Universitatea Transilvania din Brașov

ȘCOALA DOCTORALĂ INTERDISCIPLINARĂ

Facultatea: DESIGN DE PRODUS ŞI MEDIU

DEPARTAMENTUL DESIGN DE PRODUS, MECATRONICĂ ŞI MEDIU

Drd. Jr. Andra-Manuela BOTEZ (căs. BEJINARU-MIHOC)

CERCETĂRI TEORETICE ȘI EXPERIMENTALE ASUPRA DEZVOLTĂRII SISTEMELOR BIOMETRICE

THEORETICAL AND EXPERIMENTAL RESEARCH ON THE DEVELOPMENT OF BIOMETRIC SYSTEMS

REZUMAT / ABSTRACT

Conducător ştiinţific

Prof.dr.ing., dr. marketing Angela REPANOVICI

BRAȘOV, 2018

Universitatea Transilvania din Brașov

D-lui (D-nei) .....

COMPONENȚA

Comisiei de doctorat

Numită prin ordinul Rectorului Universității Transilvania din Braşov
Nr. 9615 din 05.11.2018

PREŞEDINTE:	Prof.dr.ing. Codruța JALIU Decan Facultatea de Design de produs și Mediu, Universitatea Transilvania din Braşov
CONDUCĂTOR ŞTIINȚIFIC:	Prof.dr.ing.,dr.marketing Angela REPANOVICI Universitatea Transilvania din Braşov
REFERENȚI:	Prof.dr.ing. Santiago Fernandiz BOU Universitatea Politehnică din Valencia
	Prof.dr.ing. Mircea REGNEALĂ Universitatea din București
	Prof.dr.ing. Anca DRĂGHICI Universitatea Politehnică Timișoara

Data, ora şi locul susținerii publice a tezei de doctorat: 14 decembrie 2018, ora 12^{00}, sala Sala E24 (Căsuța Solară).

Eventualele aprecieri sau observații asupra conținutului lucrării vor fi transmise electronic, în timp util, pe adresa arepanovici@unitbv.ro

Totodată, vă invităm să luați parte la şedința publică de susținere a tezei de doctorat.

Vă mulțumim.

PREFAȚĂ

Teza de doctorat intitulată "Cercetări teoretice și experimentale asupra dezvoltării sistemelor biometrice" prezintă un studiu referitor la îmbunătățirea sistemelor de securitate din biblioteci. În cadrul lucrării se propune realizarea unui sistem experimental bazat pe recunoașterea facială pentru securitatea colecțiilor și persoanelor în biblioteci, având în vedere că în ultimii ani, securitatea personală este o problemă, datorită numeroaselor atacuri teroriste.

Teza de doctorat a fost realizată în colaborare cu firma **Visage Cloud**. Pe această cale îi mulțumesc pentru colaborare și pentru soluțiile oferite domnului Bogdan Bocse, manager partener la Visage Cloud și membru fondator, care m-a susținut în baza principiului: "pentru o minte deschisă nu există uși închise".

Mulțumesc doamnei prof.univ. dr. ing. dr. marketing Angela REPANOVICI, conducătorul științific, pentru contribuția deosebită în formarea mea profesională, sprijinul științific și moral acordat, coordonarea, soluțiile inovative, recomandările și observațiile realizate pe toată perioada efectuării studiilor doctorale.

Mulțumesc domnilor profesori din cadrul Universității Transilvania Brașov, **Departamentul Design de Produs, Mecatronică şi Mediu**, pentru sprijinul științific, îndrumările și interesul acordat cercetărilor din cadrul tezei de doctorat. Mulțumesc domnilor profesori prof.dr.ing. Luciana CRISTEA, prof.dr.ing. Codruța Ileana JALIU, prof.dr.ing. Ileana Constanța ROȘCA, prof.dr.ing. Mihaela Ioana BARITZ și colectivului departamentului pentru ajutorul oferit în realizarea tezei.

Mulțumesc domnului prof.dr.ing. Anișor NEDELCU de la Facultatea de Inginerie Tehnologică și Management Industrial pentru toate sfaturile oferite și sprijinul acordat.

Mulțumesc domnului profesor Santiago Fernandiz Bou, de la Universitatea Politehnică din Valencia, Spania, pentru soluțiile și materialele oferite în interesul obținerii rezultatelor în cadrul tezei de doctorat și pentru posibilitatea de a colabora cu Universitatea Politehnică din Valencia, prin efectuarea stagiului de cercetare extern.

Mulțumesc comisiei, Prof.dr.ing. Codruta JALIU, Decan Facultatea de Design de Produs și Mediu, Universitatea Transilvania din Brașov, Prof.dr.ing. Santiago Fernandiz Bou Universitatea Politehnică din Valencia, Spania, Prof.dr. Mircea REGNEALĂ, Universitatea din București, Prof.dr.ing. Anca DRAGHICI, Universitatea Politehnică Timișoara, pentru că au acceptat să facă parte din comisie şi au analizat lucrarea.

Mulțumesc familiei pentru susținerea, încrederea și sprijinul oferit, precum și tuturor celor care mi-au fost alături, direct sau indirect, și m-au susținut pe durata studiilor doctorale.

CUPRINS

CONTENTS

INTRODUCERE

Biometria se referă la identificarea automată a unei persoane pe baza propriilor caracteristici fiziologice sau comportamentale. Această metodă de identificare este preferată față de metodele tradiționale care implică parole și numere de identificare personale (PIN-Personal Identification Number) din mai multe motive, inclusiv evitarea necesității ca persoana identificată să fie prezentă fizic la punctul de identificare și/sau a amintirii vreunei parole sau a unui simbol. Diferite tipuri de sisteme biometrice sunt utilizate pentru identificarea în timp real. Cele mai răspândite se bazează pe recunoașterea feței și potrivirea amprentelor digitale; alte sisteme biometrice utilizează scanarea irisului și a retinei, vorbirea, compararea caracteristicilor faciale și termogramele faciale, precum și geometria mâinilor.

Tehnologiile biometrice sunt definite ca **"metode automatizate de verificare sau recunoaștere a identității unei persoane în viață pe baza unei caracteristici fiziologice sau comportamentale"**.

Există două cuvinte-cheie în această definiție: "**automatizat**" și "**persoană**". Cuvântul "automatizat" diferențiază biometria de domeniul mai larg al științei identificării umane. Tehnicile de autentificare biometrice sunt efectuate, exclusiv, prin utilizarea unor aparate, în general un calculator digital.

Avantajele biometriei: 1. Trăsăturile biometrice nu pot fi pierdute sau uitate (spre deosebire de parole). 2. Caracteristicile biometrice sunt dificil de copiat, partajat și distribuit (parolele pot fi anunțate în site-urile “crackers”). 3. Ele impun ca persoana autentificată să fie prezentă la momentul și la punctul de autentificare.

În concluzie, se poate afirma că autentificarea biometrică este un proces de securitate care se bazează pe caracteristicile biologice unice ale unui individ pentru a verifica dacă el este cel care spune că este. Sistemele de autentificare biometrice compară o captură de date biometrice cu datele autentice stocate, confirmate într-o bază de date. Dacă se potrivesc ambele eșantioane ale datelor biometrice, se confirmă autentificarea.

Biometria oferă operațiuni de securitate de gestionare a identității la nivel înalt, care au mai multe avantaje față de mijloacele tradiționale, iar acum sunt disponibile la costuri mai mici.

Sistemele biometrice se bazează pe mai multe procese distincte: înscrierea, capturarea în timp real, extragerea de șabloane și compararea șabloanelor. Scopul înscrierii este colectarea și arhivarea eșantioanelor biometrice și generarea de șabloane numerice pentru comparații viitoare. Prin arhivarea eșantioanelor prime, se pot genera noi șabloane de înlocuire în cazul în care se introduce în sistem un algoritm de comparație nou sau unul actualizat.

Se face distincția între capturarea în timp real şi înscrierea ca proces de colectare în timp real a eșantioanelor biometrice "probe" în urma unei încercări de acces sau de identificare și compararea acestora cu o "galerie" de șabloane deja înscrise.

Trei obiective importante sunt urmărite pe parcursul lucrării de față, intitulată **Cercetări teoretice și experimentale asupra dezvoltării sistemelor biometrice**:

1. stabilirea sistemului general informațional pentru securitatea colecțiilor și persoanelor în biblioteci.
2. identificarea cerințelor privind securitatea colecțiilor și persoanelor în biblioteci.
3. realizarea unui sistem experimental bazat pe recunoașterea facială pentru securitatea colecțiilor și persoanelor în biblioteci.

Obiectivul general: *Stabilirea sistemului general informațional pentru securitatea colecțiilor și persoanelor în biblioteci* vizează următoarele **obiective specifice**:

a) Studiu privind cadrul general al securității colecțiilor și persoanelor în biblioteci.
b) Studiu privind aspectele teoretice ale securității colecțiilor și persoanelor în biblioteci.

Cel de-al doilea obiectiv general: *Identificarea cerințelor privind securitatea colecțiilor și persoanelor în biblioteci* conține următoarele **obiective specifice:**

a) Cercetare statistică privind securitatea persoanelor și colecțiilor în biblioteci.
b) Analiza datelor statistice și generarea cerințelor de securitate în biblioteci.

Al treilea obiectiv general: *Realizarea unui sistem experimental bazat pe recunoașterea facială pentru securitatea colecțiilor și persoanelor în biblioteci* are la bază următoarele **obiective specifice***:*

a) Realizarea aplicației informatice pentru securitatea persoanelor și colecțiilor în biblioteci.
b) Realizarea bazei de date cu utilizatori.
c) Determinare experimentală cu privire la securitatea persoanelor și colecțiilor în biblioteci.

Referitor la tipul de abordare, prezenta lucrare se concentrează pe:

1. **O abordare formală** – Astfel, teza are în componență **5 (cinci) capitole**, **2 anexe, 116 imagini** şi **15 tabele**;
2. **O abordare structurală** – În prima parte, a lucrării sunt prezentate unele aspecte teoretice şi ulterior se analizează în profunzime rezultatele cercetărilor actuale.

Primul capitol este intitulat ***Cadrul general al securității colecțiilor şi al persoanelor în biblioteci***. În acest capitol sunt abordate probleme legate de "securitate", termen ce poate avea o varietate de conotații în lumea bibliotecii. Securitatea Internetului și securitatea materialelor bibliotecii reprezintă, ambele, aspecte importante ale serviciului de bibliotecă, dar mai importantă este siguranța utilizatorilor și a personalului.

În ultimii ani, siguranța a devenit o problemă de mare importanță în biblioteci. Există o serie de proceduri destinate protecției utilizatorilor, a angajaților și a proprietății. În secolul XXI, acest subiect se extinde și la siguranța și securitatea internetului. Multe biblioteci realizează ghiduri care conțin prevederi ce oferă informații detaliate referitoare la siguranță și securitate.

Există cel puțin patru sub-teme la subiectul general: (1) măsuri de precauție pentru a proteja utilizatorii și personalul împotriva actelor de violență; (2) protejarea materialelor de colectare

împotriva furtului/vandalismului; (3) garanții procedurale și planuri de răspuns pentru dezastrele naturale și provocate de om și (4) protecția internetului.

Acest capitol tratează în subcapitolul 1. şi 2. **siguranța personală** (pentru utilizatori și personal): măsuri de precauție împotriva actelor de violență, iar în subcapitolul 3. **măsuri de precauție pentru a proteja colecțiile bibliotecii** împotriva furtului, deoarece aceste două aspecte sunt cele care influențează în mod direct clienții.

Referitor la subcapitolul 1, directorii și personalul din toate tipurile de biblioteci continuă să fie preocupați de acțiunile unor clienți care uneori afectează în mod nefavorabil serviciile bibliotecilor, inclusiv persoanele fără adăpost, cu o boală mintală sau consumatori de substanțe interzise.

Deși este dificil să se confrunte cu utilizatorii care ignoră regulile bibliotecii, amenințând alți clienți sau personalul, creând altfel disconfort sau haos, există, totuşi, căi şi soluții care pot fi aplicate. Unele dintre aceste soluții pot necesita abordări diferite și parteneriate cu grupuri externe, cum ar fi organele de drept, serviciile sociale, consilierii pentru sănătatea mintală și abuzul de substanțe, și chiar departamentul de resurse umane.

O comunicare eficientă conduce atât la un confort sporit al utilizatorilor bibliotecii cât şi la o creştere a moralului personalului acesteia transformând biblioteca într-un spațiu unde toată lumea se simte binevenită.

Aspecte teoretice privind sistemele de recunoaștere facială este titlul celui de al 2-lea capitol, care îşi propune definirea şi prezentarea sistemelor de recunoaştere biometrică. Biometria este recunoașterea automată a persoanelor pe baza caracteristicilor lor comportamentale și biologice. Este un instrument prin care se confirmă faptul că este vorba de persoane care sunt deja cunoscute (sau necunoscute) - și, prin urmare, aparțin unui grup cu anumite drepturi (sau unui grup cărora li se refuză anumite privilegii). Se bazează pe prezumția că persoanele pot fi distinse din punct de vedere fizic și comportamental în mai multe moduri. Sistemele biometrice sunt folosite din ce în ce mai mult pentru a recunoaște persoanele și pentru a reglementa accesul la spațiile fizice, la informații, la servicii și la alte drepturi sau beneficii, inclusiv posibilitatea de a traversa frontierele internaționale. Motivele pentru utilizarea biometriei includ îmbunătățirea confortului și eficienței tranzacțiilor de acces de rutină, reducerea fraudei și sporirea siguranței publice și a securității naționale.

O temă larg răspândită în cercetarea biometrică o constituie recunoașterea feței dintr-o imagine. Procesul de identificare sau verificare automată a persoanelor din cadre sau imagini video digitale, în funcție de baza de date disponibilă, se numește *recunoașterea feței*. Obiectivul căutării de fețe dintr-o imagine sursă sau video este denumit *detectarea feței*. Detectarea feței a devenit unul dintre cele mai importante subiecte de cercetare, datorită creșterii preocupărilor legate de securitate și a numeroaselor alte aplicații (interacțiunea om - calculator, biometria, supravegherea persoanelor etc.) În literatura de specialitate sunt prezentate numeroase tehnici disponibile pentru detectarea și recunoașterea feței. Unele tehnici au condus la soluții eficiente în obținerea preciziei corespunzătoare și reducerea timpului de procesare.

1. Un mare număr de abordări de detectare și recunoaștere a feței sunt analizate prin prisma preciziei recunoașterii și a timpului de procesare.

2. Este prezentată o analiză privind tehnicile liniare și non-lineare pentru recunoașterea feței.
3. Este prezentat un studiu privind metodele de recunoaștere a feței pentru abordarea expresiei faciale.
4. Există diferite tehnici de recunoaștere a feței, în care una dintre abordări se bazează pe problema dilemei de ocluzie parțială, unde fețele sunt prelucrate să devină de nerecunoscut pentru a înșela sistemul de securitate.

În acest capitol au fost analizate cele mai comune metode de analiză a imaginii utilizate în practică, care descriu standardul pentru modelele de comportament care se formează în detectarea și recunoașterea feței. Au fost precizate avantajele și dezavantajele tehnicilor de recunoaștere a feței

S-a efectuat clasificarea tehnicilor de detectare a feței, au fost analizați unii dintre algoritmii de recunoaştere facială. Analiza principală a componentelor (PCA), Analiza componentelor independente (ICA), Analiza liniar discriminativă (LDA) şi Clasificatorul Haar sunt cei patru algoritmi de recunoaștere facială detaliați în subcapitolul 3.

Dificultățile şi neajunsurile apărute la sistemele de verificare biometrică au fost menționate în încheierea capitolului 2.

Preocupările managerilor de bibliotecă cu privire la asigurarea securității atât a personalului (incluzând în acest termen atât utilizatorii cât şi angajații bibliotecii) precum şi dezideratul de a veni în întâmpinarea cerințelor instituțiilor în vederea optimizării sistemului de securitate, au condus la dezvoltarea unor programe performante. Pentru a cunoaşte opiniile tuturor utilizatorilor referitoare la sceast subiect a fost inițiată o cercetare de marketing. Urmare a celor prezentate anterior, a fost realizată ***Cercetare statistică privind determinarea opiniilor managerilor de bibliotecă și a bibliotecarilor cu privire la nevoia de implementare a unui nou sistem de securitate și sistemele existente din biblioteci***, cercetare descrisă în cadrul **capitolului 3**.

Etapa cercetării calitative se referă la stabilirea problematicii, pornind de la cerințele respondentului. Cercetarea cantitativă reprezintă un proces mai complex; permite formularea unor concluzii pertinente. Cercetarea statistică are la bază importanța pe care o are evaluarea obiectivă a sistemelor de securitate a colecțiilor și a persoanelor din biblioteci, crearea unui sistem de recunoaştere facială care să optimizeze acest proces.

În desfăşurarea cercetării s-a pornit de la ipoteza potrivit căreia bibliotecarii preocupați de securitatea persoanelor doresc să implementeze un sistem de recunoaștere facială în biblioteca în care activează, bibliotecarii pentru care cel mai potrivit sistem de recunoaștere biometrică în vederea asigurării securității colecțiilor și a persoanelor este recunoașterea facială, sunt de acord cu implementarea unui astfel de sistem în bibliotecă, bibliotecarii care au încredere în sistemele de recunoaștere facială sunt în favoarea implementării unui astfel de sistem în biblioteca, bibliotecarii care activează în biblioteci mari, sunt de acord cu implementarea unui sistem de recunoaștere facială, cu cât nivelul de pregătire al bibliotecarilor este mai mare, cu atât aceştia sunt mai dispuși să implementeze un sistem de recunoaștere facială, bibliotecarii cu funcție de conducere sunt mai dispuși să implementeze un

sistem de recunoaștere facială în bibliotecă, cu cât experiența la locul de muncă al angajatului este mai mare cu atât mai mult ei sunt dispuși să implementeze un sistem de recunoaștere facială.

Conceperea chestionarului, analizarea şi interpretarea datelor culese sunt detaliate în cadrul capitolului.

Cel de-**al 4-lea capitol,** ***Optimizarea sistemului de securitate din biblioteci prin implementarea unui sistem de recunoaștere facială*** este dedicat în întregime aplicației VisageCloud. Aplicația informatică dezvoltată, monitorizează accesul în biblioteci, fiind creată ca răspuns la cererea tot mai mare de a avea un sistem eficient de control al accesului și prezenței într-o locație, în contextul terorismului. Capitolul începe prin prezentarea câtorva noțiuni introductive, necesare înțelegerii funcționării aplicației practice. Următorul subcapitol prezintă **Modelul de domeniu al aplicației VisageCloud** precum şi **Interfața de programare (API - Application Programming Interface)** necesare realizării aplicației propriu-zise. În ingineria software, un model de domeniu este un model conceptual al domeniului care încorporează atât comportamentul, cât și datele. Un model de domeniu este un sistem de abstractizări care descrie aspecte ale unei sfere de cunoaștere, influență sau activitate (domeniu). Modelul de domeniu, în limbajul de modelare Unified Modeling Language (UML), este ilustrat printr-o diagramă de clasă prezentată în subcap. 4.2.1

API-ul VisageCloud este un API REST (Representational state transfer) în Cloud care poate fi utilizat în aplicații pentru a permite accesul la recunoașterea facială și la capacitățile de clasificare

Interfața de programare a aplicațiilor Cloud (Cloud API) este un tip de API care permite dezvoltarea de aplicații și servicii utilizate pentru furnizarea de hardware, software și platforme cloud.

În subcapitolul 3, ***VisageCloud: detectarea și recunoașterea feței*** sunt parcurse etapele necesare funcționării efective a aplicației: de la obținerea cheii API pentru a putea accesa aplicația, la crearea unei colecții de profiluri cunoscute (un profil reprezintă o persoană) pentru a detecta persoanele în fotografii și pentru a le cartografia în profil și apoi, prin utilizarea acelei colecții, pentru a recunoaște oamenii din fotografii noi.

Sunt descrişi cei 6 paşi care sunt necesari a fi efectuați în vederea obținerii recunoaşterii faciale a unei persoane dintr-o fotografie:

Pasul 1: Solicitarea unei chei API

Pentru a putea beneficia de facilitățile oferite de VisageCloud referitoare la recunoaşterea facială utilizatorii pot accesa programul la adresa https://visagecloud.com/.

Pasul 2: Crearea unei colecții

Pentru o gestionare mai ușoară a utilizatorilor înregistrați în sistem este necesară crearea unei colecții (un set sau un grup de persoane înregistrate).

Pasul 3: Crearea unor profiluri pentru fiecare persoană din colecție

Un profil reprezintă o persoană.

Pasul 4: Detectarea fețelor din fotografii

Constă în încărcarea unei imagini care poate conține una sau mai multe fețe

Pasul 5: Anexarea fiecărei fețe detectate unui profil

Se realizează asocierea unei fețe particulare dintr-o fotografie cu un profil existent.

Pasul 6: Efectuarea recunoașterii faciale

După ce au fost create mai multe profiluri și au fost cartografiate una sau mai multe fațete pentru fiecare dintre ele, ultimul pas este testarea operației de recunoaștere.

Aplicația poate fi deosebit de utilă pentru o supraveghere inteligentă, se poate aplica în biblioteci, precum și în industria hotelieră (turism), mai ales când unul dintre obiective este identificarea și recompensarea utilizatorilor (clienților) fideli.

Ultimul capitol ***Concluzii finale, Contribuții proprii (autentice)*** prezintă în formă sintetică rezultatele cercetării prin evidențierea contribuțiilor proprii şi a soluțiilor originale care au făcut posibilă realizarea obiectivelor stabilite în cadrul lucrării.

Documentarea s-a efectuat utilizând atât referințele bibliografice tradiționale cât şi cele electronice.

Această lucrare prezintă noi aspecte cu privire la dezvoltarea sistemelor biometrice, constituie un element de utilitate, performant, în activitatea bibliotecarilor implicați în procesul de securitate a colecțiilor şi personalului şi în acelaşi timp creează premizele continuării cercetărilor în acest domeniu.

CAPITOLUL 1

CADRUL GENERAL AL SECURITĂȚII COLECȚIILOR ȘI AL PERSOANELOR ÎN BIBLIOTECI

1.1. Noțiuni generale privind securitatea în biblioteci

Faptul că securitatea a devenit un subiect cheie al analizei criminologice, de o importanță deosebită, reflectă nesiguranța societății secolului douăzeci și unu.

În încercarea de a înțelege conceptul de securitate, Brooks (2009), menționează că expunerea la atacuri teroriste în multe părți ale lumii (Londra, 2005, Jakarta, 2004, Spania, 2004, Bali, 2002 și New York, 2001), a crescut nivelul de îngrijorarea socială față de capacitatea guvernelor de a-și proteja cetățenii. [13] Conform Zedner (2009), noi tehnici de prevenire a criminalității și a inițiativelor comunitare de siguranță se combină pentru a crea o preocupare de securitate în rândul autorităților locale, parteneriate între agenții, grupuri de voluntari, precum și cetățeni privați.

Latuszek (2000) menționează că deși multe biblioteci sunt în continuare în locații predominant liniștite din punct de vedere al zgomotului și a criminalității, nu este greu de observat un patern de neliniște în continuă creștere, în bibliotecile publice și academice.

Zedner (2009), consideră că securitatea este un concept promiscuu, fiind implementat în foarte multe domenii (securitate socială, securitatea financiară, securitatea mediului, sănătate și siguranță, securitatea umană, relații internaționale și de menținere a păcii etc.).[82] Astfel, securitatea este starea de „a fi protejat împotriva amenințărilor" - fie prin neutralizarea lor, prin evitarea, sau prin non-expunere la risc.

Maidabino și Zainab (2011) menționează în lucrarea lor faptul că scopul bibliotecilor este de a oferi acces la resursele informaționale în ambele formate de imprimare si non-imprimare. Aceștia consideră că echilibrarea accesului și securității în biblioteci, este dificilă, dar în același timp o sarcină necesară.

O serie de studii au abordat problema securității colecțiilor, precum și securitatea personală a vizitatorilor și a personalului bibliotecii. De asemenea, în diferite studii a fost descris modul în care infracțiunile și incidentele de încălcare a securității pot afecta furnizarea de servicii ale bibliotecilor către utilizatori. [35]

Latuszek a realizat o trecere în revistă a articolelor care descriu incidente datorate vizitatorilor bibliotecilor, pentru a sublinia importanța planurilor de securitate. Prin acest articol, autorul dorește să contureze o conștiință sporită a securității în biblioteci, subliniind întrebări tehnologice și preocupări legate de politică. [33]

Harris și Dimarco prezintă o perspectivă asupra modului în care Universitatea Mansfield, din Pennsylvania, a abordat problema securității personale, în mod specific, în bibliotecă. Scopul acestui articol este acela de a ajuta bibliotecile în planificarea pentru cele mai grave scenarii, aspectele

acoperite incluzând ce este autoblocarea; planificare, politici și proceduri; securitatea fizică; problema vizitatorilor, locuri sigure în bibliotecă etc.[24]

Maidabino și Zainab (2012) au propus un instrument de evaluare a implementării securității colecțiilor în bibliotecile universitare. Acest instrument înglobează cinci factori: administrarea securității colecțiilor, operații și procese, problemele oamenilor, aspecte fizice și tehnice ale securității colecțiilor și cultura securității în biblioteci.[35]

Westenkirchner oferă, în articolul său, instrucțiuni pentru bibliotecile care vor să achiziționeze un sistem integrat de supraveghere video digital bazat pe experiența Librariei Universității Auburn. Articolul cuprinde aspectele tehnice ale televiziunii cu circuit închis (CCTV) și sisteme de supraveghere video integrate Internet protocol (IP), oferind o scurtă explicație a modului în care funcționează echipamentul.[78]

1.1.1 Siguranța utilizatorilor și a personalului

Bibliotecile, muzeele și arhivele sunt considerate locații sigure pentru a fi vizitate, utilizate și a avea un loc de muncă. Din păcate, în instituțiile culturale au existat incidente, care au dus la rănirea sau răpirea anumitor persoane, precum și amenințări cu arme sau cu bombă. [29]

Această teză de doctorat are în vedere siguranța utilizatorilor bibliotecii, precum și a angajaților. Ne dorim să încurajăm oamenii să folosească și să se bucure de resursele vaste ale diferitelor biblioteci. Astfel, este esențial să luăm măsuri și să consolidăm concepția că bibliotecile sunt locuri sigure în care să lucrăm. [3]

Siguranța utilizatorilor și a personalului este esențială. În prima etapă trebui examinată clădirea, atât în exterior, cât și în interior, pentru ca anumiți utilizatori și personal să poată intra, să folosească unitatea și să iasă fără să se rănească, indiferent dacă pleacă noaptea, sau în timpul unei urgențe. Apoi, trebuie să avem în vedere siguranța utilizatorilor față de angajați, precum și a angajaților față de utilizatori. [29]

1.1.2 Comportament problematic

Kahn (2007), consideră că personalul bibliotecii trebuie să stabilească și să afișeze politici, care să descrie conduita adecvată în clădire. Comportamentele și practicile care nu sunt acceptabile ar trebui să fie clar definite. Autoarea menționează că aceste politici trebuie aplicate în mod uniform, mai întâi cu un avertisment și apoi cu orice restricții, sau revocări de privilegii publicate în politica bibliotecii. Avertismentele de a înceta comportamentul inadecvat sunt adesea date de către personalul superior, șef de departament și administratori. Cu toate acestea, toți membrii personalului ar trebui să fie confortabili în a face astfel de comentarii. În cazul în care utilizatorul nu respectă politicile după un avertisment, trebuie contactat departamentul de securitate sau șeful de departament dacă nu există polițiști în clădirea respectivă.

