COLLECTION SECURITY MANAGEMENT, BASED ON FACIAL RECOGNITION, AT UNIVERSITY LIBRARIES

Andra Botez, PhD Student

Alexandru Bejinaru-Mihoc, PhD Student

Angela Repanovici, Prof., PhD

Abstract: Facial recognition is a technique that uses unique facial features to identify an individual. The automated face recognition system is a challenging problem and has gained much attention over the last few decades. This method has an advantage over password and access card authentication in that it is based on something you are, which is not easily copied or stolen. This article follows the advantages and disadvantages of implementing a security system based on facial identification in a university library.
Keywords: biometrics, face identification, surveillance, security system, university library.

1. Introducere

Datele biometrice sunt cracteristici care diferă de la o persoană la alta (sau grup de persoane), fiind importante în multe aplicații de securitate, cum ar fi accesarea unei clădiri, sau a unui sistem, identificarea unei persoane de interes într-o anumită circumstanță, precum și în a stabili dacă acțiunile unei persoane prezintă o amenințare.[12]

Biometriaesteunproces utilizatpentru aidentifica sauautentifica identitateaunui individfolosind oricaredintr-o seriedecaracteristici fizicesaucomportamentale.[5]

Cei mai utilizați factori fiziologici din domeniul biometric sunt:

- *Recunoașterea irisului* - este o tehnică care folosește pattern-uri de culoare și formă în iris pentru a confirma identitatea unei persoane.
- *Recunoașterea facială* – este o tehnică ce folosește caracteristici faciale unice pentru a identifica un individ.

Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7

- *Recunoașterea vocii* – este o tehnică care utilizează un tipar de voce, pentru a analiza modul în care o persoană spune un anumit cuvânt sau o secvență de cuvinte unice pentru acel individ.
- *Recunoașterea amprentelor* digitale este o tehnică care utilizează distribuția terminațiilor și bifurcațiilor de pe deget pentru a confirma identitatea unei persoane.[10]

În scopul identificării, sistemele biometrice necesită două etape de funcționare: înscriere și autentificare. În decursul etapei de înscriere, se obțin datele biometrice, legate de o identitate cunoscută, și codificate pentru stocare, recuperare și corelare. Dispozitivele senzoriale, cum ar fi un scanner de amprente, sunt folosite pentru a colecta datele.Unșablonde referință esteapoi creat,urmând a fi stocatîntr-o bazăde date centralizatăsauunsistemportabildescentralizat, cum ar fi unsmart cardsau un telefon mobil. Verificarea are loc atunci când cineva pretinde o identitate particulară, de exemplu, pentru a obține acces la un laborator de înaltă securitate. Sistemul biometric compară datele noi scanate, cu o versiune înregistrată anterior. Accesul este apoi acceptat sau respins.[5]

Atât marile, cât și micile biblioteci, se confruntă cu problema securității colecțiilor. Parolele pot fi uitate, sparte sau observate intenționat sau neintenționat de o altă persoană. Uitarea parolelor sau pierderea „smart-cardurilor” înseamnă o pierdere de timp prețios pentru administratorii de rețea și utilizatori. Trăsăturile anatomice nu pot fi copiate ușor și nici pierdute.[3] Biometria poate fi integrată în securitatea bibliotecilor, ajutând atât personalul, cât și utilizatorii.

2. Identificarea facială

Recunoașterea facială este o tehnologie care folosește computerul pentru a analiza imaginile feței și a extrage caracteristicile pentru recunoașterea identității subiectului.[15]

Fața captată trebuie să fie comparată cu un număr foarte mare de imagini înregistrate, deoarece sistemul funcționează ca o bază de date, iar cu ajutorul algoritmului de căutare facială, se poate face măsurarea punctelor nodale, cum ar fi:, oasele feței, lățimea nasului, linia maxilarului, distanța între ochi, adâncimea orbitelor, bărbia.[9];[1]

Recunoașterea facială este folosită în diverse domenii, cum ar fi: supraveghere și controlul accesului, dar și în scopul interacțiunii om-calculator. Securitatea informațiilor și marketing-ul electronic utilizează acest sistem de asemenea, datorită timpului rapid de procesare a informației.[4]

Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7

Detectarea facială poate fi considerată ca fiind un caz specific de detectare a obiectelor, intitulat "detectarea obiectului dintr-o clasă". În "detectarea obiectului dintr-o clasă" ("object-class detection"), sarcina este de a găsi locațiile și dimensiunile tuturor obiectelor dintr-o imagine care aparțin unei anumite clase. Detectarea facială poate fi considerată ca fiind un caz mai general de localizare a feței. În localizarea feței, sarcina este de a găsi locațiile și dimensiunile unui număr cunoscut de fețe (de obicei unul). Dedectarea facială nu conține aceste informații suplimentare.[13]

