând automat persoanele suspecte sau căutate de autorități. Acest lucru a permis autorităților să răspundă mai rapid la incidente și să prevină atacurile teroriste sau alte forme de criminalitate. În plus, tehnologia a fost folosită pentru a ajuta la identificarea victimelor în cazuri de catastrofe naturale sau atacuri teroriste, accelerând procesul de asistență și salvare.

O altă îmbunătățire majoră a fost implementarea recunoașterii faciale în dispozitivele mobile și accesul securizat la informații. Multe smartphone-uri moderne utilizează tehnologia de recunoaștere facială pentru a oferi un nivel suplimentar de securitate, permițând deblocarea dispozitivului doar prin intermediul recunoașterii biometrice. Aceasta oferă un acces rapid și securizat, fără a necesita parole sau alte metode de autentificare mai vulnerabile.

În comerțul electronic și în serviciile bancare online, recunoașterea facială a adus o schimbare semnificativă în ceea ce privește verificarea identității. Acum, clienții pot efectua tranzacții sau accesa conturile lor în mod securizat, fără a fi nevoie de parole complexe sau autentificări prin e-mail. Algoritmii de recunoaștere facială au redus considerabil riscurile de fraudă și furt de identitate, oferind un nivel sporit de încredere în sistemele online.

Un alt domeniu în care algoritmii de recunoaștere facială au îmbunătățit viața cotidiană este cel al experiențelor personalizate, în special în industria divertismentului și marketingului. Tehnologia este utilizată pentru a analiza reacțiile emoționale ale utilizatorilor față de conținutul vizual, precum reclame sau filme, permițând companiilor să personalizeze și să adapteze ofertele în funcție de preferințele acestora. De asemenea, platformele sociale utilizează recunoașterea facială pentru a automatiza etichetarea fotografiilor și pentru a facilita interacțiunile online.

În domeniul asistenței medicale, recunoașterea facială a adus îmbunătățiri semnificative în monitorizarea pacienților și în diagnosticare. De exemplu, spitalele folosesc algoritmi de recunoaștere facială pentru a monitoriza constant expresiile pacienților, detectând semne timpurii ale durerii sau disconfortului. În plus, tehnologia a fost utilizată pentru a diagnostica anumite afecțiuni genetice rare, care pot fi identificate pe baza trăsăturilor faciale.

În transportul public și aeroporturi, recunoașterea facială a simplificat procesele de verificare a identității, accelerând fluxul de pasageri și reducând timpii de așteptare. În multe aeroporturi internaționale, pasagerii pot trece prin punctele de control doar pe baza verificării faciale, eliminând necesitatea prezentării documentelor fizice în mod repetat. Acest lucru a îmbunătățit semnificativ experiența de călătorie și a redus riscul de utilizare a documentelor false.

De asemenea, algoritmii de recunoaștere facială au contribuit la îmbunătățirea siguranței în mediul corporativ, prin implementarea de sisteme de acces securizat în clădiri sau zone restricționate. Astfel, angajații pot accesa spațiile de lucru fără a folosi carduri de acces sau alte metode vulnerabile la pierderi sau furt.

În concluzie, algoritmii de recunoaștere facială au adus numeroase îmbunătățiri în societate, făcând tehnologia mai accesibilă, sigură și eficientă. Deși există încă provocări legate de confidențialitate și utilizarea abuzivă a datelor biometrice, beneficiile evidente în ceea ce privește securitatea, eficiența și personalizarea experiențelor demonstrează impactul pozitiv al acestei tehnologii în viața de zi cu zi.

Recunoașterea facială oferă beneficii clare, analiza vulnerabilităților algoritmilor care stau la baza acestei tehnologii este esențială pentru a preveni riscurile asociate cu utilizarea sa. O înțelegere profundă a acestor puncte slabe va permite dezvoltarea unor soluții mai robuste și mai etice, asigurând astfel o utilizare responsabilă a tehnologiei în viitor.

BIBLIOGRAFII

[1] DE LEEUW, K., BERGSTRA, J. (2007). The History of Information Security: A Comprehensive Handbook. Amsterdam: Elsevier. pp. 264–265

[2] Thales Group, „A Brief History of Facial Recognition Technology", Thales. Data accesării: 1 octombrie 2024. [Online]. Disponibil la: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition.

[3] ISTRATI, D. Temperature Capture And Image Processing System: A Case Study. In Journal of Engineering Science. Vol. XXIX, no. 2 (2022), pp. 108 – 115. https://doi.org/10.52326/jes.utm.2022.29(2).10UDC[621.397.424:772.96+004.93]:616.98:578.834.1

[4] JAIN, A. K., FLYNN, P. și ROSS, A. (Eds.), Springer, 2007 Handbook of Biometrics: Aplicațiile practice ale recunoașterii faciale în diverse domenii. pp 50-90

[5] VECHIU, A.-M., ISTRATI, D. „Sécurité des applications dans AWS : configuration et gestion des services sans serveur". Data accesării: 10 octombrie 2024 [Online]. Disponibil la:http://repository.utm.md/bitstream/handle/5014/28077/Conf-TehStiint-UTM-StudMastDoct-2024-V2-p949-954.pdf?sequence=1&isAllowed=y

[6] SCHROFF, F., KALENICHENKO, D. PHILBIN, J. „FaceNet: A unified embedding for face recognition and clustering", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 815–823, 2015.

[7] GOODFELLOW, I., BENGIO, Y., COURVILLE, A. Deep Learning. MIT Press, 2016. Înțelegerea algoritmilor folosiți în recunoașterea facială, inclusiv trăsături geometrice și metode moderne de învățare

[8] CHINGOVSKA, I., ANJOS, A., & MARCEL, S. „On the effectiveness of local binary patterns in face anti-spoofing." IEEE Biometrics Special Interest Group (BIOSIG), pp. 1-7, 2012. Metodele de detectare a atacurilor de tip spoofing și alte vulnerabilități

[9] OpenAI, Adversarial Examples and Their Implications for AI Safety, 2020

[10] BUOLAMWINI, J., GEBRU, T. „Gender shades: Intersectional accuracy disparities in commercial gender classification",77–91, 2018.

[11] RANJAN, R., SANKARANARAYANAN, S., CASTILLO, C. D., & CHELLAPPA, R., „An open-source implementation of face recognition with deep neural networks." IEEE Transactions on Biometrics, Behavior, and Identity Science, 1(1), pp. 1-14, 2019.

[12] ISTRATI, D. „A Brief Overview of Intelligent Interfaces in Production Systems." *XIIth Informational Conference on Electronics, Communications and Computing*, 20-21 October 2022, Chișinău, TUM, pp. 158-161. https://doi.org/10.52326/ic-ecco.2022/CS.02

[13] ASTAFI, V., ISTRATI, D. „L'INTERACTION L'HOMME-MACHINE". volumul I. Pag. 320-323 https://utm.md/wp-content/uploads/2020/05/UTM-CTS-SMD-2020-Volumul-I.pdf