1.1.3 Copii și tineri adulți

Nu este un lucru neobișnuit să existe copii nesupravegheați în biblioteca publică. Ei pot fi lăsați singuri atât ziua, cât și seara, în timp ce părinții lor sunt la lucru. Supravegherea copiilor care folosesc colecțiile bibliotecilor este o îngrijorare. Astfel, trebuie să se stabilească politici care să protejeze copiii de străini și de situații în care s-ar putea răni. Nu numai că biblioteca trebuie să fie conștientă că există copii nesupravegheați în unitate, dar există cazuri când aceștia sunt zgomotoși, perturbatori sau abuzați de alți copii. În această situație se poate stabili o politică care limitează numărul de copii care pot lucra la o masă sau se poate crea o cameră pentru activități de grup sau de zgomot. Dacă există adolescenți care se află în vizită, poate ar trebui stabilită o limită în ceea ce privește numărul lor. Dacă nivelurile de zgomot devin intolerabile, este necesar să ne adresăm gardienilor de securitate sau unui supraveghetor pentru a avertiza copiii să fie liniștiți sau să plece. Este important să existe politici postate și aplicate uniform, care sunt întărite atunci când nivelul zgomotului scapă de sub control. Pe lângă încercarea de a controla copiii și tinerii adulți, bibliotecarii și alți membri ai personalului ar trebui să fie conștienți de ce se întâmplă în partea lor din bibliotecă.

1.1.4 Utilizatori adulți

Dacă instituția nu este o organizație privată, ea nu poate limita accesul în clădire și folosirea colecțiilor. Așadar, este posibil să aibă persoane fără adăpost, cu deficiențe mintale sau cu utilizatori itineranți în mijlocul oamenilor de afaceri obișnuiți, studenților și al altor rezidenți ai comunității. Există mai multe cărți care descriu cum să te comporți cu utilizatorii problematici [29].

1.1.5 Întrebări neconfortabile sau suspecte

Kahn (2007), subliniază în lucrarea sa faptul că din 11 septembrie 2001, bibliotecarii au devenit mai conștienți cu privire la întrebările de referință neobișnuite. Aceste întrebări ar putea include adrese și fotografii ale funcționarilor publici, hărți și desene ale clădirilor publice și guvernamentale, precum și desene sau modele pentru bombe și arme. În același timp trebuie conștientizat faptul că anumite întrebări care pot părea suspecte, pot face parte dintr-un proiect sau temă pentru acasă în cazul elevilor.

1.1.6 Vizitatori dificili

Bibliotecile și arhivele (precum și societățile istorice și muzeele într-o măsură mai mică, deoarece aceștia percep, de obicei, o taxă de admitere) sunt locuri sigure, calde și confortabile pentru persoanele fără adăpost, pentru persoanele bolnave psihic și pentru oamenii enervanți, neplăcuți, sau gălăgioși; cei care folosesc limbaj obscen; au miros neplăcut; dorm sau stau la calculator toată ziua și navighează pe internet. Atâta timp cât acești vizitatori nu deranjează pe nimeni, nu le poate interzice nimeni accesul în bibliotecă. Cu toate acestea, Turner vorbește despre bibliotecari și personalul de securitate care au cerut vizitatorilor care miroseau urât să se întoarcă după ce s-au splat și și-au curățat hainele. [29]

Vizitatorii mai problematici sunt cei care se ascund după stive și fac avansuri sexuale inadecvate vizitatorilor și membrilor personalului. Membrii personalului care aranjează cărțile sunt cei mai

vulnerabili la avansurile sexuale, la fel ca și membrii personalului de referință care îi ajută pe utilizatori să găsească materialele pe care le caută printre rafturi. Instalarea oglinzilor convexe pentru a afișa zonele de stivă în afara zonei de vedere este o modalitate de reducere a comportamentului necorespunzător și de protejare a membrilor personalului. Pentru a evita aceste probleme, trebuie stabilite politici scrise, care să interzică comportamentele sexuale inadecvate în bibliotecă. [2]

1.1.7 Vizitatori agresivi

Există multe motive pentru care vizitatorii să pară agresivi. Ei pot fi frustrați de proiectul lor de cercetare, de răspunsurile la întrebările adresate membrilor personalului, de asemenea pot fi tulburați sau bolnavi psihic. Uneori utilizatorii bibliotecii sunt mari sau înalți și astfel, par a fi agresivi doar atunci când sunt percepuți în ambientul altei persoane. Cel mai frecvent se poate întâmpla acest lucru atunci când membrii personalului stau la biroul de informare. Acești vizitatori nu sunt neapărat agresivi, ei sunt doar copleșitori. Această senzație de agresiune se poate diminua ajustând spațiul personal. [29]

Din când în când, există un utilizator care este agresiv sau supărat când ajunge la biroul de referință sau de informare. Pentru a evita un conflict, Kahn (2007), propune ca angajatul să asculte cu atenție plângerea sau problema și să încerce să răspundă fără a-l mai deranja. Membrul personalului trebuie să încerce să dezamorseze situația prin a-i oferi vizitatorului posibilitatea de a explica ce este greșit, sau de ce este atât de supărat. Aceste forme de agresiune se pot rezolva gândind în perspectivă și fără prejudecăți. [29]

În ceea ce privește vizitatorii abuzivi verbali, ei sunt cei care manifestă un limbaj abuziv sau inadecvat și pot fi destul de agitați. Din nou, membrii personalului trebuie să încerce să îi calmeze pe utilizatori ascultând cu atenție, să încerce să nu își asume o poziție defensivă sau agresivă. Astfel, atunci când utilizatorul este nemulțumit în legătură cu amenzile sale restante sau cu cărțile lipsă, angajatul bibliotecii trebuie să îi prezinte alternativele de rezolvare a problemei apărute. [2]

1.1.8 Intruși, amenințări cu bombă, amenințări cu ostateci și arme

Conform Kahn (2007), dacă cineva din personal primește o amenințare cu bombă, trebuie să întrebe informatorul când va exploda bomba, ce tip de bombă este, unde este amplasată, și alte întrebări care arată interesul acestuia. Membrul personalului trebuie să mențină o voce și o atitudine calmă. În timpul telefonului, acesta trebuie să îi facă un semn celui mai apropiat angajat pentru a apela poliția sau securitatea imediat. Membrul personalului care a răspuns la telefon nu trebuie să îl pună pe informator în așteptare, ci trebuie să încerce să obțină cât mai multe informații. Dacă pericolul pare iminent, sau atunci când departamentul de securitate instruiește astfel angajații, trebuie evacuată clădirea, într-o locație îndepărtată, sigură, care ar trebui să fie aceași ca în planul de răspuns în caz de catastrofe. Nimeni nu trebuie să reintre în clădire până când pompierii, sau echipa de dezamorsare bombe nu autorizează acest lucru.
Pentru asigurarea securității trebuie să se afișeze semne care să interzică toate tipurile de arme, inclusiv armele ascunse, în clădire. Se poate face o listă, care ar trebui să includă toate tipurile de arme de foc și cuțite de toate formele și dimensiunile. Dacă există focuri de armă în clădire, aceasta

trebuie evacuată cât mai atent, vizitatorii fiind trimiși afară sau în adăpostul pentru tornadă. Dacă sunt focuri de armă în imediata vecinătate, persoanele trebuie să se întindă pe podea, în spatele mobilierului, sau a altui tip de protecție solidă, dacă este posibil. Nu este indicat să se miște până când zona nu este asigurată de departamentul de securitate, de ofițerii de poliție, sau de pompieri. [3]

1.1.9 Evacuare de urgență: foc, tornadă și vreme rea

Personalul și utilizatorii trebuie să părăsească clădirea imediat când sună alarma de incendiu. Personalul trebuie adunat la locația exterioară, identificată de echipa de răspuns la dezastre sau de echipa de planificare a securității. Acest loc de adunare se află în afara clădirii și ușor accesibil. [29]

În cazul în care se aud sirenele raidului aerian, acestea indică de obicei o observare a tornadelor. În unele comunități, acestea indică furtuni puternice sau uragane. Utilizatorii trebuie transportați în adăposturi pentru tornadă subterane sau într-un loc în interiorul clădirii care nu are ferestre. Acest adăpost nu trebuie părăsit până când nu se aude clar sirena sau acest lucru este cerut de către ofițerii de securitate sau de siguranță publică. [2]

Unele instituții folosesc gardieni de pază sau departamente pentru a îndruma uitilizatorii și personalul la ieșirea de urgență sau la adăpost. Înainte de un dezastru sau o alertă meteo nefavorabilă, trebuie discutat cum o să ajute personalul bibliotecii utilizatorii în scaune cu rotile pentru ajunge într-o locație sigură. Biblioteca trebuie să colaboreze cu departamentul de securitate și departamentul de pompieri cu privire la această problemă, astfel încât aceștia să fie conștienți de situația în care pot fi angajații și personalul cu handicap în caz de dezastru, incendiu sau de urgență. [3]

1.2. Protecția personalului din biblioteci

1.2.0 Personalul

Există o gamă largă de opinii cu privire la protejarea siguranței personalului față de vizitatori și de alți angajați; adică relațiile interpersonale. Shuman și Turner acoperă aceste aspecte în publicațiile lor. [29] Trebuie stabilită o politică de securitate care să protejeze siguranța fizică a angajatului, solicitându-i să notifice pe cineva sau să primească permisiunea înainte de a fi în clădire. Acest lucru este deosebit de important dacă clădirea este curățată și întreținută după ce toată lumea se întoarce acasă pentru ziua în curs. A nu fi singur în clădire pare a fi o problemă de bun simț, dar acest lucru se întâmplă de multe ori. [3]

Nu ar trebui să existe niciodată o singură persoană care să lucreze cu publicul. Știm că acest lucru se datorează faptului că personalul este redus drastic sau pentru că este vorba de weekend. Calendarele de lucru ar trebui să includă un membru al personalului supleant sau de gardă, care să poată completa atunci când cineva este bolnav. În plus, ar trebui să existe întotdeauna un membru al personalului de rang înalt în timpul orelor în care instituția este deschisă, să răspundă la întrebări și să răspundă unei situații de urgență la bibliotecă sau arhivă. [29]

Pentru o bună funcționare a instituției, un membru al personalului de conducere, administrator sau supraveghetor, ar trebui să fie disponibil prin telefon, în cazul apariției unei probleme. De asemenea, este important ca oricine este supraveghetorul desemnat să cunoască politicile instituției și să aibă capacitatea de a lua decizii în cunoștință de cauză. [29]

Un alt factor deosebit de important pentru buna funcționare a unei biblioteci este percepția personalului asupra propriei siguranțe în interiorul clădirii. Nu numai că ar trebui să se simtă în siguranță în timpul zilei, în birouri de referință, de informare și de circulație, dar și în birourile și sălile de lucru. [29]

Este indicat să se stabilească politici de securitate și siguranță pentru membrii personalului care lucrează după ore, astfel încât să știe pe cine să cheme într-o situație de urgență, indiferent dacă sunt agenți de pază, supraveghetori sau poliția. Trebuie postate numere de telefon prin intermediul telefoanelor de birou pentru a avea acces ușor. [3]

1.2.1 Alți angajați

Departamentul de securitate ar trebui să efectueze o verificare de fond asupra personalului de întreținere și a personalului de curățenie, precum și asupra agenților de pază. Dacă instituția angajează o companie pentru a se ocupa de aceste locuri de muncă, atunci departamentul de securitate ar trebui să efectueze un control de fond asupra companiei și să se asigure că este stabil și asigurat. Gardienii de securitate trebuie să fie la datorie în orice moment atunci când există contractori sau personal de curățenie și întreținere în clădire. Rolul acestora este de a realiza siguranța acestor angajați și contractori și de a proteja colecțiile de furt și mutilare. [29]

1.3 Tipuri de sisteme de securitate utilizate în biblioteci

Trebuie să se stabilească politici care să țină evidența daunelor deliberate, realizate de vizitatori, asupra colecțiilor, inclusiv probleme comune de rupere a paginilor, imaginilor, sau articolelor din jurnale și enciclopedii; scoaterea paginilor din coperți; și furtul de materiale audiovizuale și digitale. [29] Aceste politici ar trebui să fie puse în aplicare prin suspendarea privilegiilor oferite utilizatorilor bibliotecii și arest pentru infracțiunile multiple și grave.

Cu toate acestea, există încă acei vizitatori care scot cărțile din coperți sau care nu se obosesc să le returneze. [29]

Este esențial să existe agenți de pază, care să verifice toți vizitatorii și personalul, care își încetează activitatea, pentru a confirma faptul că materialele au fost verificate și predate. De asemenea, este foarte eficient să existe porți de securitate care detectează obiective electronice sau magnetice introduse în cărți. Din păcate, multe sisteme de bibliotecă mici nu își pot permite prețul acestor măsuri de securitate. În astfel de cazuri, membrii personalului trebuie să aibă biroul aproape de ieșire, astfel încât să poată urmări cine pleacă, ce au în mâini, dar și în bagaj. În cazul în care biblioteca dispune de un sistem automat de returnare a materialelor, fără agenți de pază sau dispozitive de verificare, membrii personalului trebuie să fie vigilenți suplimentar și să urmărească obiceiurile și acțiunile vizitatorilor atunci când părăsesc clădirea. [29]

1.3.1 Benzile de securitate Tattle-Tape

Benzile de securitate Tattle-Tape și elementele electonice sau magnetice sunt folosite de mulți ani. Benzile de securitate sunt introduse în cotorul cărților cu coperți tari, sau între pagini, în cazul cărților normale; iar elementele magnetice sunt de obicei puse pe coperta din spate a cărții. Aceste dispozitive de securitate declanșează alarma, atunci când o persoană trece prin porțile de securitate cu o carte.

1.3.2 Sistemul RFID

Identificarea prin radiofrecvență (RFID) este cel mai fiabil mod de identificare electronică, de captare a datelor, de control, urmărire și inventariere, utilizând comunicații RF. [31] Această tehnologie îmbunătățește vizibilitatea și reduce timpul de funcționare și cerințele de muncă. [67]

Un obiectiv RFID, numit etichetă, este inserat în cărți și în carcasele materialelor audiovizuale, putând rezolva unele din problemele de urmărire și verificare a acestor materiale. Costul mediu pentru instalarea unui dispozitiv este de un dolar, incluzând atât hardware-ul, cât și software-ul. Bibliotecile încep să pună aceste dispozitive în colecțiile lor, iar muzeele folosesc dispozitivele pentru a marca și a identifica elementele cu risc de furt din colecțiile lor. [29]

Bibliotecile gestionează un inventar considerabil, cuprinzând atât materiale tipărite, cât și materiale audiovizuale în colecțiile lor. În prezent, tehnologia codurilor de bare este folosită de majoritatea bibliotecilor pentru activitățile lor zilnice. [67]

Bibliotecile utilizează o bază de date bibliografică pentru a urmări informațiile de circulație despre elementele dintr-o colecție. Fiecare carte, după ce a fost achiziționată de bibliotecă, are un număr unic, denumit de obicei un cod de bare. [40]

Desigur, există unele probleme de securitate care gravitează în jurul vieții private a vizitatorilor. American Library Association (ALA) a publicat orientări pentru utilizarea RFID în biblioteci, referindu-se la libertatea intelectuală. [29]

Tipuri de sisteme RFID

Conform Kahn, 2007, sistemele RFID se împart în mai multe categorii:

- Sisteme EAS (Electronic Article Surveillance) – au o capacitate de stocare mică, de un bit, dar suficientă pentru a detecta prezența sau absența unui obiect.
- Sisteme portabile de captură de date – Terminalul portabil conține un cititor RFID.
- Sisteme în rețea – Dispozitivul de citire are o poziție fixă şi este conectat direct la un sistem de management al informațiilor în rețea.
- Sisteme de poziționare – Dispozitivul de interogare este plasat pe un vehicul, este conectat la un computer de bord şi comunică datele, prin frecvențe radio, unui sistem de management al informațiilor.

1.3.2.1 Componentele unui sistem RFID

Sistemele RFID au mai multe componente decât etichetele RFID menționate deja, la fel ca și sistemele de coduri de bare ce cuprind mai multe elemente, nu doar barele imprimate. Se face o distincție între următoarele trei componente: etichete RFID; cititoare RFID; sisteme backend (adică middleware și aplicații) [27], [28]

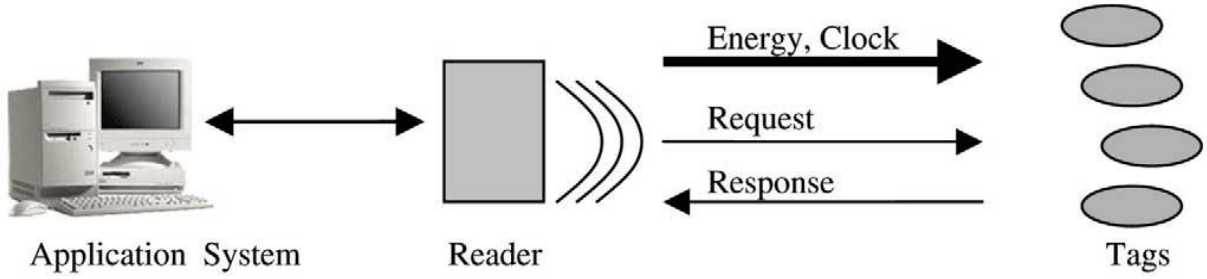


Fig. 1 *Prezentare generală a unui sistem RFID cu etichete pasive* [27]

Într-un sistem tipic RFID, **eticheta și cititorul** comunică informații între ele prin unde radio. Când un obiect marcat intră în zona de citire a unui cititor, cititorul semnalează eticheta pentru a transmite datele stocate. Odată ce datele de pe etichetă sunt primite de către cititor, informațiile sunt transmise înapoi la computer printr-o interfață de rețea. [67]

Cititoarele RFID trimit și primesc date către și de la etichete. Cititorul este unitatea care furnizează transponderului RFID energie și declanșează semnale de comunicare pentru a forța transponderul să execute acțiunea solicitată. [31] Astfel, ele sunt alcătuite dintr-o antenă, electronica necesară pentru comunicare, un microprocesor pentru controlul dispozitivului și o interfață pentru transmiterea datelor către sistemul de backend procesare. [28]

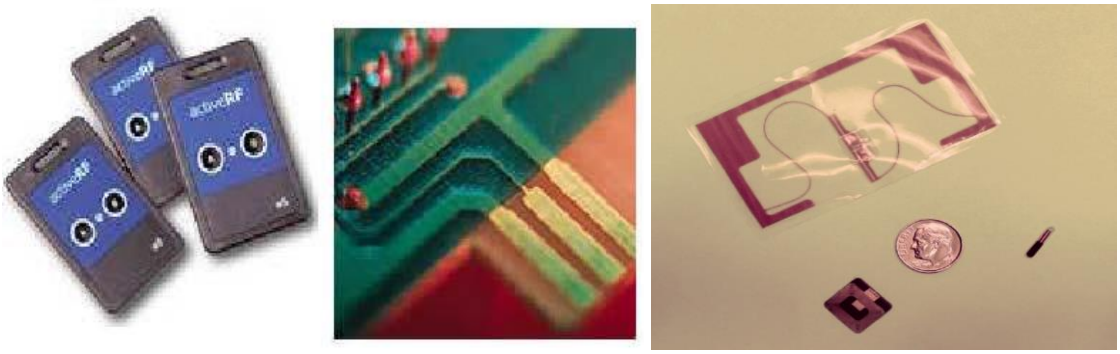


Fig. 2 *Exemple de etichete*

Există **două tipuri** complet diferite de etichete referitoare la alimentarea cu energie: cele *pasive* și cele *active*.

Colecțiile bibliotecilor s-au confruntat întotdeauna cu pericolul furtului, deteriorării și pierderii accidentale. Multe biblioteci s-au bazat timp îndelungat pe porțile de securitate electromagnetice care alarmează atunci când sunt declanșate de benzi magnetice sensibilizate în cărți. Unele sisteme folosesc acum RFID (identificarea frecvențelor radio) sau alte tehnologii, alarma anunțând pur și simplu personalul și vizitatorul cu privire la un posibil furt.

Fig. 3 *Porți RFID*

1.3.2.2 Stația de auto-împrumut

Bibliotecile dotate cu un sistem de auto-împrumut pot oferi utilizatorilor posibilitatea de a împrumuta materialele preferate în orice moment și cu un plus de intimitate. Utilizatorii bibliotecii pot fi independenți având acces la contul lor și putând gestiona materialele împrumutate; utilizatorii pot accesa opțiunea de a plăti amenzi și chiar pot primi și o chitanță pentru sumele achitate.

Fig. 4 *Stație de auto-împrumut*

Fig. 5 *Stația de auto returnare*

1.3.2.3 Stația de returnare automată

Sistemul de returnare automată a cărților este extrem de util, deoarece utilizatorii nu mai sunt condiționați de ora la care doresc să returneze materialele împrumutate. Folosind sistemul RFID, utilizatorul trebuie să își acceseze contul și beneficiază de posibilitatea de a returna materialele împrumutate cu o "verificare în timp real".

1.4. Concluzii

Bibliotecile universitare se confruntă cu o serie de provocări de securitate referitoare la colecțiile lor (atât tipărite, cât și netipărite). Colecțiile bibliotecilor constituie baza (temelia) pentru serviciile oferite comunității și servesc ca bunuri importante în bibliotecă. Ca atare, asigurarea și protejarea colecțiilor poate ajuta bibliotecile să ofere un serviciu eficient ca răspuns la cerințele de informare ale comunității universitare. Securizarea colecției implică necesitatea ca bibliotecile să furnizeze, să mențină și să-și protejeze bunurile pentru a asigura longetivitatea, accesibilitatea și furnizarea efectivă a serviciilor către utilizatori. Pentru a atinge acest obiectiv, bibliotecile au nevoie de o strategie eficientă pentru a evalua gradul de securitate a colecțiilor, încălcările cu care se confruntă și pentru a stabili un nivel acceptabil de implementare a securității colectării.

RFID asigură o urmărire rapidă și continuă a bunurilor cu o intervenție minimă a omului. Vizibilitatea sporită și precizia contribuie la reducerea semnificativă a costului forței de muncă și a stocurilor. Pe lângă acești factori de cost cuantificabil, beneficiile intangibile, inclusiv coordonarea interorganizării sporită și satisfacția clienților, necesită modele avansate de analiză a investițiilor RFID. [67]

Rezumând avantajele sistemelor RFID în raport cu alte sisteme de identificare utilizate în prezent și în special cu codul de bare: [31]

- Fără baterie. Tensiunea de alimentare derivată din câmpul RF
- Nu este necesară o linie de vizibilitate pentru comunicare
- Gama mare de operare și comunicare
- Funcția de citire și scriere a memoriei transponderului
- Viteza de comunicare ridicată
- Capacitate mare de date (memorie de utilizator)
- Securitate ridicată a datelor
- Capacitatea de criptare / autentificare a datelor
- Capacitate de citire a etichetelor multiple cu anticoliziune (50-100 etichete)
- Durabilitate și fiabilitate
- Rezistență la influența mediului
- Reutilizabilitatea transponderului
- Funcționarea fără mâini
- Putere foarte scăzută.

Sistemele de management al identității care îmbunătățesc viața privată ar putea oferi un nivel mai ridicat de transparență și control pentru utilizator.

CAPITOLUL 2

ASPECTE TEORETICE PRIVIND SISTEMELE DE RECUNOAȘTERE FACIALĂ

2.1 Sisteme de recunoaștere biometrică

În lumea de astăzi, unde tehnologia crește cu un ritm rapid, există încă anumite probleme legate de autentificarea persoanelor, probleme care trebuie soluționate în viața de zi cu zi. Recunoașterea unei persoane poate fi realizată prin diferite metode cum ar fi: *ce știm?* (bazat pe cunoștințe, de exemplu, o parolă, PIN), *ce avem?* (bazat pe un lucru/token, de exemplu, card pentru ATM, card de credit, smart card), și *ce suntem?* (bazat pe indicatori biometrici, de exemplu, față, vorbire, mers). Parola sau cardul pot fi distribuite, uitate, sau furate, dar nu și datele biometrice. Dobândirea datelor biometrice este mai complexă în comparație cu a face combinații de cifre sau furtul cardului. Astfel, biometria este mai sigură în comparație cu celelalte metode.

Biometria se bazează pe principiul măsurării fiziologice și caracteristicilor comportamentale, cum ar fi amprenta digitală, caracteristicile faciale, modele de voce, sau chiar și modul în care o persoană merge. Fiecare metodă are avantaje și dezavantaje; unele fiind mai de încredere, mai sigure, mai ușor de captat și mai puțin invazive decât celelalte. [44]

În biometrie, factorii fiziologici cel mai des întâlniți sunt prezentați în cele ce urmează.

- *Recunoașterea irisului* este o tehnică care folosește pattern-uri de culoare și formă în iris pentru a confirma identitatea unei persoane. [9]
- *Recunoașterea facială* este o tehnică ce folosește caracteristici faciale unice pentru a identifica un individ. [9] Apar, însă, 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. [9], [44]
- *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. [9] Această metodă are două dezavantaje majore: **înscriere** și **securitate**.
- *Recunoașterea amprentelor* digitale este o tehnică care utilizează distribuția terminațiilor și bifurcațiilor de pe deget pentru a confirma identitatea unei persoane. [9] Această tehnică a fost considerată un identificator unic de încredere. Are și unele dezavantaje: senzorii de identificare a amprentelor digitale nu citesc întotdeauna în mod fiabil amprentele. [44]
- *Urmele de ureche* adică bazată pe unicitatea "desenului" sau formatul urechii: forma generală a pavilionului, dimensiune, caracteristici proprii, poziție etc. [8],[45]
- *Urmele de buze* lăsate pe diferite obiecte. Se analizează următoarele caracteristici ale buzelor: formă, grosime şi lungime. [8],[45]

- *Profile ADN* (acidul dezoxiribonucleic – acid nucleic format din molecule organice dintre cele mai complexe). [8],[45]
- *Semnătura electronică* exprimată prin date în formă electronică. În România legea nr 455/2001 stabileşte regimul juridic al semnăturii electronice şi al înscrisurilor în formă electronică. [8],[45]

Fiecare metodă sau tehnologie biometrică (fiziologică sau comportamentală) are propriile avantaje şi limite. (Tab.1). [8]

Tabelul 1. Comparații asupra unor tehnologii biometrice, după [1]

Tehnologia biometrică	Univer-salitate	Unicitate	Perma-nență	Eficacitate	Accepta-bilitate
Față	R	S	M	S	R
Amprentă	M	R	R	R	M
Geometrie mână	M	M	M	M	M
Apăsare pe tastă	S	S	S	S	M
Semnătură	S	S	S	S	R
Venele de la mână	M	M	M	M	M
Iris	R	R	R	R	S
DNA	R	R	R	R	S
Mers	M	S	S	S	R
Voce	M	S	S	S	R
Termografiere facială	R	R	S	M	R
Scanare retină	R	R	M	R	S

Notă: R –ridicat; M – mediu; S –slab

Au fost identificate sistemic două căi pentru măsurarea performanțelor sistemelor biometrice [8]:

1. rata respingerilor false, exprimată prin procentul de persoane autorizate respinse de sistem;
2. rata acceptărilor false, exprimate prin procentul de persoane neautorizate acceptate de sistem.