Atunci când datele de intrare pentru un algoritm sunt prea mari pentru a fi prelucrate, vor fi transformate într-o reprezentare redusă, a unui set de caracteristici.După etapa extragerii caracteristicilor, segmente ale feței sunt extrase din imagini. Dacă folosim direct aceste segmente, pentru extragerea caracteristicilor, apar niște dezavantaje. În primul rând, fiecare segment conține, de obicei peste 1000 de pixeli, care sunt prea mari pentru a construi un sistem de recunoaștere robust. În al doilea rând, segmente ale feței pot fi luate de la diferite aliniamente ale aparatului de fotografiat, cu diferite expresii faciale, iluminări și pot suferi de ocluzie și confuzie.Pentru a depăși aceste neajunsuri, extragerea caracteristicilor este efectuată prin arhivarea informației, reducerea dimensiunii, extracție cu scoatere în relief și curățarea zgomotului de imagine. De obicei, după această etapă, un segment al feței este transformat într-un vector cu dimensiune fixă sau un set de puncte de reper și a locațiilor corespunzătoare acestora. Transformarea datelor de intrare în setul de caracteristici se numește extragerea caracteristicilor.[13]

Printre diferitele tehnici biometrice, recunoașterea facială nu este cea mai fiabilă și eficientă metodă. Cu toate acestea, un avantaj cheie este faptul că nu necesită un ajutor (sau aprobare) din partea subiectului de testare. Sistemele proiectate în mod corespunzător, instalate în aeroporturi, multiplexuri, și alte locuri publice pot identifica indivizi din rândul mulțimii.[13]

3. Modele de recunoaștere facială

Un număr de algoritmi actuali de recunoaștere a feței folosesc reprezentări ale feței găsite prin metode statistice necontrolate. De obicei aceste metode găsesc un set de imagini de bază și reprezintă fețe ca o combinație liniară a acestor imagini. Analiza componentelor principale (PCA) este un exemplu foarte popular de astfel de metode. Baza imaginilor găsite de către PCA, depind doar de relațiile dintre pixeli pereche în imaginea bazei de date. Într-o sarcină, cum ar fi

Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7

recunoașterea feței, în care informațiile importante pot fi conținute în relațiile de înaltă ordine dintre pixeli, pare a fi rezonabil să ne așteptăm ca imaginile de bază mai bune, să poată fi găsite prin metode sensibile la aceste statistici de înaltă ordine. Analiza componentei independente (ICA) o generalizare a PCA, este o astfel de metodă.

Într-un articol de specialitate Martinez A.M. and Kak, A.C., au făcut o analiză a modelelor PCA (Analiza componentelor principale) versus LDA (Analiza lineară discriminantă), în cadrul paradigmei bazate pe recunoașterea obiectului. În general, se crede că algoritmul bazat pe LDA sunt superioare celor bazate pe PCA, dar cei doi au arătat că acest lucru nu este întotdeauna adevărat. Concluzia lor generală este că, atunci când setul de date de formare este mic, PCA poate depași LDA si, de asemenea, că PCA este mai puțin sensibilă la diferite seturi de date de formare.[7]

Xu Yong, Zhang Zheng and all. propun un nou algoritm de detectare a feței, luând în considerare axa de simetrie a acesteia, prin proiectarea unui cadru care să producă un dicționar aproximativ al axei simetrice virtuale, pentru creșterea preciziei de recunoaștere a feței. Autorii consideră că este de remarcat faptul că noul algoritm de producere a fețelor virtuale simetrice față de axă, este matematic, foarte maleabil și ușor de implementat. Rezultatele experimentale demonstrează superioritate în recunoașterea facială a imaginilor feței virtuale obținută prin folosirea metodei propuse de ei, față de imaginea feței originale.[14]

Într-un articol de specialitate, Kim, Dong-Ju, Shon, Myoung-Kyu and all., propun o metodă de preprocesare și o tehnică de extracție facială îmbunătățită, pentru un sistem de recunoaștere al feței puternic iluminat. Sistemul propus constă într-un nou descriptor de preprocesare, un descriptor caracteristic de iluminare puternică, și un modul de fuziune ca etape secvențiale. Acest sistem introduce un model binar-central îmbunătățit, ca descriptor de preprocesare si un diferențial al componentelor de analiză 2-D, ca descriptor al caracteristicilor, pentru a realiza o îmbunătățire a performanței.[6]

Muhammad Bashir, împreună cu Abu-Bakar Syed Abd Rahman prezintă un algoritm de detectare a profilului feței bazat pe caracteristicile singularităților curbate, ce pot fi aproximate cu foarte puțini coeficienți și într-o manieră non-adaptativă, oferind o bună reprezentare direcțională și putând capta informații de margine a feței umane, din unghiuri diferite. În primul rând, o schemă simplă de segmentare a culorii pielii bazată pe HSV (Hue-Saturation-Value/ Nuanță-Saturație-Valoare) și YCgCr (luminance-green chrominance-red chrominance/ luminanță-verde

Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7

crominanță-roșu crominanță) modele de culoare folosite pentru a extrage blocuri de piele. În testul de performanță, rezultatele au aratat ca algoritmul propus poate detecta fețele profilului în imagini color cu o rată de detecție bună și rată scăzută de neidentificare a feței.[8]

4. Concluzii

Recunoașterea facială poate fi considerată o tehnologie ușor de implementat și accesibilă, deoarece majoritatea soluțiilor utilizează camerele built-in (sau o cameră web relativ ieftină) pentru a funcționa. Dotarea bibliotecilor cu un astfel de sistem de securitate poate avea numeroase avantaje, printre care se numără: imaginea este capturată de la distanță, fără a se folosi contactul fizic, ușurând accesul utilizatorilor în bibliotecă (fără legitimație de intrare). De asemenea sistemul capturează imagini în spații publice, ajutând la prinderea răufăcătorilor. Se pot folosi baze de date legale (în colaborare cu poliția sau alte organe de stat care folosesc astfel de baze de date).

Actualele modele de identificare facială pot avea probleme cu identificarea persoanelor în condiții de iluminare slabă și cu detectarea stării de viață a individului, o condiție necesară pentru a asigura un nivel competitiv de securitate.[10]Variația condițiilor de iluminare este una dintre cele mai mari provocări în recunoașterea facială de la distanță. În special, atunci când imaginile sunt captate de la distanțe mari, nu ai control asupra condițiilor de iluminare. Ca rezultat, imaginile captate suferă adesea de lumină extremă (din cauza soarelui) sau de lumină slabă (din cauza umbrei, vreme rea, seara, etc).[11]

Bibliografie

Aron I. *Biometria. Metodă de investigare criminalistică,* 2014, Editura Sitech, ISBN 978-606-11-4035-0, Craiova.

Bartlett M.S. , Movellan J.R. , Sejnowski T.J.*Facerecognition by independent component analysis,* 2002, IEEE Transactions on Neural Networks, USA, 13(6), ISSN: 1045-9227, 1450 – 1464.

Boldea M., Boldea C.R. ”*Identificare biometrică”,* 2003, Revista *Informatica Economica*, nr. 1(25).

Cament L. A., Castillo L. E., Perez J.P., Galdames F.J., Perez C.A., *Fusion of local normalization and Gabor entropy weighted features for face identification,* 2014, Image Processing Laboratory, Department of Electrical Engineering and Advanced Mining Technology

Center, Universidad de Chile, Av. Tupper 2007, Santiago, Chile, Pattern Recognition 47, 568–577.

Clodfelter R. "*Biometric technology in retailing: Will consumers accept fingerprint authentication?*", 2010, ElsevierLtd.; Journal of Retailing and Consumer Services 17, 181–188.

Kim DJ; Shon MK; Lee S; Kim E., *Illumination-Robust FaceRecognition Approach Using Enhanced Preprocessing and Feature Extraction*, 2016,Journal Of Nanoelectronics And Optoelectronics, 11(2), 141-147.

Martinez A.M., Kak A.C.*PCA versus LDA (Article)* , Robot Vision Lab, School of Electrical and Computer Engineering, Purdue University, IN 47907-1285, USA.

Muhammad B., Abu-Bakar S.A. *Face detection in profile views using Fast Discrete Curvelet Transform (FDCT) and Support Vector Machine (SVM)*, 2016, International Journal On Smart Sensing And Intelligent Systems, 9(1), 107-122.

Phillips P.J., Moon H., Rizvi S.A., Rauss P.J., *The FERET evaluation methodology for face-recognition algorithms*, 2000, IEEE Transactionson Pattern Analysisand Machine Intelligence, 22(10), 1090–1104.

Piccolotto P., Maller P. *Biometrics from the User Point of View: Deriving Design Principles from User Perceptions and Concerns about Biometric Systems*, 2014, Technology Journal, 18(4).

Rama C., Jie N., Vishal M.P. *Remote identification of faces: Problems, prospects, and progress*, 2012,Center for Automation Research, University of Maryland, College Park, MD 20742, United States, Pattern Recognition Letters 33, 1849–1859.

Rodriguez A., Kumar V. "*Segmentation-Free Biometric Recognition Using Correlation Filters*", 2014,Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA; Academic Press Library in Signal Processing**.**

Subrat K.R., Siddharth S.R. *A Survey on Face Detection and Recognition Techniques in Different Application Domain*, 2014, I.J. Modern Education and Computer Science, 8, 34-44.

Xu Y.,Zhang Z., Lu G.M.,Yang, J. *Approximately symmetrical face images for image preprocessing in facerecognition and sparse representation based classification*, 2016, Pattern Recognition , 54, 68-82.

Yang M.H., Kriegman D.J., Ahuja N. *Detecting faces in images: a survey*, *IEEETrans.* 2002, Pattern Anal. Mach. Intell. 24 (1), 34–58.

Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7