În funcționarea unui biosistem se disting două etape de lucru [66]:

1. *verificare.* Utilizatorul după depunerea semnăturii biometrice în sistem susține o anumită identitate printr-un cod PIN, nume de login, etc. Drept răspuns, sistemul de recunoaștere validează sau anulează cerere utilizatorului, comparând semnătura biometrică actuală cu cea de înrolare, asociată cu o identitate particulară; [8]
2. *identificare.* În acest mod, sistemul încearcă să recunoască utilizatorul prin compararea semnăturii biometrice prezentate cu toate semnăturile înscrise în baza de date, făcând comparații fără a cere identitate specifică din partea utilizatorului. Identificarea este o componentă crucială în recunoașterea negativă, în cazul în care utilizatorul neagă deținerea unei identități particulare. De fapt, recunoașterea negativă împiedică o persoană să aibă mai multe identități. [8]

Principiile (etapele) de funcționare ale tehnologiilor biometrice sunt prezentate în figura 6

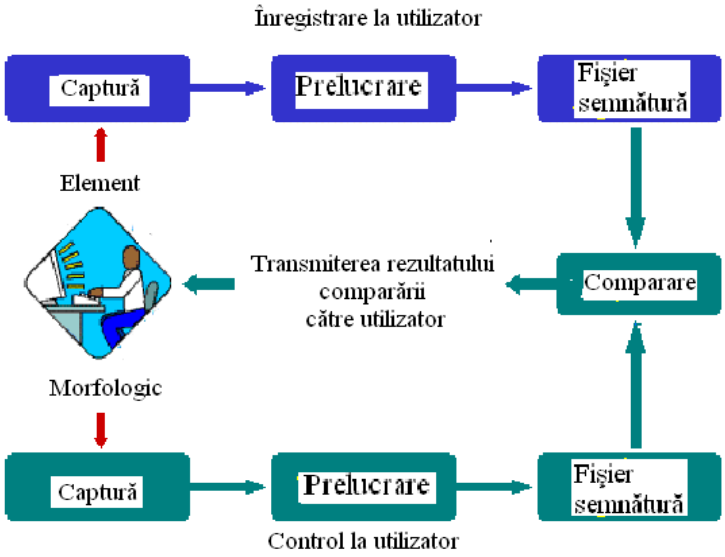


Fig.6 *Schema structurală de principiu a tehnologiei biometrice*

2.2 Identificarea facială

Una dintre cele mai importante aplicații ale analizei imaginilor o constituie recunoașterea feței. A fost o adevărată provocare construirea unui sistem automatizat care să fie capabil să identifice, să verifice şi să clasifice fețele persoanelor reprezentate în imaginile digitale.

"Imaginea digitală este o reprezentare codificată a unei imagini bidimensionale" [38]. Evoluția tehnologiilor moderne a permis o mai ușoară recunoaştere facială. Una dintre aceste tehnologii o reprezintă înlocuirea, în esență, a imaginii cu o versiune care accentuează cele mai relevante detalii pentru identificarea feței; în cazul gradientilor (o săgeată care arată fluxul de la lumină la întuneric pe întreaga imagine) aceasta implică înlocuirea fiecărui pixel cu o reprezentare a modului în care luminozitatea pixelului se compară cu pixelii din jurul acestuia.

O altă propunere se referă la așa-numita "proiecție" a unei fotografii 2D pe un model 3D, cum ar fi un cilindru. Înfășurarea unei fețe în jurul unei a treia dimensiuni poate, deseori, să dezvăluie forme de simetrie și caracteristici distinctive care sunt mult mai greu de găsit într-o imagine plană și statică.

Odată ce această pregătire a imaginii a fost finalizată, sistemul "codifică" în final fața sau își comprimă caracteristicile și modelele mai deosebite într-un fișier simplificat mai mic, care există doar pentru a face verificări încrucișate cu alte fețe codificate.

Întotdeauna, o imagine sau un flux video reprezintă **intrarea** într-un sistem de recunoaștere a feței. **Rezultatul** este o identificare sau o verificare a subiectului sau a subiectelor care apar în imagine sau video. Unele abordări definesc un *sistem de recunoaștere a feței* ca un proces în **trei** etape [34]: 1) detectarea facială; 2) extragerea caracteristicilor; 3) recunoașterea facială. Conform acestui punct de vedere, fazele de detecție a feței și de extragere a caracteristicilor ar putea să funcționeze simultan.

1) **Detectarea feței** este definită ca procesul de extragere a fețelor din diferite cadre. Deci, sistemul identifică în mod pozitiv o anumită regiune a imaginii ca fiind o față.
2) Următoarea etapă - **extragerea caracteristicilor** - implică obținerea de caracteristici faciale relevante din datele de intrare.
3) În final, sistemul **recunoaște fața**. Având ca obiectiv recunoașterea facială, sistemul stabilește o identitate dintr-o bază de date. Această fază implică o metodă de *comparare*, un *algoritm de clasificare* și o *măsurare de precizie a similarității*.

Unele sisteme **detectează și localizează** fețele în același timp, altele aplică mai întâi o rutină de detectare și apoi, dacă rezultatele sunt pozitive, încearcă să localizeze fața. Pot fi necesari algoritmi de urmărire. În mod obișnuit, algoritmii de detectare a feței utilizează aceiaşi pași generali În primul rând, se efectuează o reducere a dimensiunii datelor, pentru a atinge un timp de răspuns acceptabil. Următoarea fază implică, **extragerea caracteristicilor sau a metricii faciale.** Acestea vor fi apoi ponderate, evaluate sau comparate pentru a decide dacă există o față și unde este aceasta. În cele din urmă, unii algoritmi aplică o rutină de învățare și introduc noile date în modelele existente.

Tehnicile folosite în detectarea fețelor sunt adesea folosite în recunoașterea feței.

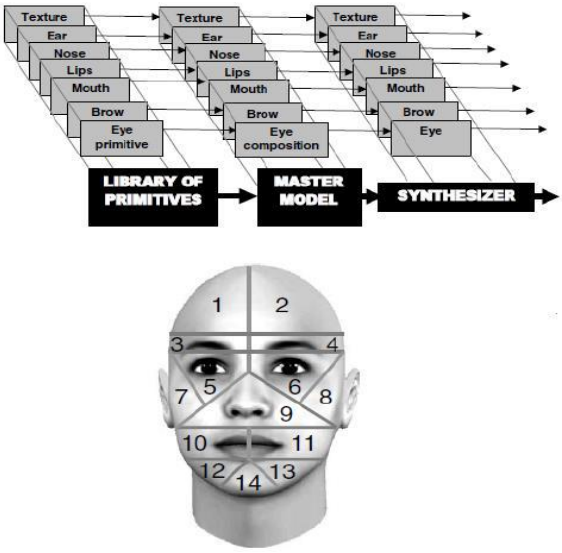


Fig. 7 *Partiționarea feței pentru analiza facială* [38]

Conform literaturii de specialitate, recunoașterea facială este realizată într-un proces ce cuprinde cinci etape: 1. capturarea imaginii; 2. detectarea facială; 3. extragerea caracteristicilor; 4. compararea șabloanelor; 5. găsirea elementelor pereche.

2.2.1. Capturarea imaginii

Primul pas al acestui proces este obținerea materialului pentru analiză, și anume o imagine a feței. Sistemele de recunoaștere facială sunt împarțite în două tipuri generale: acelea care folosesc imagini statice ale feței și cele care analizează imagini dinamice ale feței dintr-o filmare video.

2.2.2 . Detectarea facială

Detectarea facială reprezintă etapa a doua și cu ajutorul software-ului este detectată locația tuturor chipurilor din imaginea capturată. Detectarea facială este considerată un caz particular de detectare a obiectelor, intitulat "object-class detection". "Object-class detection" urmărește să recunoască și să găsească instanțe de categorii de interese în imaginile de intrare. [48], [79]

2.2.3. Extragerea caracteristicilor

În recunoașterea formelor și în procesarea de imagine, extragerea caracteristicilor este o formă specială de reducere a dimensionalitatii. 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. Extragerea caracteristicilor este efectuată prin arhivarea informației, reducerea dimensiunii, extracție cu scoatere în relief și curățare a 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**. [9], [48] Rezultatul procesului este generarea șablonului.

2.2.4. Compararea șabloanelor

Pasul patru este de a compara șablonul generat la pasul anterior cu caracteristicile existente într-o bază de date de fețe înregistrate. Într-o aplicație de identificare, acest proces produce scoruri care indică cât de bine se potrivește șablonul generat cu cele înregistrate în baza de date. În aplicația de verificare, șablonul generat este comparat numai cu un șablon din baza de date, acela al identității pretinse.[79]

2.2.5. Găsirea elementelor pereche

Pasul final este de a determina dacă scorurile obținute în etapa patru sunt suficient de mari pentru a declara o potrivire între șablonul generat și cel înregistrat. Normele care reglementează nivelul la care se poate declara o potrivire între cele două șabloane sunt de cele mai multe ori configurabile de către utilizatorul final, astfel încât acesta poate determina nivelul de securitate la care sistemul trebuie să funcționeze în funcție de utilitate.[79]

2.3 Algoritmi 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 fețele ca o combinație liniară a acestor imagini. Analiza componentelor principale (PCA) este un exemplu foarte larg răspândit referitor la astfel de metode.

Yan, Kriegman și Ahuja au elaborat o clasificare, care a fost acceptată de către specialiştii în domeniu. Metodele sunt împărțite în patru categorii. Aceste categorii se pot suprapune, astfel încât un algoritm ar putea aparține la două sau mai multe categorii. Clasificarea poate fi făcută după cum urmează:

1. *Metode bazate pe cunoaștere*

Sunt metode bazate pe codificarea cunoștințelor despre chipurile umane, fundamentate pe reguli. Ele încearcă să surprindă cunoștințele despre fețe și să le transpună într-un set de reguli. Este ușor să fie deduse câteva reguli simple. De regulă, fața este compusă din ochi, ambii ochi fiind dispuşi simetric, ariile din jurul ochilor fiind mai închise la culoare decât obrajii. Caracteristicile feței pot fi distanța dintre ochi sau diferența de intensitate a culorii dintre zona ochiului și zona inferioară.

2. *Metodele bazate pe caracteristici invariante*

Metoda invariantă a metodei se bazează pe extragerea caracteristicilor invariante care există chiar și atunci când poziția din care este luată imaginea sau condițiile de iluminare variază. Principalul dezavantaj al acestei metode este performanța slabă a acesteia în prezența obturării sau zgomotului. Detecția feței folosind segmentarea culorii pielii este cea mai răspândită metodă bazată pe această abordare.

3. *Metode de potrivire a şabloanelor*

Metodele de potrivire a șabloanelor încearcă să definească fața ca o funcție. Se caută găsirea unui tipar standard pentru diversele categorii de fețe. Definirea caracteristicilor distincte se realizează independent. De exemplu, fața este compusă din ochi, conturul feței, nasul și gura. De asemenea, un model de față poate fi construit de muchii (limite). Dar aceste metode se limitează la fețe care sunt frontale și neblocate. O față poate fi, de asemenea, reprezentată ca o siluetă.

4. *Metode bazate pe înfățișare*

Șabloanele din metodele bazate pe aspect sunt învățate din exemplele din imagini. În general, metodele bazate pe *înfățişare* se fundamentează pe procedee din analiza statistică și cele de învățare mecanică pentru a găsi însuşirile esențiale ale imaginilor feței. Unele metode bazate pe aspect funcționează într-o rețea probabilistică. O imagine sau un vector de funcții este o variabilă aleatoare care poate sau nu să fie parte a unei fețe. O altă abordare este definirea unei funcții discriminante între cele două clase față și non-față. Aceste metode sunt, de asemenea, utilizate în extragerea caracteristicilor pentru recunoașterea feței.

2.3.1. PCA (Analiza Componentelor Principale)

Analiza componentei principale (PCA) este cel mai utilizat instrument în analiza multivariată. PCA este o tehnică statistică care transformă un set de date cu mai multe variații ale variabilelor intercorelate, într-un set de date noi, format din combinații liniare necorelate ale variabilei originale. PCA calculează axele necorelate care calculează suma maximă a variațiilor în imagine. [32]

PCA este o tehnică eficientă dacă se lucrează cu volume mari de date. De asemenea, metoda este utilă pentru reducerea numărului dimensiunilor spațiului caracteristicilor, dar cu păstrarea caracteristicilor principale pentru a minimiza pierderile de informație.

Recunoașterea feței reprezintă o problemă complexă din domeniul analizei imaginilor și al viziunii calculatorului. Spațiul de stocare a informațiilor este una dintre cele mai importante provocări în proiectarea sistemului biometric. Din cauza lățimii de bandă și a capacității de stocare limitate,

imaginile trebuie comprimate înainte de stocare și transmitere. Există **două tipuri fundamentale de tehnici de compresie**; *compresia fără pierderi* (lossless) şi *compresia cu pierderi* (lossy). Compresia cu pierderi este utilizată frecvent la comprimarea datelor audio, video, stop-cadrelor în aplicații cum ar fi media streaming. Dimpotrivă, compresia fără pierderi este necesară pentru texte şi fişiere de date cu ar fi registre bancare şi documente text. În multe cazuri, este convenabilă întocmirea unui fişier fără pierderi care poate fi utilizat la generarea de fişiere pentru diferite scopuri.

2.3.2. ICA (Analiza componentelor independente)

Analiza Componentelor Independente a (ICA), este o tehnică statistică care dezvăluie factorii ascunși care stau la baza unor seturi de variabile sau semnale aleatoare. Informațiile care descriu o față pot fi incluse în ambele dependențe, fie ele de ordin liniar, cât și dependențe de ordin mare, printre pixelii imaginii. Aceste dependențe de ordin mare pot fi capturate în mod eficient printr-o reprezentare în spațiu ICA. Analiza componentelor independente (ICA) minimizează atât dependențele de ordinul al doilea cât și pe cele de ordin superior în datele de intrare și încearcă să găsească baza de-a lungul căreia datele (atunci când sunt proiectate pe ele) sunt statistic independente. [6] Aceste coordonate sunt conținute în matricea de amestecare A = W-1.

Bartlett et al. au furnizat două arhitecturi ale ICA, pentru îndeplinirea sarcinii de recunoaștere a feței [48]:
1. **Arhitectura I** – Imagini de bază statistic independente
2. **Arhitectura II** – reprezentarea codului factorial.

Cercetătorii care au abordat acest subiect consideră metrica indusă de ICA ca fiind superioară altor metode, în sensul că poate furniza o reprezentare mai robustă la efectul zgomot, cum ar fi variațiile de lumină. [3]

2.3.3. Clasificatorul Haar

O caracteristica Haar constă în două sau mai multe regiuni dreptunghiulare, verticale sau orizontale adiacente, iar valoarea sa este diferența între sumele de pixeli din cadrul acestor regiuni dreptunghiulare.[42] Variațiile de contrast între grupurile de pixeli sunt folosite pentru a determina zonele întunecate si zonele de lumina relative. Două sau trei grupe adiacente, cu o variatie relativa de contrast, dintr-o caracteristica Haar sunt utilizate pentru a detecta o imagine. Functiile Haar pot fi scalate cu ușurință prin creșterea sau reducerea dimensiunii grupului de pixeli examinat. Acest lucru permite folosirea diferitelor functii pentru detectarea obiectelor de diverse dimensiuni.[48]

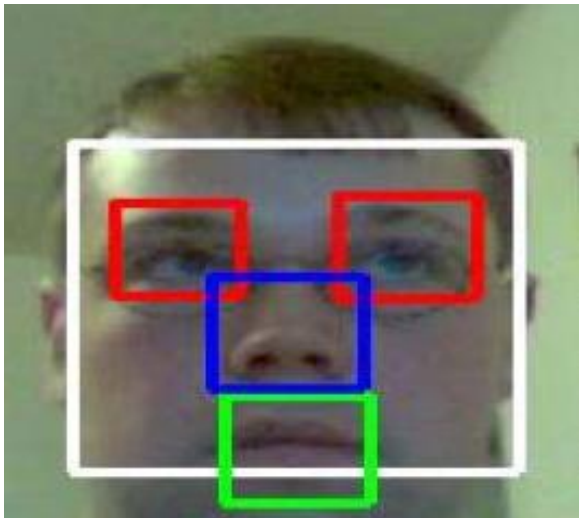


Fig. 13 *Exemplu de detecție cu ajutorul clasificatorului Haar* [48]

2.3.4. LDA (Analiza liniară discriminantă)

Analiza liniară discriminantă (LDA) este o metodă bine cunoscută pentru reducerea dimensiunii în recunoaşterea modelelor. Ea proiectează datele originale de mari dimensiuni pe un spațiu dimensional scăzut, unde toate clasele sunt bine separate prin maximizarea coeficientului Raleigh. LDA creează o combinație liniară de caracteristici independente care produce cea mai mare diferența între clasele dorite. Ideea de bază in cazul LDA este de a găsi o transformare liniară, astfel încât grupurile de caracteristici să poată fi separate după transformare, care poate fi realizată printr-o analiză a matricei de dispersie.

2.4 Dificultăți şi neajunsuri apărute la sistemele de verificare biometrică

- **Susceptibilitatea senzorului biometric la date zgomotoase sau greşite**: (o imagine de amprentă cu o cicatrice sau o mostră de voce modificată de frig sunt exemple de date zgomotoase)
  Trăsătura biometrică capturată poate fi distorsionată datorită condițiilor imperfecte de achiziție. Această limitare poate fi văzută în aplicațiile care utilizează recunoașterea facială. Calitatea imaginilor faciale capturate poate fi afectată de condițiile de iluminare și de expresiile feței. Datele zgomotoase pot apărea, de asemenea, din senzorii defecți sau întreținuți necorespunzător.
- **Este posibil să nu fie compatibilă cu anumite grupuri de populație**. Imaginile cu amprentă digitală ar putea să nu fie capturate corespunzător pentru vârstnici și pentru copiii mici din cauza amprentelor digitale estompate (stinse) sau incomplet formate.
- **Variații „intraclass”:** Aceste variații sunt cauzate, în mod obișnuit, de un utilizator care interacționează incorect cu senzorul (de exemplu, prezintă o poziție incorectă a feței) sau când caracteristicile unui senzor sunt modificate în timpul autentificării (de exemplu, senzori optici față de senzorii tactili pentru amprente).
- **În cadrul unei populații mari, biometria unimodală este predispusă la asemănări inter-clasice**. Recunoașterea facială poate să nu funcționeze corect pentru gemenii identici, deoarece este posibil ca aparatul foto să nu poată distinge între cele două subiecte. Din această cauză pot apărea potriviri eronate.
- **Absența universalității:** Este posibil ca sistemul biometric să nu poată achiziționa date biometrice semnificative de la un subset de utilizatori. De exemplu, un sistem biometric de amprente poate extrage caracteristici incorecte din amprentele anumitor persoane, datorită calității slabe a crestelor papilare.
- **Atacurile informatice:** Sistemele biometrice unimodale sunt destul de vulnerabile la atacurile informatice în care datele pot fi imitate sau falsificate. Se menționează crearea unei clone a amprentei digitale folosind tehnica Matsumoto “degetele de gumă” sau folosind urme latente ale amprentelor de pe anumite obiecte care au reuşit să “păcălească” sistemele de cele mai multe ori.

Trebuie remarcat faptul că detectarea facială nu permite obținerea de rezultate exacte pentru niciuna dintre tehnicile uzuale aplicate.

Principalii factori care pot crea dificultăți în detectarea automată a fețelor (în imagini bidimensionale):

- poziția şi orientarea acestora în imagine (frontal, profil, sub un unghi etc.) - anumite caracteristici faciale (ochi, nas) putând fi parțial sau total ascunse; [74]
- prezența / absența unor componente structurale - unele caracteristici faciale precum barbă, mustață, ochelari putând fi, sau nu, prezente şi existând o mare variabilitate a acestora din punct de vedere al formei, culorii sau dimensiunilor;
- expresia facială - geometria feței fiind afectată de aceasta; [74]
- obturarea - fețele putând fi parțial mascate (acoperite) de alte obiecte (inclusiv alte fețe);
- condițiile în care a fost realizată fotografia - iluminarea (spectrul, poziția şi/sau distribuția sursei / surselor de lumină, intensitatea) şi caracteristicile aparatului foto (lentilele, senzorul) afectând foarte puternic felul în care o figură apare în imagine. [74]

2.5 Cadrul legal comunitar aplicabil în materia datelor biometrice

O preocupare constantă a legiuitorului, atât național cât comunitar, a fost aceea de reglementare a unui cadru legal adecvat de protecție a datelor cu caracter personal. Această preocupare rezidă în nevoia de a asigura o utilizare corectă și legală a datelor personale ale individului, supusă unui control strict care să impiedice orice formă de abuz asupra personalității și libertății individului. În lumina principiilor fundamentale care guvernează valorile social-umane individuale, legiuitorul a instituit atât pe plan național cât și pe plan european o serie de legi și, respectiv, directive care consacră, în mod imperativ, regulile cu privire la protecția datelor cu caracter personal.

Totodată, progresul tehnologic foarte rapid a impus editarea unor norme juridice în măsură să împiedice folosirea abuzivă a datelor cu caracter personal. În acest sens, norma legală vine sa preîntâmpine acest pericol și asigură protecția individului.

Legat de cele afirmate mai sus, trebuie spus că tehnicile de recunoaștere facială au cunoscut o majoră îmbunătățire, ceea ce ce constituie deopotrivă atât un succes tehnologic cu reale beneficii, cât și un potențial pericol pentru sociatate.

Regulamentul european de protecție a datelor cu caracter personal este, exact, o astfel de lege nouă, aplicabilă tuturor statelor comunitare, care se pliază pe noile realități.

2.6 Concluzii

Biometria reprezintă un set de tehnologii (numite tehnologii biometrice) care exploatează caracteristicile fizice sau comportamentale ale omului, cum ar fi amprenta, semnătura, irisul, vocea, fața, mersul și un gest al mâinii pentru a putea realiza diferențierea persoanelor. Parametrii biometrici menționați anterior sunt unici pentru individ și există puține șanse ca alte persoane să înlocuiască aceste caracteristici, astfel încât tehnologiile biometrice sunt considerate cele mai puternice din punctul de vedere al securității.

În concluzie:

- Biometria devine treptat o parte a vieții noastre de zi cu zi și este una dintre provocările majore pentru o lume mai sigură. Piața produselor de autentificare și identificare se află în ascensiune, datorită nevoii în creștere de securitate personală în sectorul privat, profesional și public.
- Biometria este din ce în ce mai des utilizată pentru cărți de identitate, în aeroporturi, instituții penitenciare, pentru acces în sedii securizate, vot electronic, securitatea plăților bancare sau tranzacțiile prin Internet.
- Biometria este o alternativă la parole și la alte elemente de identificare pentru a elimina orice urmă de îndoială cu privire la identitate. Aceasta face posibilă verificarea faptului că utilizatorul este persoana care pretinde a fi.

Identificarea facială reprezintă subiectul abordat în al doilea subcapitol al capitolului 2.

În comparație cu alte sisteme biometrice, cum ar fi amprentele, măsurătorile de iris, sistemul de detectare facială nu funcționează cu o precizie extremă, dar analiza fețelor are câteva avantaje. În primul rând, sistemul de recunoaștere a feței poate utiliza camere video standard (spre deosebire de costul și complexitatea captării amprentelor digitale sau a imaginii irisului) și, în al doilea rând, chipul uman este capturat, chiar fără să știe și poate fi utilizat pentru sistemele de securitate.

Obiectivul unui astfel de sistem este de a găsi cea mai bună potrivire din secvența de imagini capturate prin utilizarea camerei (aparatului de fotografiat) cu o imagine dată. Folosind un set de baze de date de imagini, sistemul de recunoaștere a feței ar trebui să poată identifica sau confirma una sau mai multe persoane din scenă. Înainte de recunoașterea feței, sistemul trebuie să determine dacă există sau nu o față într-o imagine dată sau într-o secvență video a imaginilor. Odată ce detectarea feței a fost realizată, regiunea feței trebuie izolată din scenă pentru recunoașterea feței. Detectarea feței și extragerea trăsăturilor feței sunt deseori efectuate simultan.

Metodele de extragere a trăsăturilor feței, reprezintă partea principală (nucleul) algoritmilor de recunoaștere facială, deoarece utilizarea directă a pixelilor imaginii în sistemul de timp real nu este posibilă, din cauza cantității mari de date.

De cele mai multe ori, pentru a reduce seturile de date se utilizează metoda Analizei Componentelor Principale (PCA), care descrie seturile de date în calitate de coeficienți, care evaluează variația datelor. Pentru reducerea seturilor de date sunt utilizate și alte metode, cum ar fi analiza independentă a componentelor (ICA), analiza liniară discriminantă (LDA), și Clasificatorul Haar.

Ultimul subcapitol analizează câteva probleme şi limitări cu care se confruntă detectarea și recunoașterea facială în vederea unei mai bune detectări și acurateți a recunoașterii. Deşi oferă multiple avantaje, persistă întrebări cu privire la eficacitatea sistemelor biometrice ca mecanisme de securitate sau de supraveghere, gradul lor de utilizare și gestionabilitate, oportunitatea în contexte foarte diferite, impactul social, efectele asupra vieții private și implicațiile juridice și politice.

CAPITOLUL 3

CERCETARE STATISTICĂ PRIVIND DETERMINAREA OPINIILOR MANAGERILOR DE BIBLIOTECĂ ȘI A BIBLIOTECARILOR CU PRIVIRE LA NEVOIA DE IMPLEMENTARE A UNUI NOU SISTEM DE SECURITATE ȘI SISTEMELE EXISTENTE DIN BIBLIOTECI

3.1 Descrierea instrumentelor folosite în cadrul cercetării statistice

3.1.1 Scopul și obiectivele care stau la baza cercetării

Studiul a plecat de la dorința noastră de a propune un sistem complementar permisului de intrare în bibliotecă, bazat pe recunoașterea facială a utilizatorilor. Cercetarea a avut drept **obiectiv** determinarea opiniilor bibliotecarilor, atât cu funcții de execuție, cât și de conducere, cu privire la sistemele de securitate din biblioteci, precum și referitor la implementarea unui sistem de recunoaștere facială a utilizatorilor.

3.1.2 Ipotezele cercetării

1. Bibliotecarii preocupați de securitatea persoanelor, în contextul terorismului, sunt dornici să implementeze un sistem de recunoaștere facială în biblioteca în care activează.
2. Bibliotecarii care cred că cel mai potrivit sistem de recunoaștere biometrică pentru securitatea colecțiilor și a persoanelor este recunoașterea facială, ar fi de acord cu implementarea unui astfel de sistem în biblioteca în care activează.
3. Bibliotecarii care au încredere în sistemele de recunoaștere facială sunt de acord cu implementarea unui astfel de sistem în biblioteca în care activează.
4. Bibliotecarii care activează în biblioteci mari, sunt de acord cu implementarea unui sistem de recunoaștere facială.
5. Cu cât crește nivelul de pregătire al bibliotecarilor, cu atât sunt mai dispuși să implementeze un sitem de recunoaștere facială în biblioteca în care activează.
6. Bibliotecarii cu funcție de conducere sunt mai dispuși să implementeze un sistem de recunoaștere facială în biblioteca în care activează.
7. Bibliotecarii cu experiență la locul de muncă mai mare de 31 de ani sunt mai dispuși să implementeze un sistem de recunoaștere facială în biblioteca în care activează.

3.1.3 Materialul și metoda

Metodologia de lucru utilizată, relevantă pentru identificarea opinilor respondenților față de securitatea colecțiilor și a persoanelor, a constat în conceperea unui chestionar online, alcătuit din 16 întrebări. Înainte de completarea chestionarelor li s-a atras atenția respondenților în ceea ce priveşte regimul de confidențialitate al datelor colectate. Pentru realizarea chestionarului s-a pornit de la definiția securității în bibliotecă și având în vedere obiectivele și ipotezele formulate.

Studiul a cuprins 177 de respondenți din România și din străinătate. A fost efectuat în lunile februarie/martie 2017. Utilizarea softului SPSS (Statistical Package for the Social Sciences), precum și a programului Excel a făcut posibilă prelucrarea datelor obținute.

3.1.4 Descrierea loturilor de subiecți

Pentru a identifica opinia bibliotecarilor, cu privire la securitatea colecțiilor și a persoanelor, au fost investigate două loturi de subiecți. Chestionarele au fost distribuite în cât mai multe țări, pentru o mai bună reprezentativitate.

Primul lot cuprinde 145 de respondenți, dintre care 93 sunt din România și 50 din Moldova.

Tabelul 2. Distribuția respondenților din România și Moldova, în funcție de țară

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	România	93	64.1	65.0	65.0
	Moldova	50	34.5	35.0	100.0
	Total	143	98.6	100.0	
Missing	System	2	1.4		
Total		145	100.0		

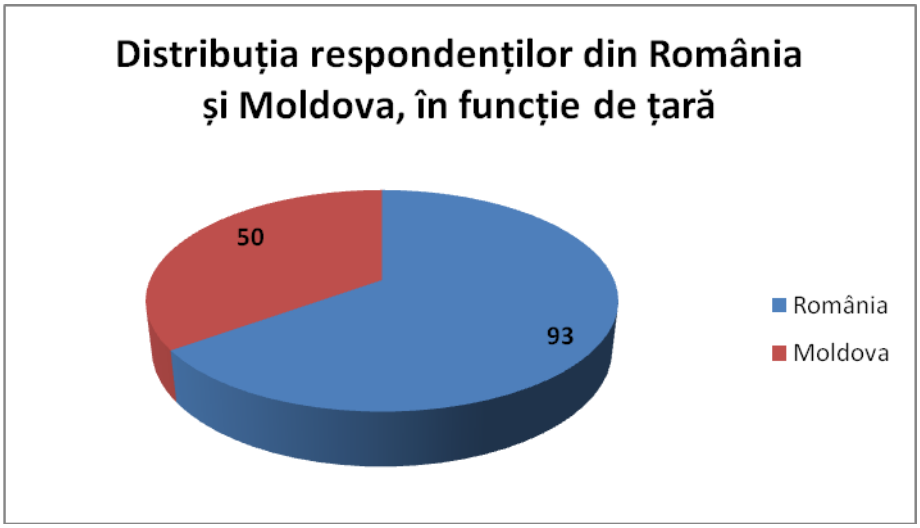


Fig. 16 *Distribuția respondenților din România și Moldova, în funcție de țară*

După cum se poate observa în figura de mai jos (Figura 17), nivelul de educație al respondenților este ridicat. Dintr-un total de 145 de subiecți din România și Moldova, 43,4% au studii universitare, 34,5% postuniversitare și 15,9% doctorale.

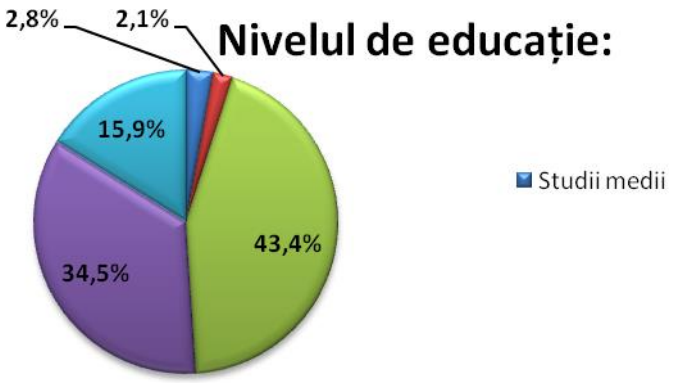


Fig. 17 *Nivelul de educație al respondenților din România și Moldova*

Chestionarele au fost distribuite atât celor cu funcție de conducere, cât și celor cu funcție de execuție. Astfel, un procent de 30,3% îi reprezintă pe cei cu funcții de conducere și un procent de 66,2% pe cei cu funcție de execuție.

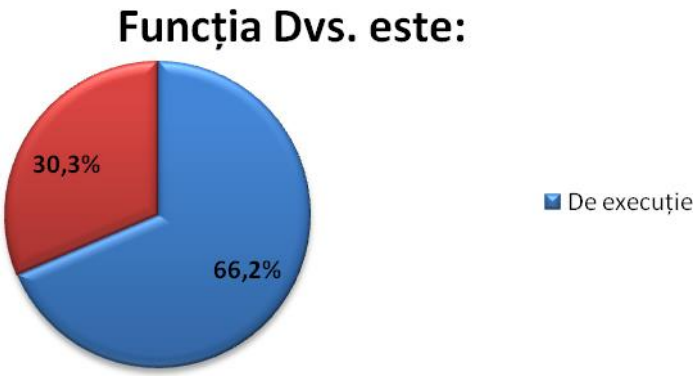


Fig. 18 *Funcția respondenților din România și Moldova*

Cei mai mulți dintre respondenții din România și Moldova, 44,1% au acumulat experiență la locul de muncă, cuprinsă între 21 și 30 de ani, 22,1% se încadrează între 11 și 20 de ani de experiență la locul de muncă, 12,4% între 31 si 40 de ani, un procent mai mic, de 10,3% au mai puțină experiență, fiind cuprinsă între 5 și 10 ani și doar 5,5% au o vechime de peste 40 de ani.

Fig. 19 *Experiența la locul de muncă a respondenților din România și Moldova*

Mai mult de jumătate din primul Lot de subiecți activează într-o bibliotecă universitară, 28,3% își desfășoară activitatea într-o bibliotecă școlară, 5,5% în una publică și în egală măsură, de 2,8%, respondenții activează în biblioteci specializate, ale Academiei, precum și alte situații, cum ar fi Biblioteca militară națională, Centru de documentare și informare, biblioteci cu acces limitat.

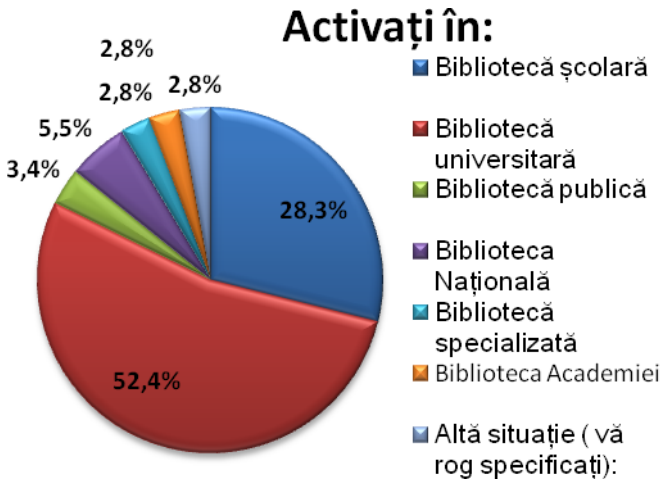


Fig. 20 *Distribuția respondenților din România și Moldova, în funcție de biblioteca în care activează*

În ceea ce privește al doilea lot, acesta este format din 32 de respondenți, dar de data aceasta din străinătate. Am dorit să obținem și părerea celor din afara țării cu privire la proiectul pe care dorim să îl implementăm, deoarece securitatea persoanelor în spațiile publice este o problemă cu care ne confruntăm în prezent, terorismul internațional putându-se manifesta oriunde în lume. Astfel, țările participante la sondaj sunt: Albania, Armenia, Belarus, Bosnia și Herțegovina, Bulgaria, Grecia, Irlanda, Muntenegru, Norvegia, Regatul Unit al Marii Britanii, Rusia, Serbia, Turcia, Ungaria. Chestionarul a fost tradus în engleză, fiind o limbă de circulație internațională.

La fel ca și în cazul României, nivelul de educație al respondenților din străinătate este foarte ridicat, toți având mai mult decât studii medii. Cei mai mulți respondenți, 34,4% sunt absolvenți de studii postuniversitare, 31,3% au studii universitare și 25% au urmat o școală doctorală.

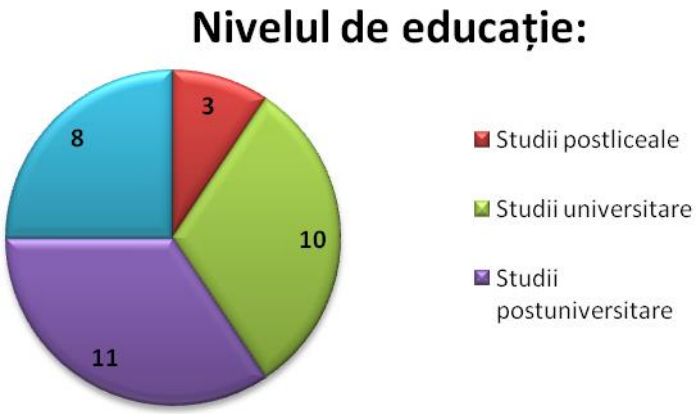


Fig. 21 *Nivelul de educație al respondenților din Lotul 2*

Cei mai mulți dintre cei intervievați în străinătate dețin un post în managementul personalului, 28,1% reprezintă personalul de conducere și doar 21,9% au funcție de execuție.

Fig. 22 *Descrierea postului de muncă a respondenților din Lotul 2*

Din totalul de 32 de respondenți, din mai multe țări, 4 au exeperiență la locul de muncă mai mică de 5 ani, 10 dintre cei intervievați au experiență cuprinsă între 5 și 10 ani, 3 între 11 și 20 de ani, 9 între 21 și 30 de ani și 6 între 31 și 40 de ani.

Fig. 23 *Experiența la locul de muncă a respondenților din Lotul 2*

Majoritatea respondenților din Lotul 2 activează într-o bibliotecă universitară, 5 în biblioteca Academiei și 3 în biblioteci specializate.

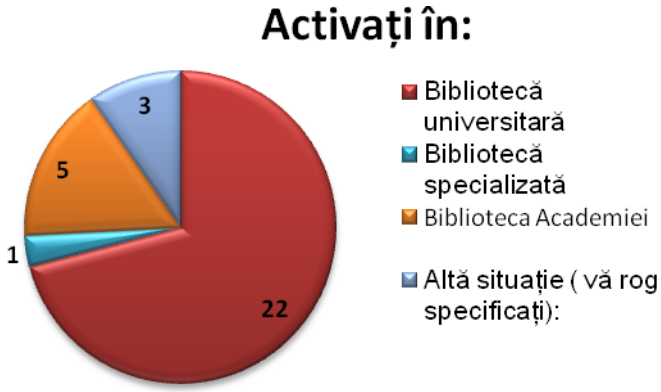


Fig. 24 *Distribuția respondenților din Lotul 2, în funcție de biblioteca în care activează*

3.2 Rezultatele cercetării

3.2.1 Descrierea rezultatelor

La întrebarea "În general, cât de mulțumit sunteți de securitatea colecțiilor din biblioteci?" majoritatea respondenților din România și Moldova, 45,5%, sunt destul de mulțumiți, 33,1% se consideră destul de nemulțumiți cu privire la acest aspect, 8,3% sunt foarte mulțumiți și 10,3% foarte nemulțumiți.

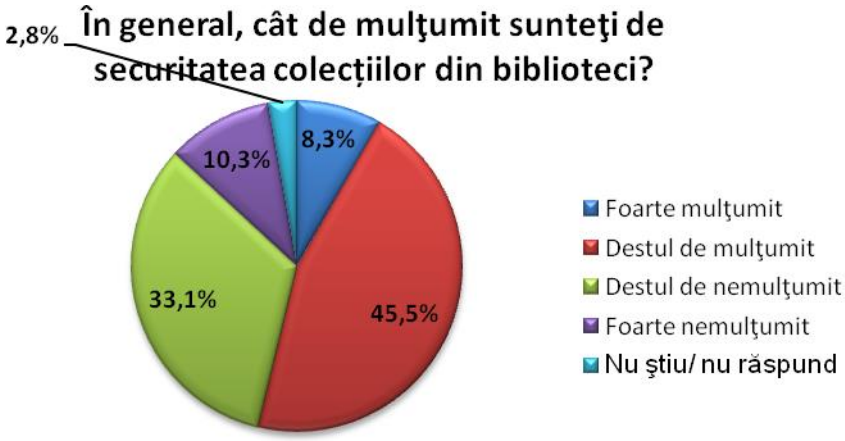


Fig. 25 *Mulțumirea bibliotecarilor din România și Moldova cu privire la securitatea colecțiilor din biblioteci*

Analizând răspunsurile bibliotecarilor din Lotul 2, am constatat că majoritatea sunt destul de mulțumiți de securitatea colecțiilor din biblioteci, dar sunt și 9 bibliotecari, destul de nemulțumiți și 3 foarte nemulțumiți de acest aspect.

Fig. 26 *Mulțumirea bibliotecarilor din Lotul 2 cu privire la securitatea colecțiilor din biblioteci*

Din graficul realizat pe baza analizei datelor colectate, se poate observa că cea mai mare problemă privind securitatea colecțiilor din bibliotecă, cu care se confruntă respondenții din România și Moldova este pierderea exemplarelor. 19,3% consideră că cea mai mare problemă este lipsa spațiului de depozitare, 15,9% susțin că furtul este principala problemă în securitatea colecțiilor, 6,9% apreciază că vandalismul este o problemă deosebit de importantă și 4,8% neatenția angajaților.

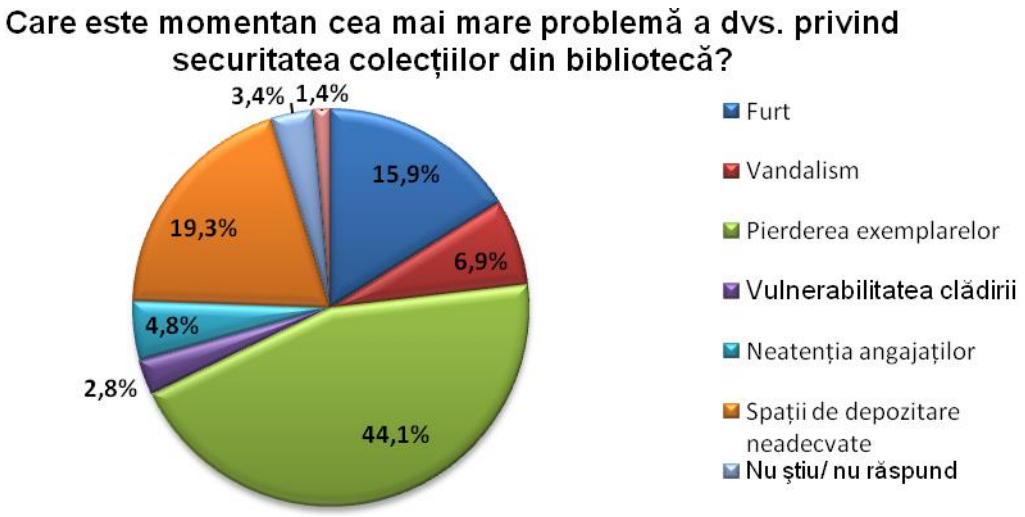


Fig. 27 *Cea mai mare problemă a respondenților din România și Moldova cu privire la securitatea colecțiilor din biblioteci*

Cei mai mulți respondenți din Lotul 2, consideră că neatenția angajaților este cea mai mare problemă privind securitatea colecțiilor din biblioteca în care activează, 7 au spus ca vandalismul reprezintă cea mai mare problemă, un număr de 6 bibliotecari au apreciat că vulnerabilitatea clădirii se situează pe prima poziție și 2 au susținut că spațiile de depozitare reprezintă principala problemă privind securitatea colecțiilor.

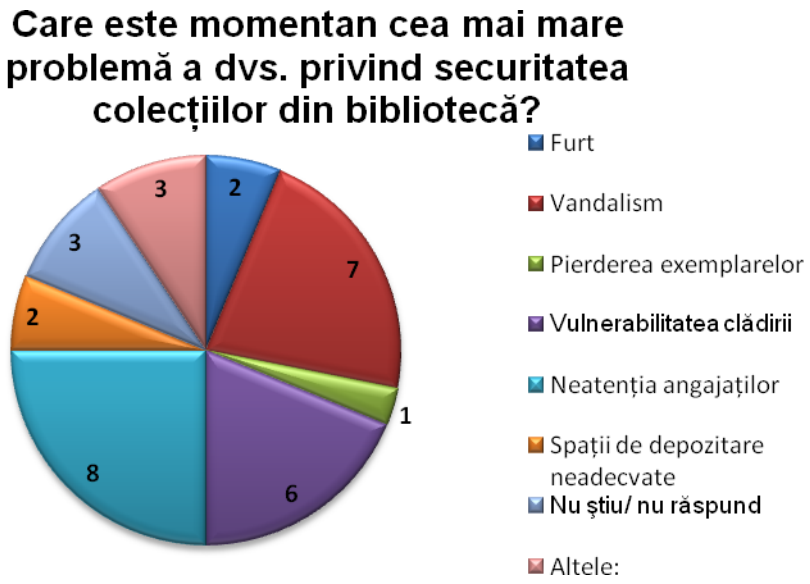


Fig. 28 *Cea mai mare problemă a respondenților din Lotul 2 cu privire la securitatea colecțiilor din biblioteci*

Dintr-un total de 145 de respondenți din România și Moldova, cel mai mare procent, 56,6% au afirmat faptul că s-a întâmplat ca cineva să intre în bibliotecă fără a avea permis, iar 35,2% a spus că nu s-a întâmplat acest lucru niciodată în biblioteca în care activează.

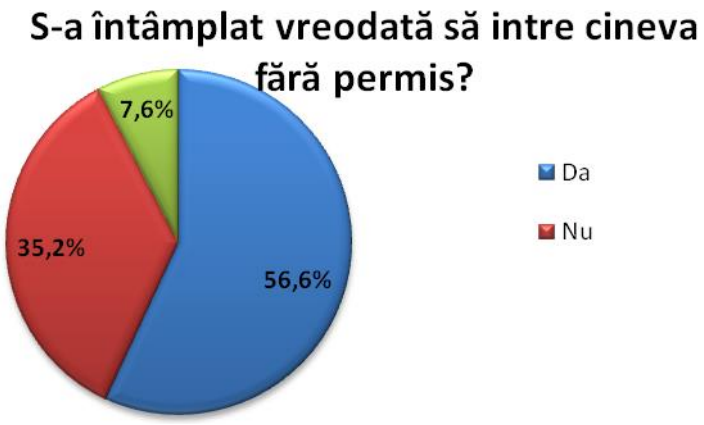


Fig. 29 *Răspunsurile bibliotecarilor, din România și Moldova, la întrebarea "S-a întâmplat vreodată să intre cineva fără permis?"*

În urma analizei datelor reiese faptul că 16 bibliotecari din lotul format din respondenți din mai multe țări, au recunoscut că s-a întâmplat să intre anumite persoane în bibliotecă fără a deține un permis și un număr de 11 respondenți au afirmat că acest lucru nu s-a întâmplat în cazul bibliotecii lor.

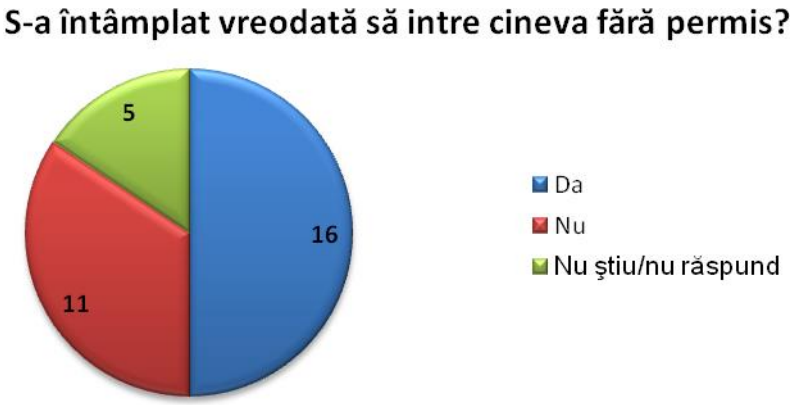


Fig. 30 *Răspunsurile bibliotecarilor, din Lotul 2, la întrebarea "S-a întâmplat vreodată să intre cineva fără permis?"*

Referitor la problema terorismului, 51,7%, adică 75 din 145 de respondenți, din România și Moldova, consideră că ar trebui să se ia măsuri suplimentare cu privire la securitatea persoanelor din bibliotecă, 33,1% nu s-au gândit la acest lucru și 8,3% au fost de părere că securitatea actuală este suficientă.

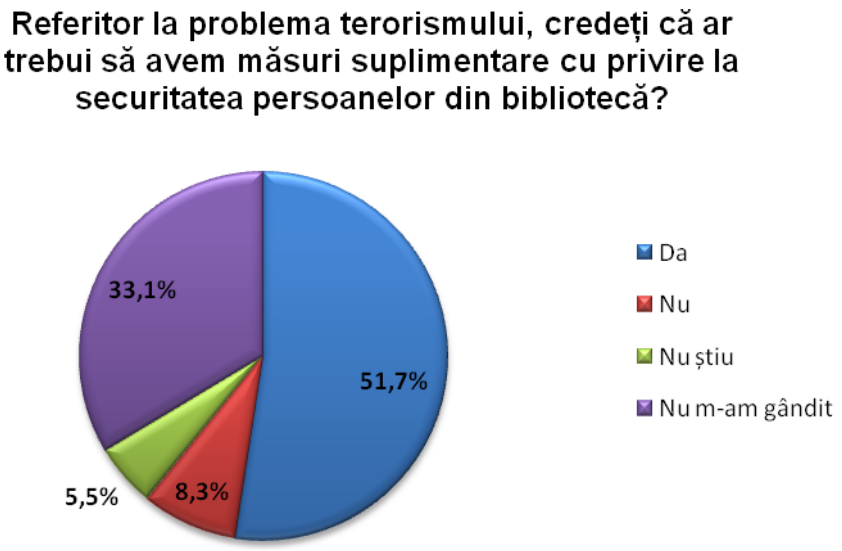


Fig. 31 *Părerea respondenților din România și Moldova, referitor la măsurile suplimentare cu privire la securitatea persoanelor din bibliotecă*

13 bibliotecari din Lotul 2 au spus că este necesar să luăm măsuri suplimentare cu privire la securitatea persoanelor din bibliotecă, în contextul terorismului. 12 nu au luat în calcul această problemă și 6 consideră că nu trebuie luate măsuri suplimentare.

Fig. 32 *Părerea respondenților din Lotul 2, referitor la măsurile suplimentare cu privire la securitatea persoanelor din bibliotecă*

Dintr-un total de 145 de respondenți din România și Moldova, 54,5%, adică un număr de 79 de bibliotecari, sunt de părere că sistemele de recunoaștere biometrică sunt cele mai sigure sisteme de securitate ce pot fi folosite în biblioteci, iar 33,1%, adică 48 din totalul respondenților consideră că Sistemul RFID este cel mai sigur.

Fig. 33 *Părerea respondenților din România și Moldova, referitor la cel mai sigur sistem de securitate, ce poate fi folosit în biblioteci*

Analizând răspunsurile bibliotecarilor din Lotul 2 putem observa că 19 dintre aceștia cred că sistemele biometrice sunt cele mai sigure metode de securitate ce pot fi folosite în biblioteci și 12 consideră că sistemul RFID este cel mai sigur sistem de securitate.

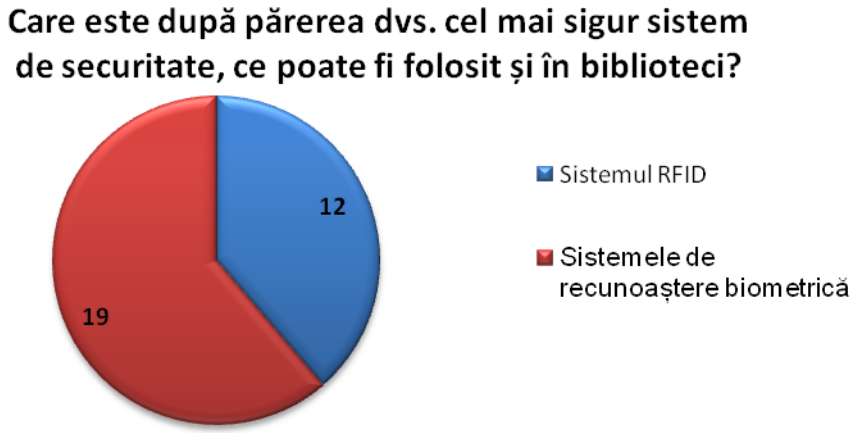


Fig. 34 *Părerea respondenților din Lotul 2, referitor la cel mai sigur sistem de securitate, ce poate fi folosit în biblioteci*

39,3% dintre respondenții din România și Moldova, cred că cel mai potrivit sistem de securitate biometric pentru biblioteci este cel bazat pe recunoaștere facială, un procent de 13,8% sunt de părere că cel dactiloscopic este cel mai potrivit și un procent destul de mare de 33,8% nu au putut da un răspuns cu privire la această problemă.

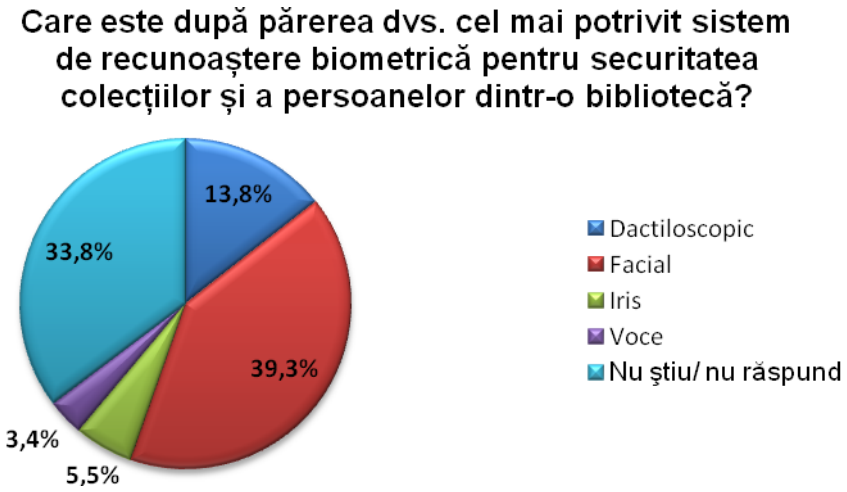


Fig. 35 *Cel mai potrivit sistem de securitate a colecțiilor și a persoanelor dintr-o bibliotecă, conform respondenților din România și Moldova*

Cea mai mare parte a respondenților din Lotul 2 nu au putut aprecia care este cel mai potrivit sistem biometric de securitate în biblioteci, 5 au considerat că sistemul de recunoaștere facial este cel mai potrivit pentru securitate colecțiilor și a persoanelor dintr-o bibliotecă, 4 sunt de părere că cel bazat pe analiza irisului și 2 au considerat sistemul dactiloscopic este cel mai potrivit.

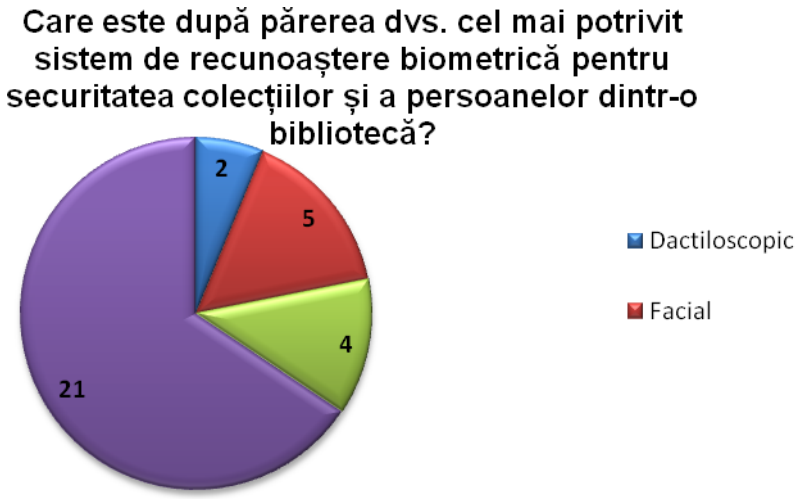


Fig. 36 *Cel mai potrivit sistem de securitate a colecțiilor și a persoanelor dintr-o bibliotecă, conform respondenților din Lotul 2*

În urma analizei datelor, putem observa că 38,6% dintre bibliotecarii din România și Moldova, au destul de multă încredere în sistemele de recunoaștere facială, 9% au foarte multă încredere, 18,6% nu au nici multă,nici puțină, pe când 7,6% nu au prea multă încredere și 0,7% nu au încredere deloc.

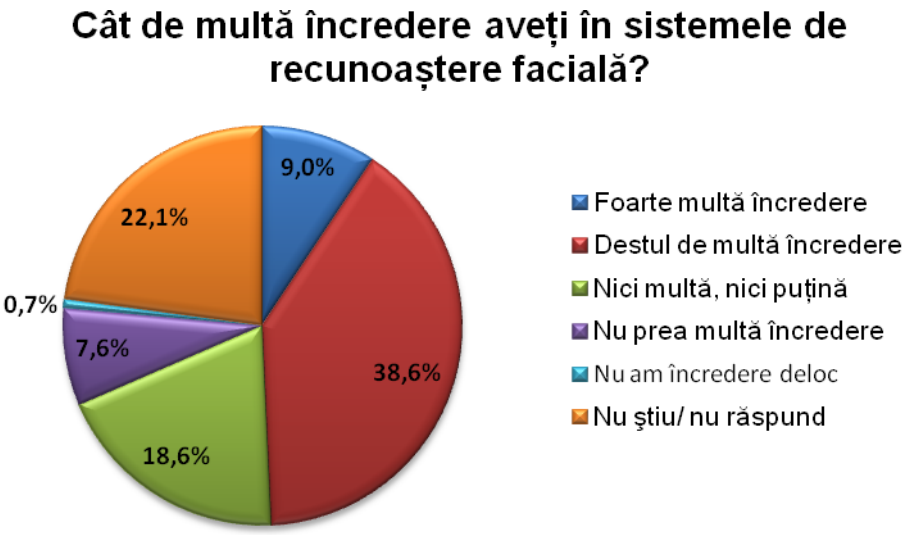


Fig. 37 *Nivelul de încredere al respondenților din România și Moldova, cu privire la sistemele de recunoaștere facială*

Din totalul de 32 de respondenți, din Lotul 2, 9 au destul de multă încredere în sistemele de recunoaștere facială, 13 nici multă, nici puțină, un respondent nu prea multă încredere, unul nu are încredere deloc și tot un respondent are foarte multă încredere.

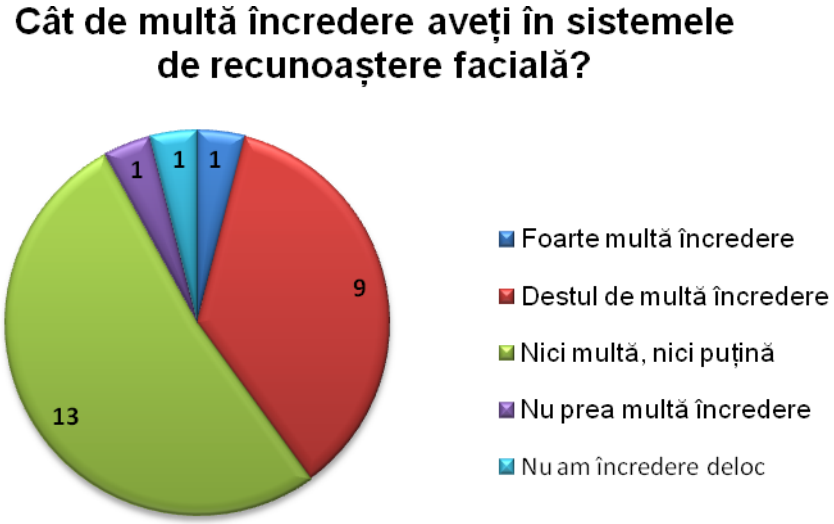


Fig. 38 *Nivelul de încredere al respondenților din Lotul 2, cu privire la sistemele de recunoaștere facială*

Dintr-un total de 145 de bibliotecari, din România și Moldova, 61,4% ar fi de acord cu implementarea unui sistem de recunoaștere facială în biblioteca în care activează, 12,4% nu ar fi de acord, iar un procent de 23,4% nu și-au exprimat părerea cu privire la acest demers.

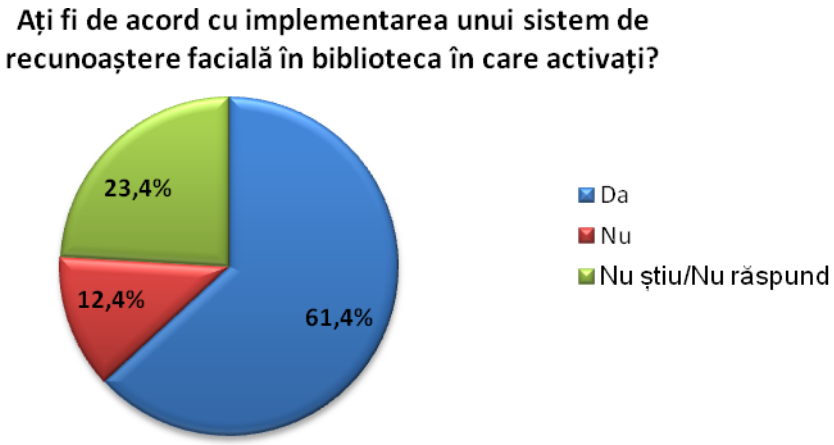


Fig. 39 *Acordul bibliotecarilor din România și Moldova cu privire la implementarea unui sistem de recunoaștere facială*

În ceea ce privește respondenții din străinătate, dintr-un total de 32, 13 au fost de acord cu implementarea unui sistem de recunoaștere facială, 11 nu au fost de acord și 8 nu si-au exprimat părerea.

Fig. 40 *Acordul bibliotecarilor din străinătate de a implementa un sistem de recunoaștere facială*

3.2.2 Testarea ipotezelor

Ipoteza 1. *Bibliotecarii preocupați de securitatea persoanelor, în contextul terorismului, sunt dornici să implementeze un sistem de recunoaștere facială în biblioteca în care activează.*

În cele ce urmează se vor emite **două** ipoteze, ipoteza de nul (H_0) care ia în considerare situația cea mai nefavorabilă, iar a doua se referă la ipoteza alternativă (H_1), opusul celei de nul.

H_0 - inexistența unei corelații între dorința bibliotecarilor de a lua măsuri cu privire la securitatea persoanelor și acordul bibliotecarilor de a implementa un sistem de recunoaștere facială;

H_1 - există corelație între dorința bibliotecarilor de a lua măsuri cu privire la securitatea persoanelor și acordul bibliotecarilor de a implementa un sistem de recunoaștere facială;

P 95% reprezintă probabilitatea de garantare a rezultatelor, marja de eroare care reflectă probabilitatea de a greși este 5%, iar în această situație rezultă că probabilitatea de testare a ipotezei de nul (p) are valoarea de 0,05.

Regula generală de testare pentru o probabilitate de garantare a rezultatelor de 95%: $x_{calculat} < x_{critic} \Rightarrow$ se respinge ipoteza de nul H_0; unde: $x_{calculat} = p_{calculat}$(Sig.) și $x_{critic} = p$, iar p = 0,05

Conform indicelui Pearson, variabila ce măsoară dorința bibliotecarilor de a lua măsuri cu privire la securitatea persoanelor, în contextul terorismului, este corelată la nivel 0,203, cu variabila ce exprimă acordul bibliotecarilor de a implementa un sistem de recunoaștere facială.

Sig= 0,008 este mai mic decât p= 0,05 astfel că se respinge ipoteza de nul H_0 , care preciza că nu există corelație între dorința bibliotecarilor de a lua măsuri cu privire la securitatea persoanelor și acordul bibliotecarilor de a implementa un sistem de recunoaștere facială. Sig=0,008, p<0,01 ceea ce semnalează o relație strânsă între cele două variabile. Astfel, cu cât bibliotecarii sunt mai preocupați de securitatea persoanelor, în contextul terorismului, cu atât sunt mai dornici să implementeze un sistem de recunoaștere facială, și invers.

Ipoteza 1, potrivit căreia bibliotecarii preocupați de securitatea persoanelor, în contextul terorismului, sunt dornici să implementeze un sistem de recunoaștere facială în biblioteca în care activează se confirmă.

Conform aceloraşi explicații de la ipoteza 1, 3 dintre ipotezele studiului se confirmă și 4 se resping.

3.3 Concluzii

Cercetarea efectuată a permis formularea următoarei concluzii: majoritatea bibliotecarilor ar fi de acord cu implementarea unui sistem de recunoaștere facială, în biblioteca în care activează, pentru a sporii gradul de securitate. S-a putut observa că respondenții din străinătate au fost mai reținuți față de acest demers, în comparație cu cei din România și Moldova.

Bibliotecarii preocupați de securitatea persoanelor, în contextul terorismului, sunt dornici să implementeze un sistem de recunoaștere facială în biblioteca în care activează. De asemenea, bibliotecarii care cred că cel mai potrivit sistem de recunoaștere biometrică pentru securitatea colecțiilor și a persoanelor este recunoașterea facială, ar fi de acord cu implementarea unui astfel de sistem. Gradul de încredere în sistemele de recunoaștere facială, joacă un rol important în decizia bibliotecarilor de a mării gradul de securitate al bibliotecii, prin instalarea noului sistem.

Din datele analizate reiese faptul că mărimea bibliotecii, funcția bibliotecarilor, sau experiența de peste 31 de ani la locul de muncă nu intervin în decizia bibliotecarilor de a implementa noul sistem de recunoaștere facială. De asemenea, nivelul de pregătire al bibliotecarilor nu intervine în această decizie, probabil din cauză că majoritatea au mai mult decât studii medii.

CAPITOLUL 4

OPTIMIZAREA SISTEMULUI DE SECURITATE DIN BIBLIOTECI PRIN IMPLEMENTAREA UNUI SISTEM DE RECUNOAȘTERE FACIALĂ

4.1 Noțiuni introductive

Sunt prezentați termenii informatici necesari înțelegerii modului de operare al sistemului de recunoaştere facială VisageCloud, care constituie subiectul acestui capitol.

4.2 VisageCloud recunoașterea facială pentru autentificare, verificare rapidă și securitate (protecție) inteligentă

Aplicația informatică dezvoltată, monitorizează accesul în biblioteci, fiind creată ca răspuns la cererea tot mai mare de a avea un sistem eficient de control al accesului și prezenței într-o locație, în contextul terorismului. Scopul sistemului este de a asigura o monitorizare rapidă, sigură și fiabilă, a accesului utilizatorilor în diferite locații publice.

VisageCloud este o soluție „end to end" de recunoaștere și clasificare a feței. Poate lucra pe fotografii, pe autocolante, cărți de identitate și fluxuri video. VisageCloud permite înregistrarea utilizatorilor la intrarea în bibliotecă, a clienților într-un hotel ş.a. Aplicația oferă informații asupra persoanelor posibil suspecte (diverse infracțiuni, terorism etc.). În plus, VisageCloud permite să obținerea de informații suplimentare de la camerele de supraveghere deja existente, obținând notificări și rapoarte în timp real. VisageCloud poate funcționa ca un serviciu de tip cloud sau on-premise. Se bazează pe o interfață API (*Application Programming Interface*), astfel încât poate fi integrat cu ușurință în alte aplicații sau sisteme.

4.2.1 Modelul de domeniu al aplicației VisageCloud

În ingineria software, un model de domeniu este un model conceptual al domeniului care încorporează atât comportamentul, cât și datele.

În ingineria ontologică, un model de domeniu reprezintă o reprezentare formală a unui domeniu de cunoștințe cu concepte, roluri, tipuri de date, persoane și reguli, bazate de obicei pe o logică descriptivă și implementate în OWL (Web Ontology Language). Un model de domeniu este un sistem de abstractizări care descrie aspecte ale unei sfere de cunoaștere, influență sau activitate (domeniu). Modelul poate fi apoi utilizat pentru a rezolva problemele legate de respectivul domeniu. Modelul de domeniu reprezintă o reprezentare a unor concepte semnificative din lumea reală care aparțin domeniului (activității) care trebuie modelat în software. Conceptele includ datele implicate în domeniul ales și regulile utilizate în activitatea respectivă privind aceste date. Un model de domeniu

utilizează în general vocabularul domeniului astfel încât o reprezentare a modelului să permită comunicarea cu părțile interesate (non-tehnice). Un model de domeniu este, în general, implementat ca un model obiect într-un strat care dispune de un nivel inferior pentru persistență și "emite" un API la un nivel superior pentru a obține accesul la datele și comportamentul modelului. Modelul de domeniu, în limbajul de modelare Unified Modeling Language (UML), este reprezentat printr-o diagramă de clasă.

Modelul de domeniu al aplicației VisageCloud conține **patru** elemente-cheie:

1. **Cont** – oferă accesul la gestionarea mai multor colecții;
2. **Colecție** - cuprinde mai multe profiluri ale persoanelor distincte (diferite). De exemplu. utilizatori, angajați etc.;
3. **Profil** – identifică un individ distinct (de exemplu, Elena, Emilia, Radu, Alexandru etc.) care aparține unei colecții;**și**
4. **Față** - o ilustrare a feței unui individ, așa cum este capturată dintr-o fotografie. Existența mai multor fețe asociate unui profil (de preferință cu iluminare diferită, perspectivă, machiaj, expresie facială sau alte caracteristici contextuale) ajută la îmbunătățirea acurateței recunoașterii faciale.

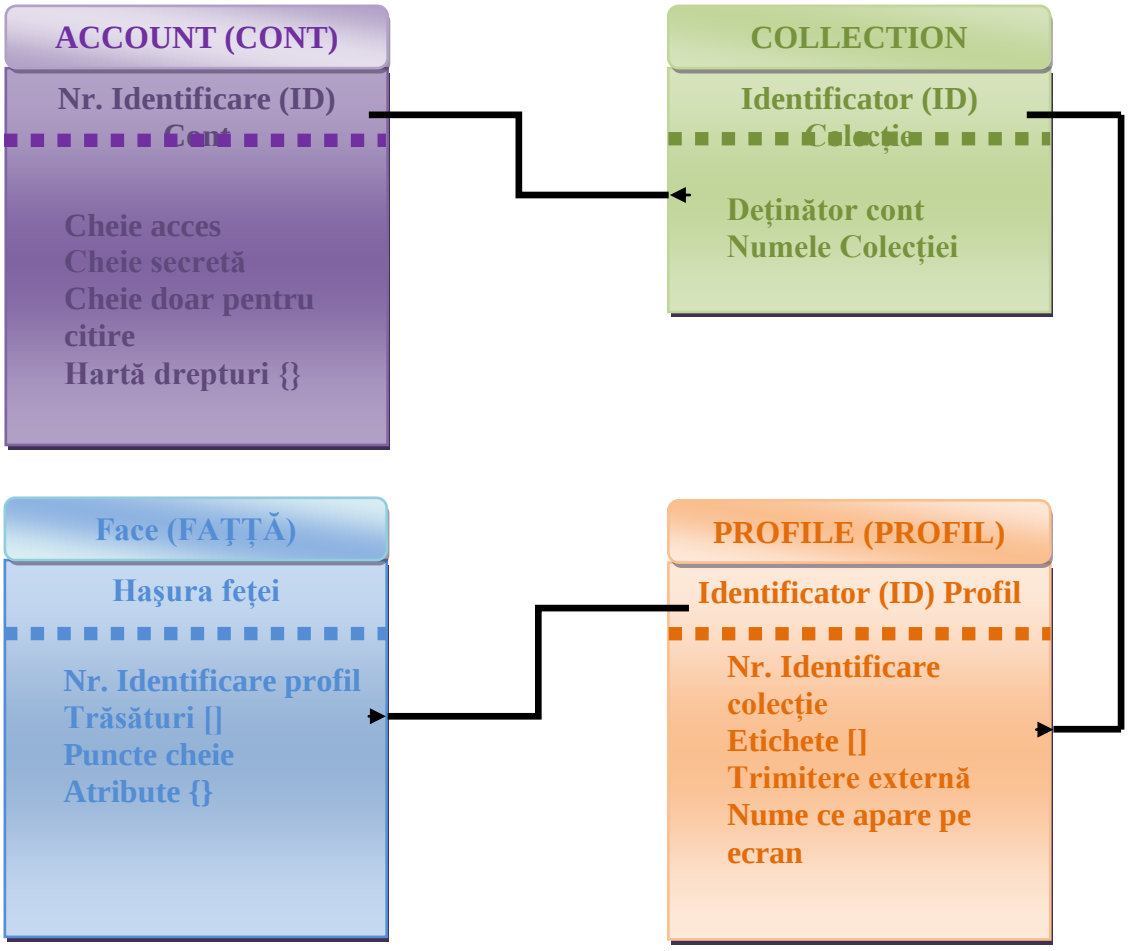


Fig.41 *Diagrama UML a aplicației VisageCloud*

4.2.2 Visage Cloud: Interfața de programare (API)

API-ul VisageCloud este un API REST în Cloud care poate fi utilizat în aplicații pentru a permite accesul la recunoașterea facială și la capacitățile de clasificare. Visage Cloud îmbină algoritmii de ultimă generație pentru recunoașterea și clasificarea facială prin tehnici de interogare, etichetare și interogare a datelor, astfel încât să faciliteze utilizarea cu maximă eficiență a datelor.

Interfața de programare a aplicațiilor Cloud (Cloud API) este un tip de API care permite dezvoltarea de aplicații și servicii utilizate pentru furnizarea de hardware, software și platforme cloud. Un cloud API servește ca o poartă sau o interfață care furnizează utilizatorilor o infrastructură cloud directă și indirectă precum și servicii software.

Interfața de programare a aplicației Visage Cloud apare în următorul ecran:

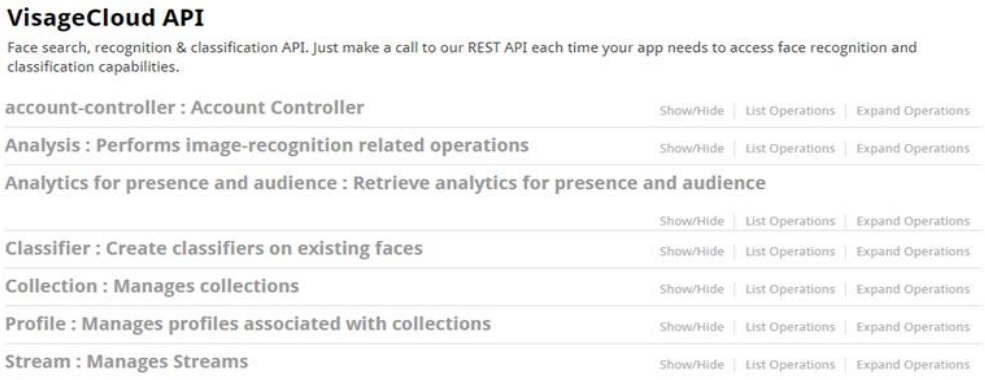


Fig.42. *Interfața de programare a aplicației Visage Cloud.*

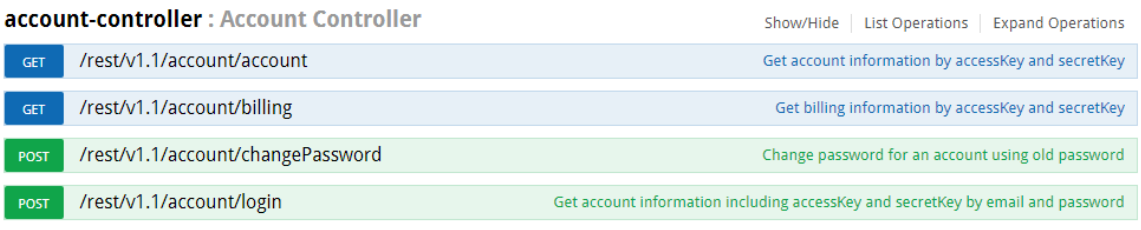
După cum se poate observa în partea stângă a ecranului sunt afișate submeniurile aplicației Visage Cloud, şi anume:

I. ***Account-controller:*** Account Controller;
II. ***Analysis:*** Performs image-recognition related operations;
III. ***Analytics for presence and audience:*** Retrieve analytics for presence and audience;
IV. ***Classifier:*** Create classifiers on existing faces;
V. ***Collection:*** Manages collections;
VI. ***Profile:*** Manages profiles associated with collections;
VII. ***Stream:*** Manages Streams,

iar în partea dreaptă apar, pe trei coloane, opțiunile ce se pot executa pentru fiecare submeniu menționat anterior. Cele trei opțiuni sunt: Show/Hide, List Operations şi Expand Operations.

I. Account Controller

La alegerea opțiunii *Acount controller* va apărea următorul ecran:



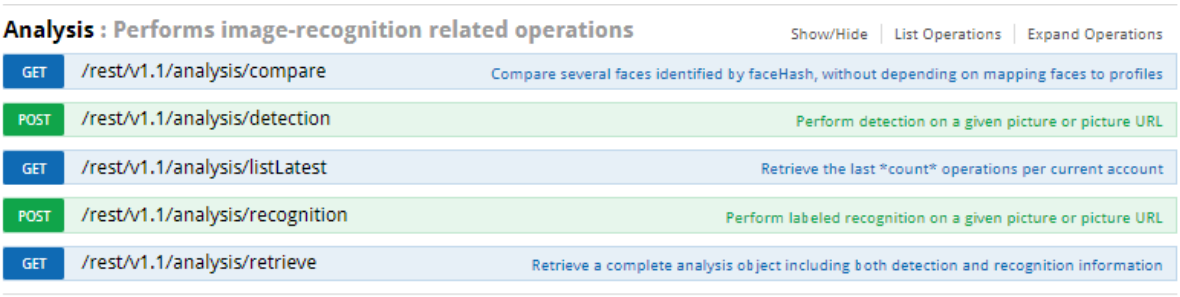
Se poate constata că opțiunea *Account* conține 4 submeniuri:

a) **Account**
b) **Billing**
c) **Change Password**
d) **Login.**

Cele patru submeniuri ale opțiunii *Account* sunt descrise în teză.

II. Analysis

Această opțiune efectuează operații legate de recunoașterea imaginii. Activând opțiunea, apare ecranul prezentat în continuare.



Operațiile executate pentru recunoaşterea facială sunt următoarele:

a) **Compare (Compararea)**. Compară mai multe fețe identificate de „faceHash", fără a depinde de maparea fețelor la profiluri. API-ul aplicației VisageCloud poate **compara** două sau mai multe fețe pentru a evalua dacă aparțin aceleiași persoane - chiar dacă această persoană este necunoscută.
b) **Detection (Detectarea)**. Efectuează *detectarea* pentru o anumită imagine dată sau situată într-o adresă URL (Uniform Resource Locator).
c) **ListLatest** - Prin activarea acestei operații pot fi regăsite ultimele operațiuni *count* pentru contul curent.
d) **Recognition (Recunoaşterea)**. Efectuează recunoașterea etichetată pe o imagine dată sau aflată la o adresă URL.

   Recunoașterea sau identificarea implică confirmarea identității unei persoane, odată ce fața ei a fost detectată în imagine, prin căutarea a sute de mii de fețe cunoscute în mai puțin de o secundă. Fiecărei potriviri (asemănări) i se dă un scor, astfel încât să se poată trece cu ușurință răspunsul și să fie luată o decizie în cunoștință de cauză.
e) **Retrieve (Regăsirea)**. Se obține o imagine complet analizată care conține atât informații de detectare cât și de recunoaștere.

III. Analytics for presence and audience

Această operație permite obținerea unor tehnici de analiză pentru prezență și pentru public, existând următoarele opțiuni:

a) **Counting**
b) **Presence/timeseries**
c) **Presence/total.**

IV. Classifier (Clasificarea)

Fețele detectate sunt **clasificate** în funcție de *vârstă, sex, etnie* sau *emoție*, astfel încât această caracteristică este deosebit de utilă în special pentru analizele de vânzare cu amănuntul și pentru proiectarea semnalelor digitale cu direcționare în timp real. Clasificarea nu urmărește să evidențieze identitățile individuale, ci mai degrabă să apeleze la analize integrate pentru a genera componența demografică a persoanelor dintr-o anumită zonă.

Dând click pe această operație se pot crea clasificări pentru fețele existente.

V. Collection (Colecția)

Operația *Collection* permite gestionarea colecțiilor.

Prin activarea opțiunii *Collection* se pot efectua următoarele operații:

a) **regăsirea tuturor colecțiilor**
b) **crearea unei noi colecții cu un anumit nume**
c) **Regăsirea conținutului unei colecții în vederea analizării datelor**
d) **Ștergerea colecției existente cu profilurile și fețele asociate**
e) **Regăsirea conținutului unei colecții existente**
f) **Actualizarea unei colecții existente cu un anumit identificator (nume specificat)**
g) **Obținerea tuturor profilurilor asociate unei colecții**

VI. Profile

Gestionarea profilurilor asociate colecțiilor se poate realiza prin selectarea opțiunii *Profile* din aplicația VisageCloud, care oferă posibilitatea realizării următoarelor operații:

a) **Obținerea statutului de înregistrare a unui profil: informații despre posibilitatea realizării autentificării**
b) **Eliminarea (dezactivarea) unei liste de fețe, identificată prin faceHashes, dintr-un profil, identificat prin ID-ul profilului respectiv**
c) **Obținerea tuturor fațetelor (faceHashes) asociate unui profil**
d) **Adaugarea unei liste de fețe, identificate prin faceHashes, unui profil identificat prin ID-ul profilului respective**
e) **Creează un profil nou fără fețe asociate acestuia (profil gol)**

f) Șterge un profil și dezactivează toate fețele care aparțin acelui profil
g) Regăsirea unui profil
h) Actualizarea unui profil existent cu un ID dat

VII. Stream (Flux)

Această operație permite gestionarea fluxurilor. Submeniurile aferente includ toate operațiile referitoare la flux: **Afișarea stării (statutului) tuturor fluxurilor din cont; Obținerea ultimelor N persoane recunoscute din flux; Eliminarea cadrelor mai vechi decât intervalul specificat; Obținerea unei imagini cadru individuală; Obținerea ultimelor N cadre prelucrate din flux; Începerea şi încheierea fluxului existent; Ştergerea fluxului existent; Crearea unui flux nou cu un anumit nume; Actualizarea unui flux existent cu un ID cunoscut; Obținerea unui flux existent cu un anumit nume de identificare (ID).**

4.3 VisageCloud: detectarea și recunoașterea feței

În cele ce urmează se va trece de la obținerea cheii API pentru a putea accesa aplicația, la crearea unei colecții de profiluri cunoscute (un profil reprezintă o persoană) pentru a detecta persoanele în fotografii și pentru a le cartografia în profil și apoi, prin utilizarea acelei colecții, pentru a recunoaște oamenii din fotografii noi.

Pasul 1: *Solicitarea unei chei API*

Pentru a putea beneficia de facilitățile oferite de VisageCloud referitoare la recunoaşterea facială utilizatorii pot accesa programul la adresa https://visagecloud.com/.

Va apărea interfața prezentată în figura 93:

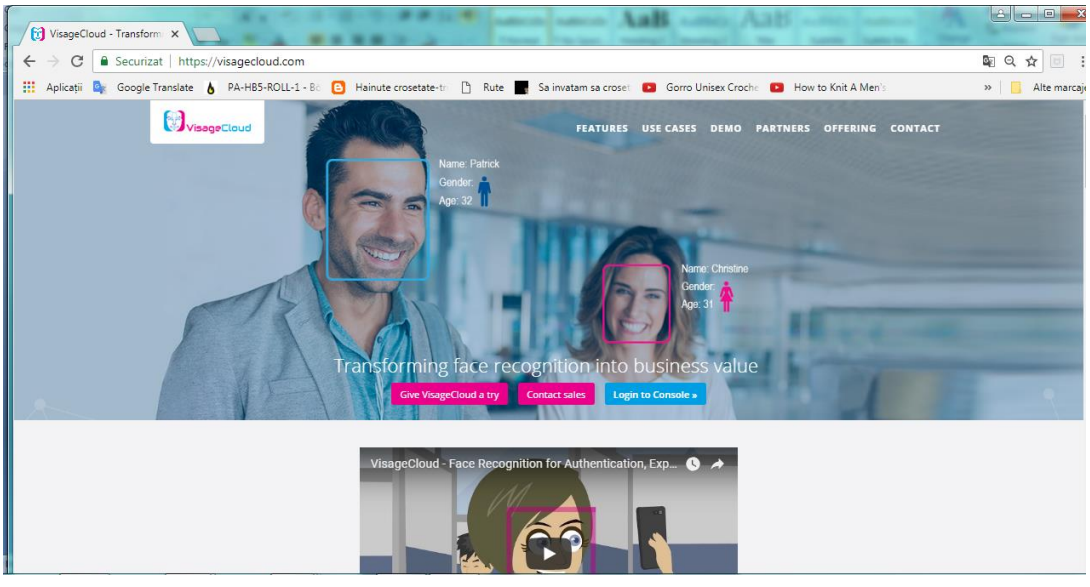


Fig. 93. *Interfața VisageCloud:* opțiunea **Login to Console**

unde se va alege opțiunea **Login to Console**. În urma acestei acțiuni vor fi solicitate datele pentru logare, şi anume: un nume de utilizator şi o parolă, după cum se poate observa în ecranul următor:

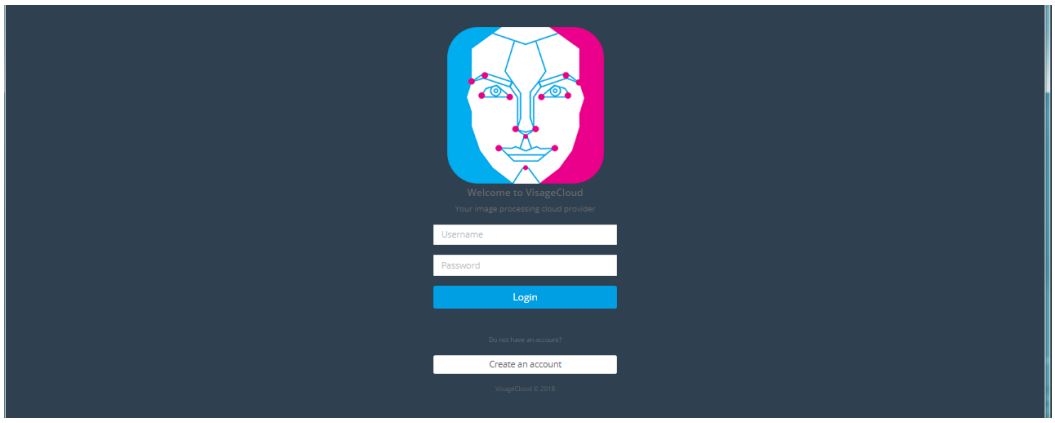


Fig. 94. *Interfața VisageCloud:* opțiunea **Login**.

Se observă, pe ecran, că utilizatorul are posibilitatea de a solicita crearea unui cont. Răspunsul sistemului la această solicitare este oferit în următoarea interfață:

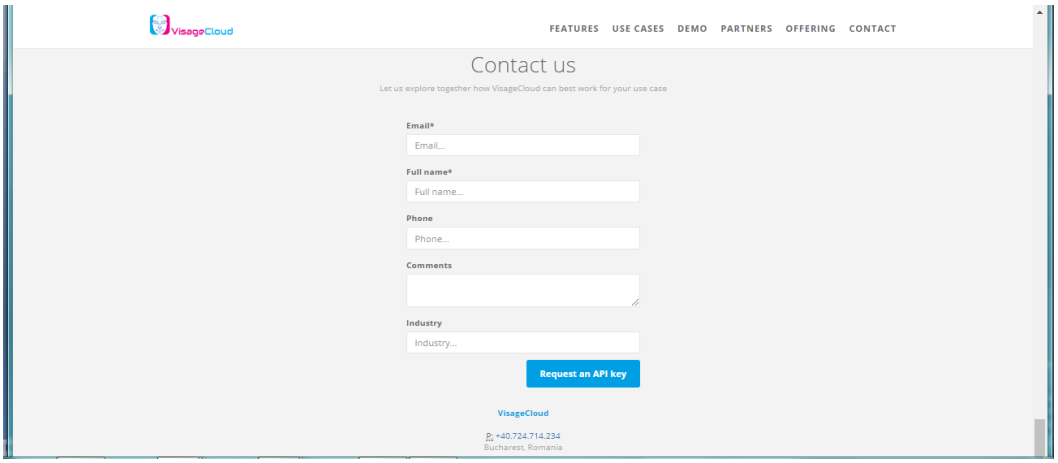


Fig. 95. *Interfața VisageCloud: Crearea unui cont.*

După completarea câmpurilor *Email* şi *Full name* care sunt obligatorii aplicația va trimite la adresa completată răspunsul la respectiva solicitare.

Vor fi furnizate **trei** chei:

1. *accessKey* care identifică în mod unic contul solicitat de utilizator
2. *secretKey* – aceasta este cheia principală a contului care permite titularului fie să efectueze detectări/recunoașteri, să creeze, să modifice, să șteargă colecții și profiluri și să acceseze informații sensibile (confidențiale) despre cont (cum ar fi lista ultimelor operații efectuate)
3. *readOnlyKey* – această cheie ar trebui să fie, de asemenea, secretă, dar permite doar efectuarea operației de detectare/recunoaștere, fără a avea opțiunile de modificare a datelor referitoare la cont sau de a vizualiza informații sensibile (confidențiale).

Toate solicitările către API trebuie autentificate prin setarea parametrului GET "*accessKey*" la valoarea accessKey și parametrul "*secretKey*" la valoarea secretKey pentru solicitările de scriere sau la valoarea readOnlyKey pentru solicitările de detectare/ recunoaștere.

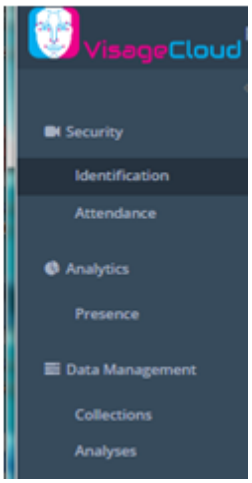
Punctele finale de analiză și recunoaștere pot fi accesate prin setarea parametrului GET "*accessKey*"

la valoarea accessKey și parametrul "*secretKey*" la valoarea readOnlyKey.

După obținerea acestor date, utilizatorul se poate loga la aplicația de recunoaştere facială VisageCloud. Ca urmare a acestei acțiuni va apărea interfața:

Fig. 96. *Interfața VisageCloud:* Logarea utilizatorului la sistem.

În colțul din dreapta sus apare numele utilizatorului care s-a logat la sistem. În partea stângă a ecranului sunt afişate operațiile permise respectivului utilizator.



În ordinea în care apar pe ecran acestea sunt:

- **Security** cu opțiunile:
  - *Identification* şi
  - *Attendance*
- **Analytics** cu submeniul:
  - *Presence*
- **Data Management care asigură gestionarea datelor prin:**
  - *Collections şi*
  - *Analyses.*

Fig. 97. *Operațiile disponibile utilizatorului Visage Cloud.*

Pasul 2: *Crearea unei colecții*

Pentru o gestionare mai ușoară a utilizatorilor înregistrați în sistem este necesară crearea unei colecții (un set sau un grup de persoane înregistrate). Pentru aceasta se va selecta opțiunea *Collections* și va apărea:

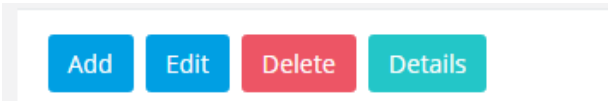


Fig. 99. *Opțiuni pentru gestionarea colecțiilor.*

După cum se poate constata în urma analizării acestei interfețe există posibilitatea efectuării următoarelor opțiuni pentru gestionarea colecțiilor:

a) **Add:** care permite adăugarea unor noi colecții.

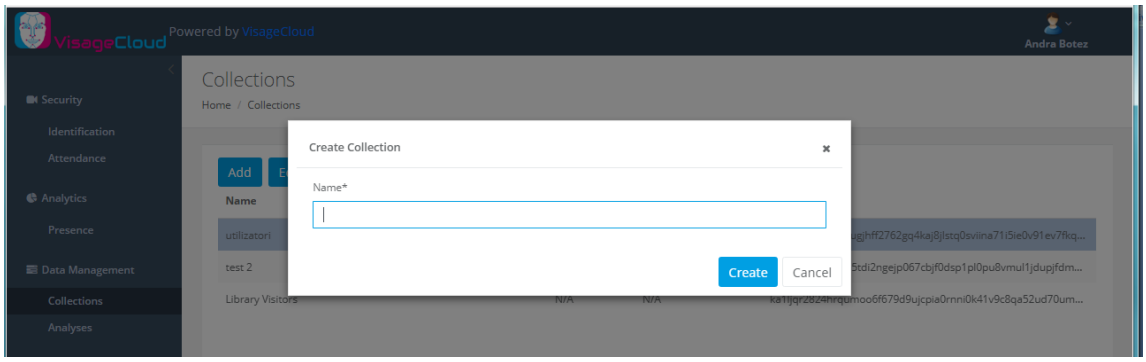


Fig. 100. *Opțiunea **Add:** care permite adăugarea unor noi colecții.*

Este necesar a se completa câmpul *Nume*. De exemplu „*test*”. Apoi se dă click pe opțiunea ***Create*.**

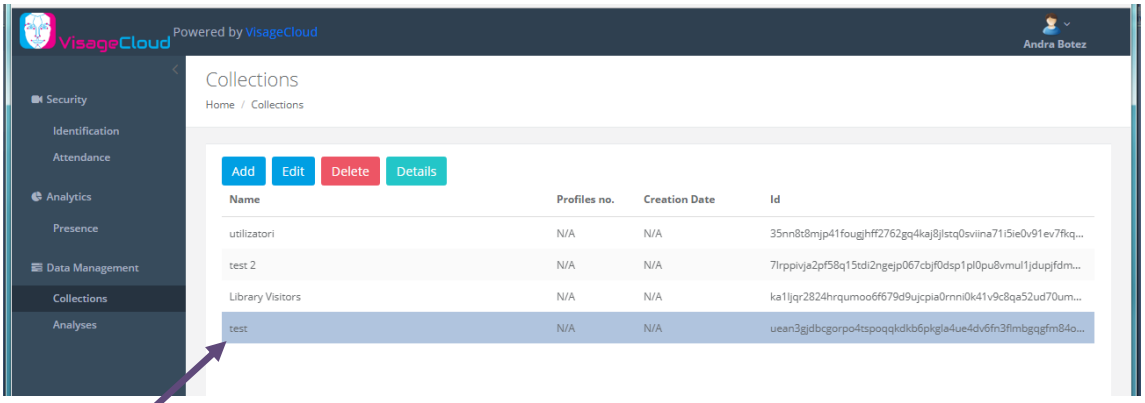


Fig. 101. *Crearea unei colecții noi.*

Colecția *test* a fost creată după cum se poate observa.

b) **Edit** care permite actualizarea denumirii colecției.

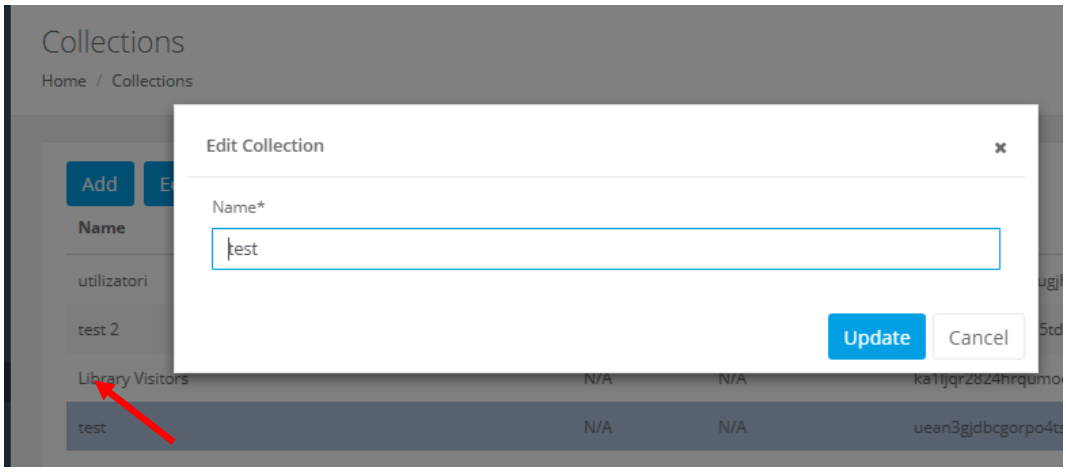


Fig. 102. *Opțiunea **Edit**: care permite actualizarea denumirii colecției.*

Se selectează o colecție, se dă click pe ea şi va apărea ecranul din imaginea anterioară. Se poate selecta *Update,* în cazul în care se doreşte o actualizare a numelui acelei colecții sau *Cancel*, dacă nu se urmăreşte modificarea.

c) **Delete** – atunci când este necesară ştergerea unei colecții. Pentru siguranță sistemul solicită confirmarea opțiunii.

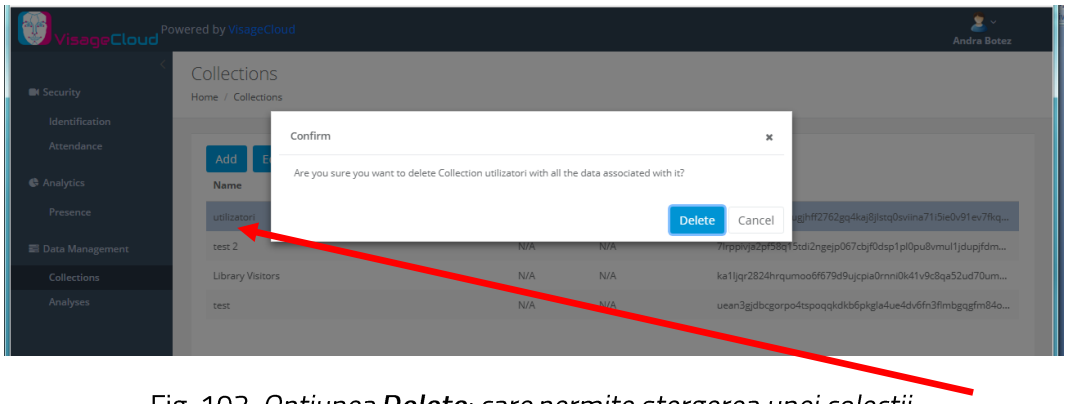


Fig. 103. *Opțiunea **Delete**: care permite ștergerea unei colecții.*

Se poate alege opțiunea *Delete* ceea ce va avea ca efect ştergerea colecției denumite *utilizatori* cu toate datele aferente ei sau Cancel, situație în care se va renunța la ştergere.

d) **Details** – opțiune care permite asocierea de *profile* pentru colecția creată după cum se observă în acest ecran.

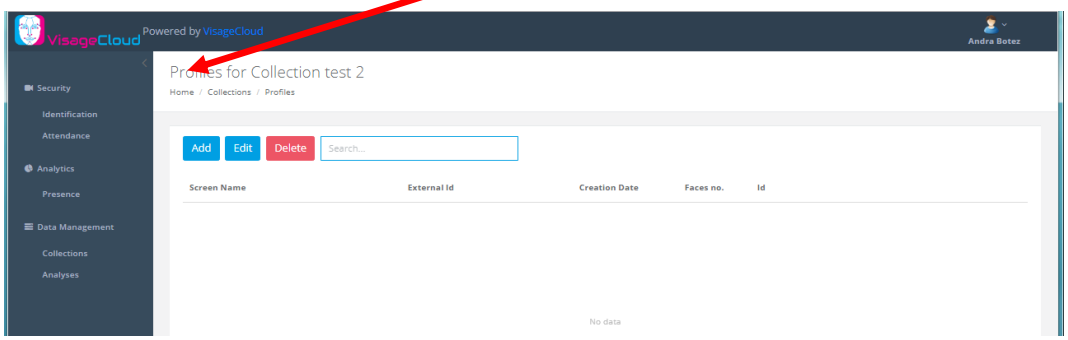


Fig. 104. *Opțiunea **Details**: care permite asocierea de profile pentru colecția creată.*

Astfel se ajunge la pasul 3.

Pasul 3: *Crearea unor profiluri pentru fiecare persoană din colecție*

Un profil reprezintă o persoană. Parametrii necesari pentru crearea unui profil sunt:

- ***accessKey, secretKey***
- ***collectionId*** - definește colecția în care doriți să creați profilul
- ***externalId*** - acest lucru permite conectarea unui profil la o bază de date externă a VisageCloud
- ***screenName*** - este o etichetă pentru fiecare profil, care poate fi citită de om;
- ***labels*** - etichetele care ne vor permite ulterior să efectuam o filtrare mai fină în recunoașterea feței.

Pentru crearea unui profil nou se porneşte de la interfața din figura 105.

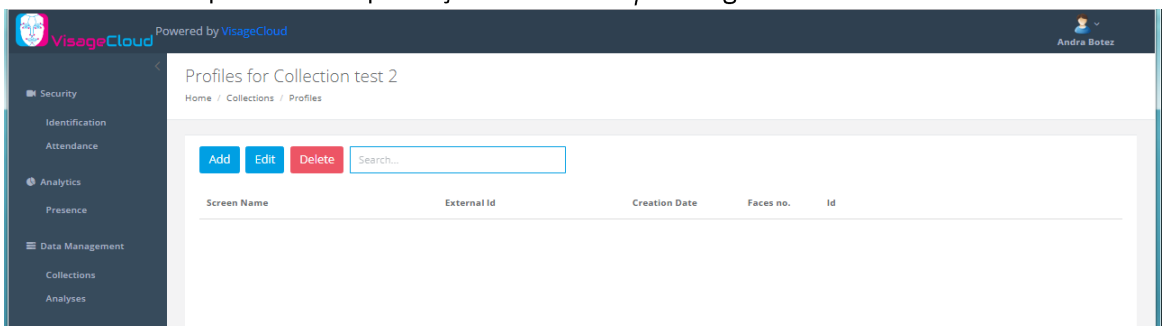


Fig. 105. *Interfața profile.*

în care, se alege opțiunea **Add** şi va apărea următorul ecran:

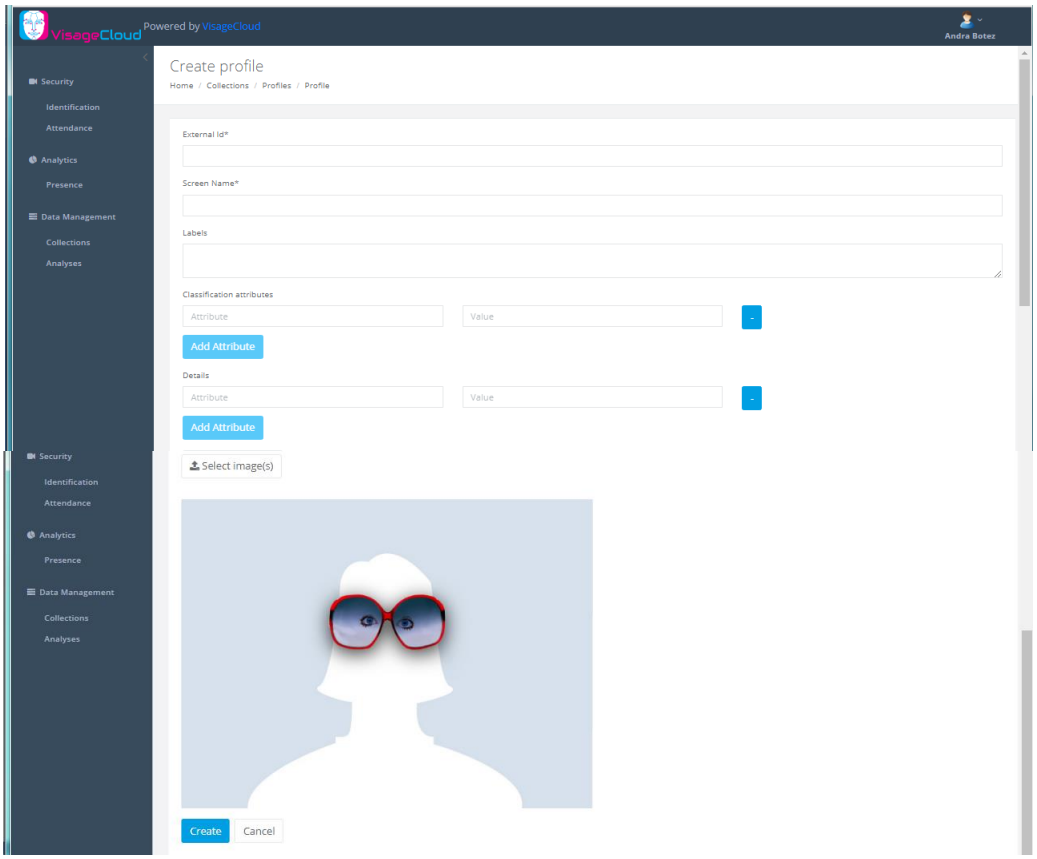


Fig. 106. *Opțiunea* ***Add:*** *crearea unui profil de utilizator.*

După completarea câmpurilor

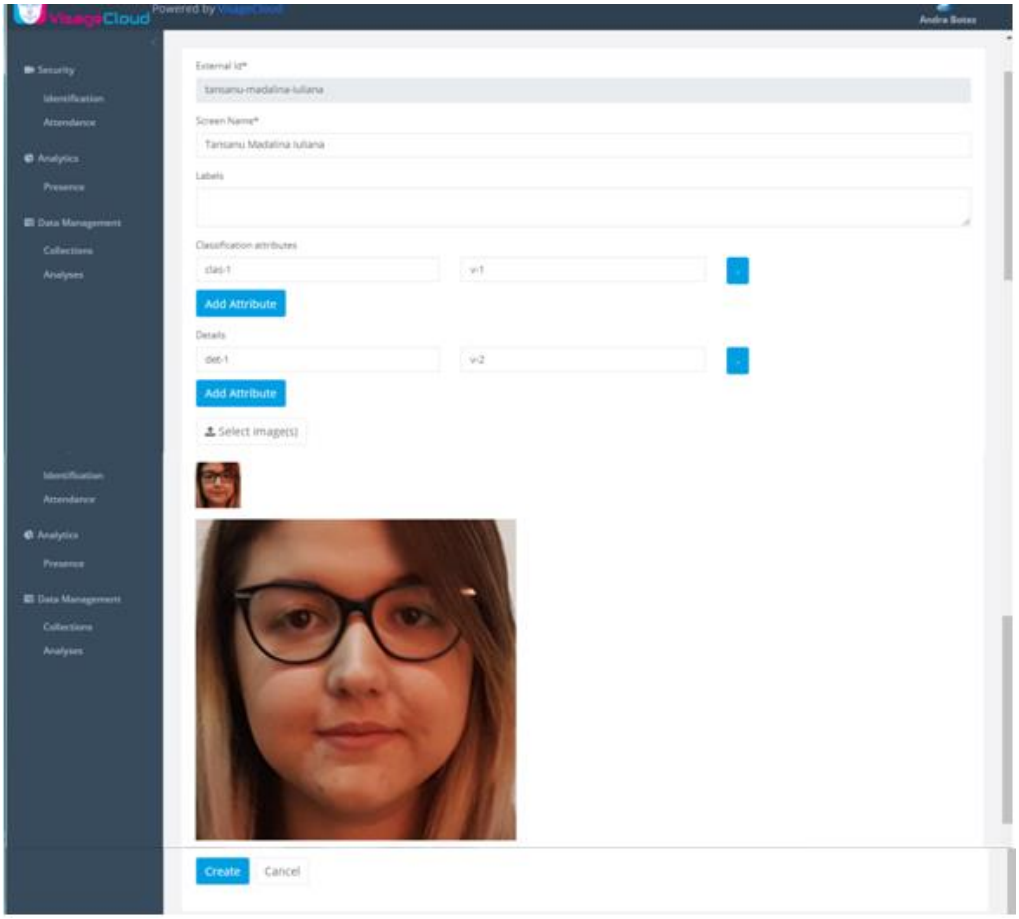


Fig. 107. *Exemplu de creere a unui profil de utilizator.*

se va alege opțiunea *Create* şi astfel va fi creat profilul pentru Tansanu Madalina Iuliana. Dacă se dorește actualizarea unui profil existent se va selecta opțiunea *Edit* iar în cazul în care este necesar a fi şters vreun profil asociat colecției opțiunea va fi *Delete.* Şi în acest caz, la fel ca şi pentru colecție sistemul solicită confirmare pentru a evita situația ştergerii din neatenție a informațiilor.

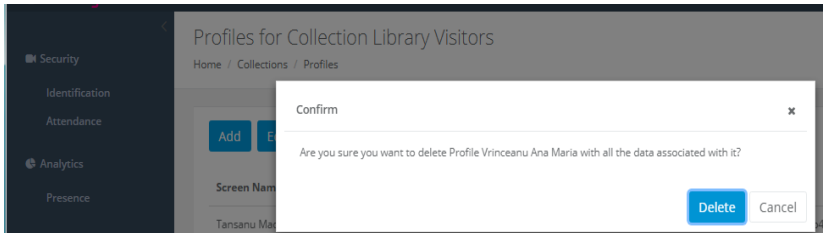


Fig. 108. *Opțiunea Confirm: pentru a se evita ștergerea unui profil din greșeală.*

VisageCloud oferă facilitatea căutării unui profil sau colecții în baza de date. Prin completarea în câmpul search a numelui căutat va apărea ecranul:

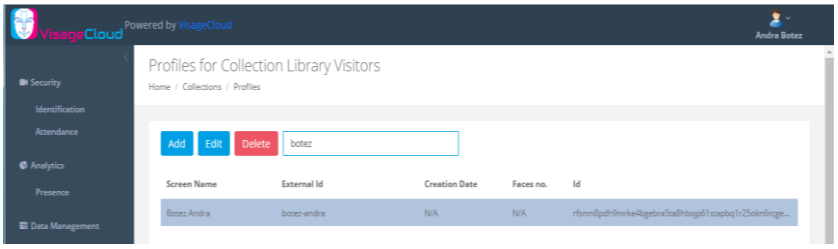
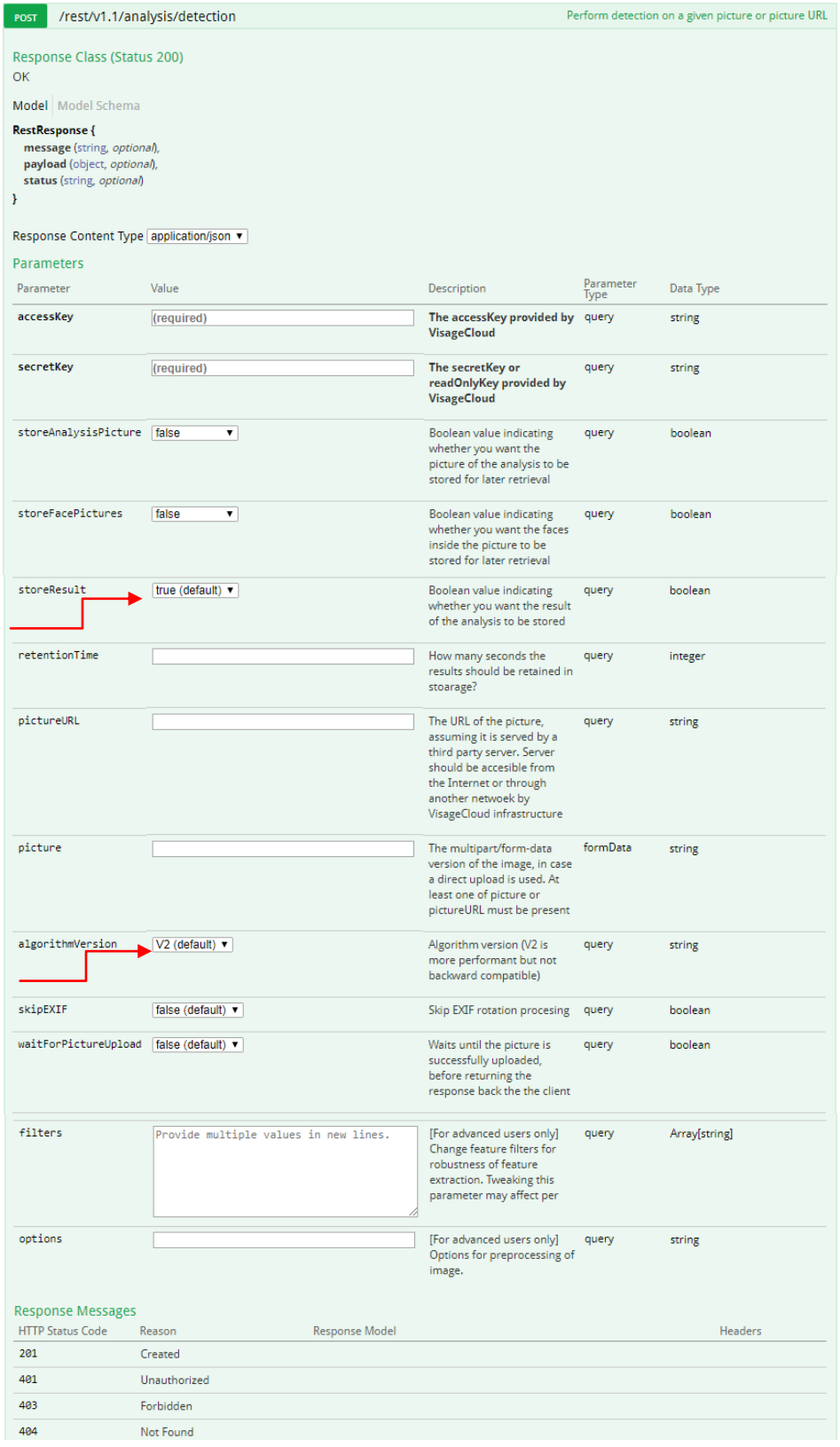


Fig. 109. *Opțiunea căutării unui profil sau colecții în baza de date.*

Pasul 4: *Detectarea fețelor din fotografii*

Constă în încărcarea unei imagini care poate conține una sau mai multe fețe.



POST /rest/V1.1/analysis/detection — Perform detection on a given picture or picture URL

Response Class (Status 200)
OK

Model | Model Schema

RestResponse {
message (string, *optional*),
payload (object, *optional*),
status (string, *optional*)
}

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
accessKey	(required)	**The accessKey provided by VisageCloud**	query	string
secretKey	(required)	**The secretKey or readOnlyKey provided by VisageCloud**	query	string
storeAnalysisPicture	false	Boolean value indicating whether you want the picture of the analysis to be stored for later retrieval	query	boolean
storeFacePictures	false	Boolean value indicating whether you want the faces inside the picture to be stored for later retrieval	query	boolean
storeResult	true (default)	Boolean value indicating whether you want the result of the analysis to be stored	query	boolean
retentionTime		How many seconds the results should be retained in stoarage?	query	integer
pictureURL		The URL of the picture, assuming it is served by a third party server. Server should be accesible from the Internet or through another netwoek by VisageCloud infrastructure	query	string
picture		The multipart/form-data version of the image, in case a direct upload is used. At least one of picture or pictureURL must be present	formData	string
algorithmVersion	V2 (default)	Algorithm version (V2 is more performant but not backward compatible)	query	string
skipEXIF	false (default)	Skip EXIF rotation procesing	query	boolean
waitForPictureUpload	false (default)	Waits until the picture is successfully uploaded, before returning the response back the the client	query	boolean
filters	Provide multiple values in new lines.	[For advanced users only] Change feature filters for robustness of feature extraction. Tweaking this parameter may affect per	query	Array[string]
options		[For advanced users only] Options for preprocessing of image.	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		
401	Unauthorized		
403	Forbidden		
404	Not Found		

Fig. 110. *Interfața de programare pentru opțiunea Detection.*

În funcție de valoarea parametrilor stabiliți în interfața de programare a aplicației VisageCloud pentru operația de detecare pot apărea diverse situații:

1. dacă parametrul "storeFacePictures" are valoarea "false" atunci VisageCloud va elimina imaginea originală după efectuarea analizei; în acest caz, "storeAnalysisPicture" nu va conține niciun răspuns.
2. dacă se efectuează detectarea de pe o imagineURL, VisageCloud va prelua imaginea de la adresa URL care a fost indicată prin completarea parametrului *pictureURL* și va returna răspunsul când detecția este terminată.

Imaginea care a fost încărcată poate conține mai multe fețe și fiecare dintre ele va fi conținută în matricea "fețe". Dacă în imagine nu sunt detectate chipuri, această matrice va fi vidă. Fiecare față distinctă va avea un atribut "hash" unic, care, în consecință, poate fi adăugat la fețele distincte ale unui profil (persoană). Această asociere între faceHash și profil permite sistemului să stabilească dacă "această față aparține lui X" sau "Y".

Pasul 5: *Anexarea fiecărei fețe detectate unui profil*

Se realizează asocierea unei fețe particulare dintr-o fotografie cu un profil existent.

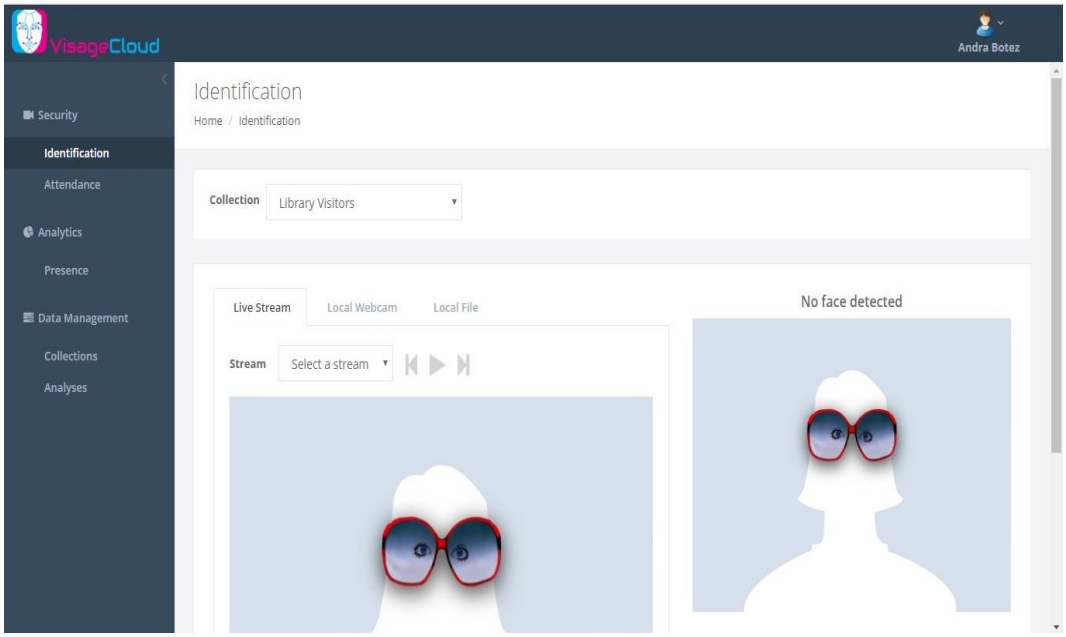


Fig. 111. *Identificarea utilizatorilor.*

Pasul 6: *Efectuarea recunoașterii faciale*

După ce au fost create mai multe profiluri și au fost cartografiate una sau mai multe fațete pentru fiecare dintre ele, ultimul pas este testarea operației de recunoaștere.
Acest lucru înseamnă că se poate încărca o nouă imagine iar aplicația va stabili persoana cu cele mai multe similitudini față de cea din imagine. Această caracteristică răspunde la întrebarea "*Cu cine seamănă persoana X*?"

După cum se poate observa imaginile pot proveni din fluxuri, Cameră Web locală sau dintr-o imagine existentă pe calculatorul personal.

Se va selecta opțiunea Local File şi va apărea ecranul următor:

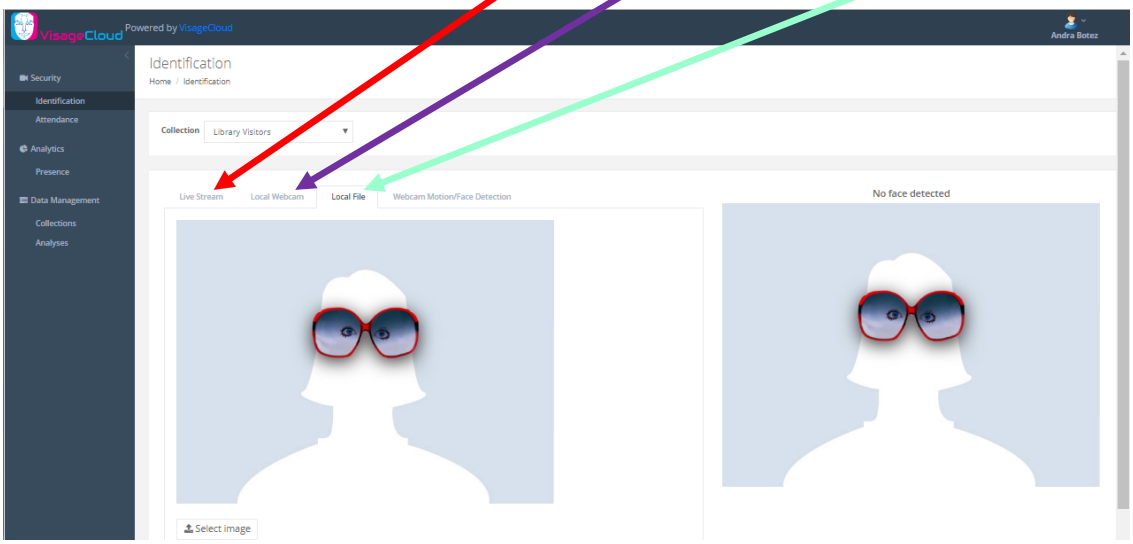


Fig. 112. *Moduri de obținere a imaginilor pentru efectuarea recunoașterii faciale.*

unde dând click pe *Select image* va încărca imaginea din computer şi o va asocia cu profilele existente. Pentru a face acest lucru, trebuie să fie specificat numele colecției pe care VisageCloud să o consulte. În acest caz *Library Visitor.*

Va apărea:

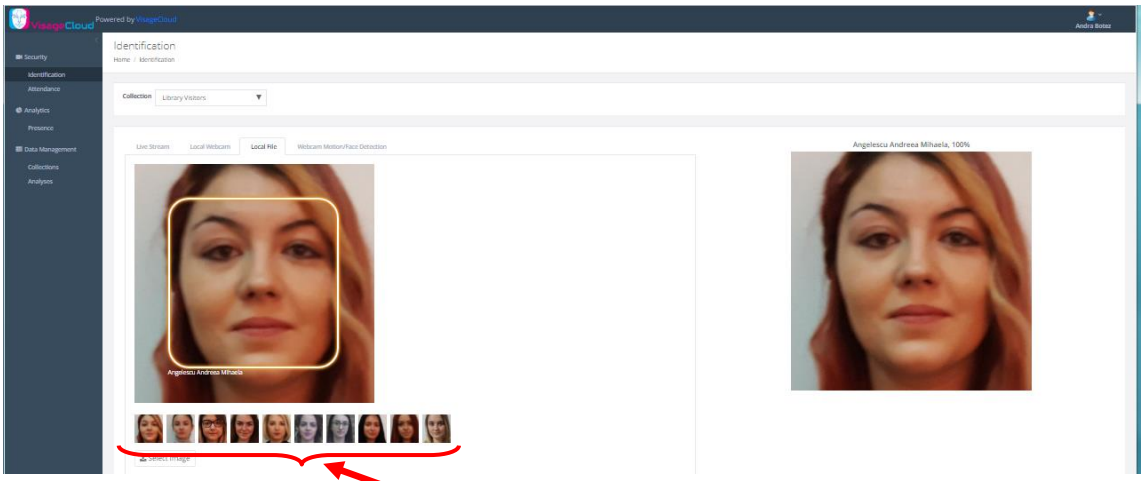


Fig. 113. *Exemplu de identificare pe baza unei imagini existente în PC.*

În submeniul "comparație" se poate observa că pentru fiecare FaceHash detectat apar o serie de potriviri, ordonate de la cea mai înaltă potrivire (cea mai mică distanță) la cea mai mică potrivire (cea mai mare distanță). În mod implicit, API returnează primele 10 similitudini, astfel încât să nu existe o supraîncărcare cu date inutile.

4.4. Studiu experimental de recunoaștere facială

Folosind sistemul descris anterior a fost efectuat un studiu experimental de recunoaștere facială.

Studiul a fost realizat în colaborare cu Biblioteca Județeană din Brașov, în februarie 2018, având un număr de 40 de participanți, studenți la Facultatea de Comunicare și relații publice, din cadrul Universității Transilvania.

Primul pas din cadrul experimentului a fost crearea colecției. Accesând butonul **Add,** din cadrul aplicației Visage Cloud, a apărut fereastra **Create Collection.** Am completat numele colecției de utilizatori "Library Visitors" și aceasta a fost creată dând click pe opțiunea **Create**.

În continuare am înregistrat pozele tuturor participanților la experiment, pentru realizarea bazei de date cu utilizatori, prin crearea de profiluri pentru fiecare persoană din colecție. Aceste profiluri conțin una sau mai multe poze, numele, precum și alte atribute cum ar fi: sexul sau grupa de vârstă.

Ultimul pas a fost testarea operației de recunoaștere. Fiecare participant la experiment a trecut prin fața camerei web și prin accesarea comenzii **Analyze** s-a putut observa identitatea celor înregistrați în baza de date.

Exemple de recunoaștere facială efectuată:

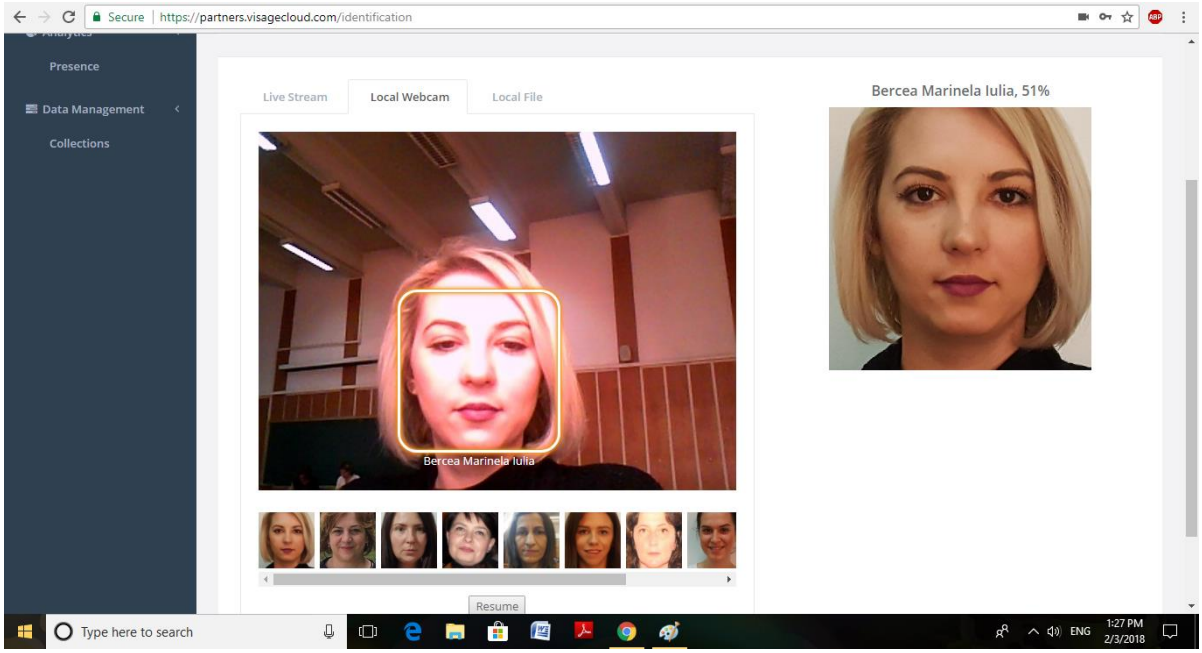


Fig. 115. *Exemplu 1 de recunoaștere facială din cadrul experimentului.*

S-a încercat o comunicare între sistemul de management al bibliotecii, modulul utilizatori și baza de date creată. Comunicarea a demonstrat compatibilitatea programului Visage Cloud cu soft-urile de management al utilizatorilor. Softul Visage Cloud poate fi folosit ca un sistem de sine stătător, precum și ca un sistem complementar în evidența utilizatorilor. Participanții la studiu au trecut prin fața sistemului și în cazul în care nu erau înregistrați sistemul a trimis o alertă.

4.5 Concluzii

VisageCloud este un program de recunoaștere facială, ce utilizează tehnologie de ultimă oră, fiind bazat pe cercetări realizate în 2015-2016. În testele pe seturi de date publice de mari dimensiuni, cum ar fi LFW (Labeled Faces in the Wild), VisageCloud a reușit să obțină o rată de recunoaștere corectă de 94-96%.

Detectarea, clasificarea și recunoșterea facială își găsesc aplicabilitatea în multe domenii: publicitatea digitală; automate de vânzare, puncte de vânzare și magazine interactive; etichetare foto; autentificare pentru aplicațiile mobile și web; sisteme inteligente de supraveghere.

- **Detectarea feței** se referă la procesul de identificare a zonelor generale ale unei imagini care conține o față. Pot exista mai multe astfel de zone și fiecare dintre acestea trebuie individual detectată și marcată cu un cadru. De asemenea, detecarea punctelor cheie ale feței face parte tot din detectarea feței și fixează punctele cheie ale feței, cum ar fi cele care descriu conturul maxilarului, gurii, nasului, ochilor și sprâncenelor.
- **Clasificarea feței,** după cum sugerează și numele, este o metodă de marcare a unei fețe cu mai multe atribute: genul, grupa de vârstă, expresia feței, culoarea ochilor, culoarea pielii, culoarea părului. Toate atributele menționate sunt acceptate de VisageCloud, fiind posibilă adăugarea de atribute suplimentare.
- **Recunoașterea feței** oferă răspuns la două tipuri de întrebări:
    1. "Cu cine seamănă cel mai mult persoana din această imagine?" (fața căutată sau 1:N față căutată) și
    2. "Este persoana din această imagine cu adevărat X / Y?" (identificarea feței sau 1:1 căutarea feței). În actuala versiune (V2) VisageCloud permite atât căutarea feței, cât și identificarea feței.

Pe măsură ce un număr tot mai mare de instituții (organizații) implementează sistemul de recunoaștere facială în operațiunile lor, este, în egală măsură, necesar să fie luate în considerare aspectele legate de asigurarea confidențialității persoanelor vizate (clienți, utilizatori etc.) de către aplicație. Numai o utilizare responsabilă, precum și o preocupare proactivă cu siguranța datelor cu caracter personal oferă în mod clar cele mai bune rezultate.

Persoanele care prelucrează datele referitoare la recunoașterea facială trebuie să asigure nu numai gestionarea eficientă a datelor, ci și utilizarea lor numai în scopul declarat.

Deoarece recunoașterea facială are nevoie de un set de referință pentru a funcționa, cele mai multe preocupări privind confidențialitatea încep cu natura acestui set de referință. Este esențial ca setul să fie creat și stocat într-o manieră etică, precum și răspunsurile să fie adecvate atât pentru situațiile autentice, cât și pentru cele false.

Aplicația poate fi deosebit de utilă pentru o supraveghere inteligentă, se poate aplica în biblioteci, precum și în industria hotelieră (turism), mai ales când unul dintre obiective este identificarea și recompensarea utilizatorilor (clienților) loiali.

CAPITOLUL 5

CONCLUZII

Biometria se referă la valori referitoare la caracteristicile umane. Autentificarea biometrică (sau autentificarea realistă) este folosită în domeniul informaticii ca o formă de identificare și control al accesului. De asemenea, este utilizat pentru a identifica persoanele din grupuri care sunt supravegheate.

Elementele biometrice de identificare sunt caracteristicile distinctive, măsurabile utilizate pentru etichetarea și descrierea persoanelor. Identificatorii biometrici sunt deseori clasificați ca fiind caracteristici fiziologice și comportamentale. Caracteristicile fizice sunt legate de forma corpului. Exemplele includ, dar nu se limitează la amprente, recunoașterea feței, ADN, geometria mâinilor, recunoașterea irisului etc. Caracteristicile comportamentale sunt legate de modelul de comportament al unei persoane, incluzând ritmul tastării, mersul și vocea.
Mijloacele tradiționale pentru controlul accesului includ sisteme de identificare bazate pe token, cum ar fi permisul de conducere sau pașaportul și sistemele de identificare bazate pe cunoștințe, cum ar fi o parolă sau un număr personal de identificare. Deoarece identificatorii biometrici sunt unici pentru indivizi, aceștia sunt mai de încredere în verificarea identității decât metodele bazate pe token și cunoștințe; cu toate acestea, colectarea de identificatori biometric ridică probleme de confidențialitate cu privire la utilizarea ulterioară a acestor informații.

În prezent, aplicațiile de recunoaștere sau autentificare apelează la o multitudine de parametri și date de tip biometric printre care: vocea, amprentele, fața, irisul, forma geometrică a mâinii, stilul de scriere, alura mersului, precum şi combinații ale acestora. În aplicațiile practice se întâlnesc cu precădere primele patru categorii deoarece permit utilizarea de senzori având performanțe adecvate și costuri reduse, cât şi datorită existenței unei fundamentării teoretice necesare prelucrării datelor disponibile.

Niciunul dintre sistemele biometrice enumerate nu poate oferi informații ideale. Din acest motiv, aplicarea unor tehnici și procedee de recunoaștere sau verificare care derivă din respectivele informații este condiționată de acceptarea unui nivel minim al valorilor. Evaluarea corectă a acestora are la bază fie proceduri de standardizare, fie competiții periodice, cu largă participare, cum ar fi cele care au loc sub egida organizției guvernamentale a SUA National Institute of Standards and Technology (Institutul național de standarde și tehnologie). Este necesar, de asemenea, ca, în cadrul fiecărei aplicații, să existe un raport acceptabil între proporțiile celor două categorii principale de erori (rata de acceptare, respectiv de rejecție falsă), pentru a reduce considerabil probabilitatea accesului unor persoane neautorizate la resurse sau spații protejate, fără însă a perturba utilizatorii cu drept de acces.

Se poate aprecia că recunoașterea facială reprezintă o tehnologie accesibilă și simplu de implementat datorită utilizării pe scară largă a camerelor încorporate (sau a unor camere web relativ ieftine) în majoritatea aplicațiilor. Dotarea 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).

Modelele de identificare facială utilizate în prezent pot întâmpina unele dificultăți în ceea ce priveşte identificarea corectă în spații slab iluminate precum şi a stării de viață a persoanei vizate, cerințe necesare pentru atingerea unui grad competitiv de securitate. [9] 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). [14] Performanțele majorității algoritmilor RF existenti, sunt influentate de cele mai mici variațiii de lumină. Au fost introduse diverse metode care să se ocupe de această problemă. Acestea sunt bazate pe conuri de lumină (Georghiades et al, 2001b;. Belhumeur și Kriegman, 1996), armonice sferice (Basri și Jacobs, 2003; Ramamoorthi și Hanrahan, 2001; Zhang si Samaras, 2003), imagini Quotient (Shashua și Riklin-Raviv, 2001. Wang et al, 2004), fețe degrade (Zhang și colab., 2009), variația totală logaritmică (Chen și colab., 2006), estimarea albedou (Biswas et al., 2009), determinare fotometrică (Zhou et al., 2007), și dicționare (Patel et al, 2011.; Lee și colab., 2005a).[14]

În urma cercetării realizate putem specifica faptul că majoritatea bibliotecarilor ar fi de acord cu implementarea unui sistem de recunoaștere facială, în biblioteca în care activează, pentru a sporii gradul de securitate. S-a putut observa că respondenții din străinătate au fost mai reținuți față de acest demers, în comparație cu cei din România și Moldova.

Bibliotecarii preocupați de securitatea persoanelor, în contextul terorismului, sunt dornici să implementeze un sistem de recunoaștere facială în biblioteca în care activează. De asemenea, bibliotecarii care cred că cel mai potrivit sistem de recunoaștere biometrică pentru securitatea colecțiilor și a persoanelor este recunoașterea facială, ar fi de acord cu implementarea unui astfel de sistem. Gradul de încredere în sistemele de recunoaștere facială, joacă un rol important în decizia bibliotecarilor de a mării gradul de securitate al bibliotecii, prin instalarea noului sistem.

Din datele analizate reiese faptul că mărimea bibliotecii, funcția bibliotecarilor, sau experiența de peste 31 de ani la locul de muncă nu intervin în decizia bibliotecarilor de a implementa noul sistem de recunoaștere facială. De asemenea, nivelul de pregătire al bibliotecarilor nu intervine în această decizie, probabil din cauză că majoritatea au mai mult decât studii medii.

Pentru dezvoltarea aplicației, se pot aduce îmbunătățiri în ceea ce privește scalabilitatea, prin construirea unei baze de date mai mari. Dacă se trece pe o bază de date de tip server, securitatea este mult mai puternică, putându-se opta pentru soluții de criptare a pozei și a numelui mai eficiente. O altă direcție de dezvoltare este îmbunătățirea predicției în diferite contexte. Cele 15 poze inițiale

sunt făcute consecutiv și sunt aproape identice, dar am putea defini mai multe ipostaze și condiții de iluminare, astfel soft-ul să detecteze corect o persoană în mai multe condiții.

Autentificarea biometrică nu va fi niciodată sigură, dar este una dintre cele mai fiabile metode de securitate actuale. Exactitatea sistemelor biometrice este afectată de factori precum non-universalitatea, zgomotul, lipsa reprezentării invariabile și caracterul non-distinctiv. Integrarea indicativelor multiple poate contribui la depășirea unora dintre aceste dezavantaje. Metodele mai bune de combinare a informațiilor din surse multiple au făcut obiectul unor cercetări ample. Nivelurile de început ale procesării (nivelurile de senzori și caracteristici) fac dificilă fuziunea informațiilor, în timp ce nivelul de decizie nu dispune de conținut suficient de informație. În consecință, nivelul de punctaj de potrivire este preferat de cercetători, acesta fiind compromisul dintre ușurința fuziunii și conținutul informațional. Sistemele biometrice nu sunt încă utilizate la scară largă din cauza performanței nesatisfăcătoare în comparație cu cerințele. Ca urmare, îmbunătățirea performanței sistemului (adică tema acestei teze) este cea mai importantă provocare pentru cercetare.

CONTRIBUȚII PERSONALE ŞI ORIGINALE

Contribuții personale şi originale

Evaluarea contribuțiilor autoarei, la dezvoltarea cunoaşterii ştiințifice, se realizează pe baza rezultatelor cercetării ştiințifice, din diferite perspective:

A. Contribuții cu caracter de sinteză

- Studiu referitor la cadrul general al securității colecțiilor și persoanelor în biblioteci.
- Studiu privind aspectele teoretice ale securității colecțiilor și persoanelor în biblioteci.

B. Contribuții cu caracter teoretic şi experimental

- Realizarea aplicației informatice pentru securitatea persoanelor și colecțiilor în biblioteci.
- Realizarea bazei de date cu utilizatori.
- Determinare experimentală cu privire la securitatea persoanelor și colecțiilor în biblioteci.

C. Contribuții cu caracter ştiințific curricular

- Elaborarea rapoartelor de cercetare ştiințifică din cadrul programului de cercetare la doctorat;
- Finalizarea tezei de doctorat;
- Stadiul actual al cercetărilor.

D. Noutatea tezei de doctorat

Teza de doctorat prezintă noutăți în ceea ce priveşte:

- Tematica şi obiectul investigațiilor teoretice;
- Analizarea comparativă a sistemelor de securitate utilizate in biblioteci.
- Analiza statistică a cerinței de implementare a unui sistem de securitate bazat pe recunoaștere facială în biblioteci.
- Realizarea arhitecturii aplicației informatice pentru securitatea persoanelor și colecțiilor în biblioteci.

E. Utilitatea rezultatelor cercetării

Utilitatea şi importanța științifică, didactică şi aplicativă a rezultatelor teoretice şi practice obținute de autor pe parcursul lucrării sunt confirmate de contribuțiile originale, precum şi aspectele prezentate în continuare:

- Dintr-o perspectivă științifică, aceste realizări reprezintă o contribuție însemnată în domeniul cercetării fundamentale, prin continuarea şi diversificarea studiilor privind aplicațiile informatice referitoare la implementarea sistemelor de securitate în biblioteci;
- Referitor la aspectele didactice sunt importante şi utile rezultatele ca atare, cu accent special pe metodologia şi tehnicile de cercetare aplicate;
- Cu privire la aspectele aplicative, fundamentarea teoretică a cunoştințelor obținute prin experiența practică, asociată realizării unui sistem de securitate destinat persoanelor și colecțiilor din biblioteci oferă un cadru adecvat cercetărilor viitoare din acest domeniu.

F. Valorificarea şi diseminarea rezultatelor cercetării în mediul academic științific

Valorificarea şi diseminarea rezultatelor cercetării în mediul academic științific s-a realizat prin:

- publicarea a 11 lucrări științifice şi articole în proceeding-urile evenimentelor științifice internaționale şi naționale ca prim autor şi coautor. Dintre acestea un articol a fost publicat într-o conferință internațională acceptată în revistă ISI, 2 articole în proceedings-uri indexate ISI, 5 articole în proceedings-uri indexate BDI și 3 în revistă BDI.

a) Lucrări proceeding ISI:

1. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A.,(2016), *Collection security management, based on facial recognition, at university libraries*. Globalization, Intercultural Dialogue And National Identity, Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7, Volume no. 3, pp 268-273. http://www.upm.ro/gidni3/?pag=GIDNI-03/vol03-Soc
2. **Botez A.M.,** Bejinaru-Mihoc A., Repanovici A., (2016), *Environmental impact on general health. Attitudes, opinions and types of behavior*. Globalization, Intercultural Dialogue And National Identity Arhipelag XXI Press, Tîrgu Mureș, ISBN: 978-606-8624-03-7, Volume no. 3, pp 274-285. http://www.upm.ro/gidni3/?pag=GIDNI-03/vol03-Soc

b) Lucrare la conferință internațională acceptată în revistă ISI

3. **Botez A.M.**, Volovici R., Volovici D., Repanovici A.,(2018), *Facial recognition system used in verification systems for library users*, **10thQualitative and Quantitative Methods in Libraries International Conference Chania, Crete, Greece.**

c) Lucrări proceeding BDI

4. Repanovici A., Bîrsan I., **Botez A.,** Druguș D. (2015), *Scientific information management using information systems within the open access to knowledge context*. Journal Plus Education, ISSN: 1842-077X, E-ISSN (online): 2068-1151, Volumul 12, Numărul 2.
5. Repanovici A., **Botez A.M.**, Stoianovici M., Roman N. (2016), *Measuring the Quality and Impact of Scientific Information. Scientometry Research Using Web of Science in the field of: Ethics in medical recovery.* Trivent Publishing, Series: Philosophy, Communication, Media Sciences, Volume: Communication Today: An Overview from Online Journalism to Applied Philosophy , pp 52-60. http://triventpublishing.eu/communicationtoday.html
6. Bejinaru-Mihoc A. **Botez A.M.**, Mitu G.L., (2015), *Regulations in the field of using medical devices. Overview. În: 6th International Conference ,,Computational Mechanics and Virtual Engineering*''. COMEC 2015, Braşov, pp.457-462.
7. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A., *Modele biometrice dactiloscopice cu aplicații în sistemele de identificare*. ISSN-L 1224-7928, Online: ISSN 2247-3548, Buletinul AGIR nr. 1/2016, pp 43-46. http://www.buletinulagir.agir.ro/numar_revista.php?id=123
8. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A.,(2016), *Library security management based on biometric methods*. The International scientific Conference of Librarians Western Balkan Information Literacy Conference, Bihac, pp 97-101.

d) Lucrări BDI

9. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A.,(2017) *Sisteme de recunoaștere facială: Probleme și perspective,* Buletinul AGIR 2, Creativitate, Inventică, Robotică.
10. Bejinaru-Mihoc A., **Botez A.M.,** (2017), *Cerințe juridice în utilizarea dispozitivelor medicale***,** Buletinul AGIR 2, Creativitate, Inventică, Robotică.
11. **Botez A.M.,** Repanovici A.,(2017) *Importanța securității persoanelor și a colecțiilor în biblioteci*, Revista Română de Biblioteconomie și Știința Informării/ Romanian Journal of Library and Information Science ISSN 1841-1940, Volume 13, Issue 1, pp. 11-20.

- realizarea rapoartelor de cercetare ştiinţifică din cadrul programului de pregătire ştiinţifică, finalizarea tezei de doctorat.

BIBLIOGRAFIE SELECTIVĂ

1. Akrouf S. (2011) *Une Approche Multimodale pour l'Identification du Locuteur, These,* Universite Ferhat Abbas-Setif, Republique Algerienne Democratique et Populaire.
2. Albrecht, S. (2012). Your local library can be a dangerous place. *Psychology Today.*
3. Albrecht, S. (2015). Library Security : Better Communication, Safer Facilities, American Library Association.
4. Biometrie-online.net. (2016). *Technologies*. [online] Disponibil la: https://www.biometrie-online.net/technologies/voix?view=category&id=14&layout= [accesat 2016].
5. Blansit, B.D., 2010. RFID Terminology and Technology: Preparing to Evaluate RFID for Your Library. *Journal of Electronic Resources in Medical Libraries*, 7(4), pp.344–354.
6. Botez A.M., Bejinaru-Mihoc A., Repanovici A. (2015) Modele biometrice dactiloscopice cu aplicații în sistemele de identificare. *Creativitate, Inventică, Robotică*, ediția a-XX-a, Brașov. Disponibil pe http://www.agir.ro/buletine/2497.pdf, [accesat la data de 25.10.2017]
7. Botez A.M., Bejinaru-Mihoc A., Repanovici A. (2016) *Collection security management, based on facial recognition, at university libraries*. Globalization, Intercultural Dialogue And National Identity 3rd Edition. Tîrgu Mureș. Disponibil pe: http://www.upm.ro/gidni3/GIDNI-03/Soc/Soc%2003%2026.pdf, [accesat la 25.08.2017]
8. Botez A.M., Bejinaru-Mihoc A., Repanovici A. (2016) *Library security management based on biometric methods*. The International scientific Conference of Librarians Western Balkan Information Literacy Conference, Bihac. Disponibil pe: http://wbilc2018.com/files/proceedings/PROCEEDINGS_WBILC2016.pdf, [accesat la 28.03.2017]
9. Botez A.M., Bejinaru-Mihoc A., Repanovici A.(2016) *Environmental impact on general health. attitudes, opinions and types of behavior*. Globalization, Intercultural Dialogue And National Identity 3rd Edition. Tîrgu Mureș. Disponibil pe: http://www.upm.ro/gidni3/GIDNI-03/Soc/Soc%2003%2027.pdf, [accesat la 28.10.2017]
10. Botez A.M., Repanovici A. (2017) *The importance of security for people and collections in libraries* (Importanța securității persoanelor și a colecțiilor în biblioteci). Revista Română de Biblioteconomie și Știința Informării, ISSN 1841-1940. Vol. 13, Issue 1, pp. 11-20. Disponibil pe: http://www.rrbsi.ro/index.php/rrbsi/article/download/20/rrbsi-vol13-iss1-2017-p11-20.pdf/, [accesat la:30.05.2017]
11. Brooks I. (2009) *Organisational Behaviour: Individuals, Groups and Organisation*. Pearson Education, 355 p.
12. Chellappa. R, Jie N., Vishal M.P. (2012) *Remote identification of faces: Problems, prospects, and progress. Pattern Recognition Letters*, 33(14), 1849–1859.

13. Guerrier Cl., Cornelie L-A., *Les aspects juridiques de la biometrie*. [Online] Disponibil pe: biometrics.it-sudparis.eu/.../rep4072e2adb7d5a.doc [accesat: 2015].
14. Harris J.L., Dimarco S.R. (2010). Locking Down a University Library: How to Keep People Safe in a Crisis: A Mansfield University of Pennsylvania Perspective. *Library & Archival Security*, 23(1), pp.27–36.
15. Heiko, K., Pohl H. (2004) RFID security. *Information Security Technical Report*, 9(4), pp.39–50.
16. Henrici D. (2008) *RFID Security and Privacy: Concepts, Protocols, and Architectures*, Berlin: Springer-Verlag Berlin Heidelberg.
17. Kahn MB (2007) *Library Security and Safety Guide to Prevention*, Planning, and Response, ALA Editions, Chicago. Disponibil pe: ProQuest Ebook Central.
18. Kitsos P., Y. Zhang (eds.) (2008) *RFID Security: Techniques, Protocols 3 and System-on-Chip Design*, New York (N.Y.) : Springer Science+Business Media, 446p.
19. Kusuma G.P., Chua C.S. (2011) PCA-based image recombination for multimodal 2D+3D face recognition. *Image and Vision Computing*, 29, 306–316.
20. Latuszek Jr., T. (2002). Library Security: A Growing Awareness. *Library & Archival Security*, 15(2), pp.3–7.
21. Lupu Cătălin (2015) *Stadiul actual privind recunoaşterea persoanelor după iris şi amprentă*. Raport de cercetare nr. 1. Coordonator ştiințific: prof. univ. dr. ing. Vasile-Gheorghiță GĂITAN. Suceava Disponibil pe http://perform.usv.ro/rapoarte/13/raport_cercetare_1.pdf, [accesat la 04.07.2016]
22. Maidabino A.A. & Zainab A.N. (2012). A holistic approach to collection security implementation in university libraries. *Library Collections, Acquisition and Technical Services*, 36(3–4), pp.107–120.
23. Mihăilescu M. I. (2014) Contribuții asupra Securității Protocoalelor Biometrice de Autentificare. Rezumat teză doctorat. Universitatea din București. Cond. șt.: prof.univ.dr. A. Atanasiu. Disponibil pe: http://fmi.unibuc.ro/ro/pdf/2014/doctorat/rezumatMihailescu.pdf, [accesat la 10.02.2017]
24. Molnar D., Wagner D. (2004) Privacy and security in library RFID: issues, practices, and architectures. *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pp.210–219.
25. Park K.Y, Hwang S.Y., (2014) *An improved Haar-like feature for efficient object detection,* Department of Electronic Engineering, Sogang University, C.P.O. Box 1142, Seoul 100-611, Republic of Korea, Pattern Recognition Letters, 42, 148–153.
26. Phillips P.J., Moon H., Rizvi S.A., Rauss P.J. (2000) The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactionson Pattern Analysisand Machine Intelligence*, 22(10), 1090–1104.
27. Piccolotto P., Maller P. (2014) Biometrics from the User Point of View: Deriving Design Principles from User Perceptions and Concerns about Biometric Systems, 2014, *Technology Journal*, 18(4).
28. Popa Gh. (2011) *Metode şi tehnici de identificare criminalistică*. București: Ed. AIT Laboratories s. r. l., ISBN: 978-606-8363-01-1.

29. Pulli B.K., Baksheev A. (2012) Real-Time Computer Vision with OpenCV. *Communications of the ACM*. **55**(6) pp.61-69.
30. Rajgarhia A. (2007) *Face Detection using Independent Component Analysis*, CS 229 Final Project Report. Disponibil pe: http://cs229.stanford.edu/proj2007/Rajgarhia-FaceDetectionUsingICA.pdf [accesat 5.10.2017]
31. Rath Subrat K., Siddharth S.R. (2014) A Survey on Face Detection and Recognition Techniques in Different Application Domain. *I.J. Modern Education and Computer Science*, **6**(8), 34-44.
32. Sacu (Druguș) D. (2014) *Cercetări privind managementul serviciilor medicale în sistemul de sănătate din România*. Rezumat teză de doctorat. Cond. Şt.: prof. univ. dr. Doina Azoicăi. Iași. Disponibil pe http://www.umfiasi.ro/Concursuri/sesapiu/mg_conf_p05_stiinte/7.%_20rezumat%20teza%20doctorat%20(romana,%20engleza).pdf [accesat 15.09.2016]
33. Sahoo S.K., Tarun Choubisa and S. R. Mahadeva Prasanna (2012) Multimodal Biometric Person Authentication: a Review, *IETE Technical Review*, **29**(1), 54-75.
34. Scribd. (2016). *Biometrie*. Disponibil la: https://www.scribd.com/document/94778231/biometrie, [accesat la 10.12.2016]
35. Scribd. (2017). *Capitolul1.pdf*. [online] Disponibil la: https://es.scribd.com/document/335661736/Capitolul1-pdf [accesat la data de 15.03.2017].
http://scs.etc.tuiasi.ro/iciocoiu/courses/ESL/homeworks/hw2/Capitolul1.pdf
36. Scribd. (2018). *Recunoaşterea_feţelor*. [online] Disponibil la: https://www.scribd.com/document/339937718/Recunoa%C5%9Fterea-fe%C5%A3elor [accesat la data de 15.03.2018]
37. Suarez O.D. (2014) OpenCV Essentials, Olton: Packt Publishing - ebooks Account, 214 p. Disponibil pe: ProQuest Ebook Central.
38. Thompson, Samuel T.C. (2006) Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*. **25**(4), pg. 222+.
39. Unar J.A., Woo Chaw Seng, Almas Abbasi (2014) A review of biometric technology along with trends and prospects. *Pattern Recognition*, **47**(8), 2673-2688.
40. Ustundag, Alp (2013).*The Value of RFID*, London: Springer London, pp. 3-12.
41. vdocuments.site. (2017). *Sistem biometric - [PDF Document]*. [online] Disponibil la: https://vdocuments.site/sistem-biometric.html [accessat 11.08. 2017].
42. VisageCloud. (2017). *VisageCloud - Transforming face recognition into business value*. [online] Disponibil la: https://visagecloud.com/faq, [accesat la 17.12.2017]
43. VisageCloud. (2018). *VisageCloud - Transforming face recognition into business value*. [online] Disponibil la: https://visagecloud.com/get- started [accesat la data de 25.02.2018]
44. Visagecloud.com. (2018). *Features*. [online] Disponibil pe: https://visagecloud.com/ features [accesat la data de 10.01.2018]
45. Visagecloud.com. (2018). *Swagger UI*. [Online] Disponibil pe: https://visagecloud.com/ swagger-ui.html [accesat la data de 15.03.2018]

46. Visagecloud.com. (2018). *The VisageCloud Domain Model.* [online] Disponibil la: https://visagecloud.com/ domain-model [accesat la data de 18.04.2018]
47. Vrejoiu M.H.; Hotăran M.A. (2013) Detectarea automată a fe elor umane. Metoda Viola-Jones, *Revista Română de Informatică şi Automatică*, **23**(2), 21-32. Disponibil pe: https://vdocuments.site/aplicatii-rna-and-facial.html. [Accesat la data de 15.05.2017]
48. Want R.(2006) An introduction to RFID Technology. *IEEE Pervasive Computing*, **5**, pp. 25-33.
49. Webopedia.com. (2016). *What is Layer? Webopedia Definition*. [online] Disponibil la: https://www.webopedia.com/TERM/L/layer.html [accesat la data de 30.03.2016]
50. Webopedia.com. (2017). *What is Ontology Web Language (OWL)? Webopedia Definition*. [online] Disponibil la: https://www.webopedia.com/TERM/O/Ontology_Web_Language.html [accesat la data de 11.08.2017]
51. Westenkirchner S. (2008) Integrated Library Security Systems. *Library & Archival Security*, **21**(2), p.159-167.
52. Woodward J.D., Horn C., Gatune J., Thomas A. (2003) *Biometrics. A Look at Facial Recognition*. Santa Monica, CA: RAND Corporation. [Online] Disponibil pe: https://www.rand.org/pubs/documented_briefings/DB396.html [accesat 17.07.2017]
53. Xu Y., Zhang Z., Lu G.M., Yang, J. (2016) Approximately symmetrical *face* images for image preprocessing in *face recognition* and sparse representation based classification. *Pattern Recognition* , **54**(C), 68-82.
54. Yang M.H., Kriegman D.J., Ahuja N. (2002) *Detecting faces in images: a survey*. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. **24** (1), 34–58.
55. Zedner Lucia (2009). *Security*: *Key Ideas in Criminology.* Taylor and Francis, 206p. Disponibil pe: ProQuest Ebook Central.
56. Zhou C., Wang L., Zhang Q., Wei X. (2013) Face recognition based on PCA image reconstruction and LDA. *Optik - International Journal for Light and Electron Optics* **124**(22) 5599– 5603.

CERCETĂRI TEORETICE ȘI EXPERIMENTALE ASUPRA DEZVOLTĂRII SISTEMELOR BIOMETRICE

Primul capitol intitulat ***Cadrul general al securității colecțiilor şi al persoanelor în biblioteci*** abordează probleme legate de "securitate", termen ce poate avea o varietate de conotații în lumea bibliotecii.
Subcapitolul 1. şi 2. Tratează **siguranța personală** (pentru utilizatori și personal): măsuri de precauție împotriva actelor de violență, iar în subcapitolul 3. Sunt prezentate **măsuri de precauție pentru a proteja colecțiile bibliotecii** împotriva furtului, deoarece aceste două aspecte sunt cele care influențează în mod direct clienții.

Aspecte teoretice privind sistemele de recunoaștere facială este titlul celui de al 2-lea capitol, care îşi propune definirea şi prezentarea sistemelor de recunoaştere biometrică. Biometria este recunoașterea automată a persoanelor pe baza caracteristicilor lor comportamentale și biologice.

O temă larg răspândită în cercetarea biometrică o constituie recunoașterea feței dintr-o imagine, care face obiectul subcapitolului 2. Procesul de identificare sau verificare automată a persoanelor din cadre sau imagini video digitale, în funcție de baza de date disponibilă, se numește *recunoașterea feței*. Obiectivul căutării de fețe dintr-o imagine sursă sau video este denumit *detectare a feței*.

S-a efectuat clasificarea tehnicilor de detectare a feței, au fost analizați patru dintre algoritmii de recunoaştere facială în subcapitolul 3.

Dificultățile şi neajunsurile apărute la sistemele de verificare biometrică au fost menționate în încheierea capitolului 2.

A fost realizată ***Cercetarea statistică privind determinarea opiniilor managerilor de bibliotecă și a bibliotecarilor cu privire la nevoia de implementare a unui nou sistem de securitate și sistemele existente din biblioteci***, studiu prezentat în cadrul **capitolului 3**. Conceperea chestionarului, analizarea şi interpretarea datelor culese sunt detaliate în cadrul capitolului.

Cel de-**al 4-lea capitol,** ***Optimizarea sistemului de securitate din biblioteci prin implementarea unui sistem de recunoaștere facială*** este dedicat în întregime aplicației VisageCloud. Aplicația informatică dezvoltată, monitorizează accesul în biblioteci, fiind creată ca răspuns la cererea tot mai mare de a avea un sistem eficient de control al accesului și prezenței într-o locație, în contextul terorismului. Capitolul începe prin prezentarea câtorva noțiuni introductive, necesare înțelegerii funcționării aplicației practice. Următorul subcapitol prezintă **Modelul de domeniu al aplicației VisageCloud** precum şi **Interfața de programare (API)** necesare realizării aplicației propriu-zise.

În subcapitolul 3, ***VisageCloud: detectarea și recunoașterea feței*** sunt parcurse etapele necesare funcționării efective a aplicației. Sunt descrişi cei 6 paşi care sunt necesari a fi efectuați în vederea obținerii recunoaşterii faciale a unei persoane dintr-o fotografie.

Ultimul capitol ***Concluzii finale, Contribuții proprii (autentice)*** prezintă în formă sintetică rezultatele cercetării prin evidențierea contribuțiilor proprii şi a soluțiilor originale care au făcut posibilă realizarea obiectivelor stabilite în cadrul lucrării.

THEORETICAL AND EXPERIMENTAL RESEARCH ON THE DEVELOPMENT OF BIOMETRIC SYSTEMS

The first chapter titled **General framework for the security of collections and individuals in libraries** addresses "security" issues, a term that can have a variety of connotations in the library world.

Subchapter 1 and 2 deal with **personal safety** (for users and staff): precautions against violence, and in subchapter 3 are presented **precautions to protect library collections against theft** because these two aspects are the ones that directly influence customers.

Theoretical aspects of facial recognition systems is the title of the 2nd chapter, which aims to define and present biometric recognition systems. Biometrics is the automatic recognition of people based on their behavioral and biological characteristics.

A widespread theme in biometric research is face recognition in an image, which is covered in subchapter 2. The process of identifying or automatically checking people in frames or digital video images, based on the available database, is called face recognition. The objective of looking for faces in a source or video image is called face detection.

Classification of face detection techniques was performed, four of the facial recognition algorithms were analyzed in subchapter 3.

Difficulties and shortcomings in biometric verification systems have been mentioned in Chapter 2.

The statistical research on **determining the views of library managers and librarians for the need to implement a new security system and the existing systems in libraries** was carried out, study presented in **Chapter 3**. The design of the questionnaire, the analysis and the interpretation of the collected data are detailed in within the chapter.

The 4th chapter, Optimizing the security system in libraries by implementing a facial recognition system is entirely dedicated to VisageCloud. The developed computer application monitors access to libraries and is designed to respond to the growing demand for an effective system to control access and presence in a location in the context of terrorism. The chapter begins by presenting some introductory notions needed to understand the operation of the practical application. The next subchapter shows the **VisageCloud Application Domain Model** and the **Programming Interface (API)** needed to complete the application itself.

In subchapter 3, **VisageCloud: Face Detection and Recognition** the necessary steps to the actual operation of the application are taken.

The last chapter **Final conclusions, Own contributions (authentic)** present in a synthetic form the results of the research by highlighting their own contributions and the original solutions that made it possible to achieve the objectives set in the paper.

CURRICULUM VITAE

INFORMAȚII PERSONALE	Andra- Manuela Botez (căs. Bejinaru Mihoc)
	Brașov (România)
	Sex

EDUCAȚIE ȘI FORMARE

2014- prezent	**Doctorand** în domeniul Inginerie și management, Universitatea Transilvania din Brașov, Facultatea de Design de produs si mediu
2009 – 2013	**Studii universitare:** Universitatea Spiru Haret din Brașov, Facultatea de Științe Juridice și Administrative, Specializarea Drept.
2010 – 2012	**Masterat:** Universitatea Transilvania din Brașov, Facultatea de Medicină, Specializarea Managementul strategiilor preventive și politici sanitare.
2007 – 2010	**Studii universitare:** Universitatea Transilvania din Brașov , Facultatea de Drept și Sociologie, Specializarea Sociologie.
2003 – 2007	**Liceul** cu program sportiv

EXPERIENȚĂ PROFESIONALĂ

18.04. 2018 - prezent	Inspector/Referent Resurse Umane
2012-2013	Practică de specialitate , Proiect Posdru.
2010-2011	Colaborator Comercial

ACTIVITATE ŞTIINIFICĂ

- Articole publicate: 11 din care: 2 lucrări proceeding ISI, 1**lucrare la conferință internațională acceptată în revistă ISI,** 5 articole în proceedings-uri indexate BDI și 3 în revistă BDI.

LIMBĂ STRĂINĂ: Engleză, Franceză

Universitatea Transilvania din Brașov

CURRICULUM VITAE

PERSONAL INFORMATION	Andra- Manuela Botez (name after marriage-Bejinaru Mihoc)
	Brașov (România)
	Sex

EDUCATION AND TRAINING

2014- present	**Phd. Student** in Engineering and Management Transilvania University of Brasov, Faculty of product design and environment,
2009 – 2013	**University studies:** Spiru Haret University of Brasov, Faculty of Law and Administration, Law specialization.
2010 – 2012	**Masteral studies:** Transilvania University of Brasov, Faculty of Medicine, Management of preventive strategies and health policies.
2007 – 2010	**University studies:** Transilvania University of Brasov, Faculty of Law and Sociology, Sociology specialization.
2003 – 2007	**Sports High School**

PROFESSIONAL EXPERIENCE

18.04. 2018 - present	Human Resources Inspector /Referent
2012-2013	Speciality Practice, Posdru Project.
2010-2011	Commercial Collaborator

ACTIVITATE ŞTIINIFICĂ

Published articles: 11 out of which: 2 ISI proceedings, 1 paper at an international conference accepted in the ISI journals, 5 articles in BDI indexed proceedings and 3 in the BDI journals.

FOREIGN LANGUAGE: English, French