



Universitatea
Ștefan cel Mare
Suceava

Facultatea de Inginerie
Electrică și Știința
Calculatoarelor

TEZĂ DE DOCTORAT

DOMENIUL CALCULATOARE ȘI TEHNOLOGIA INFORMAȚIEI

Contribuții privind recunoașterea persoanelor după iris și amprentă

REZUMAT

CONDUCĂTOR ȘTIINȚIFIC:

Prof.univ.dr.ing. Vasile-Gheorghiuță GĂITAN

DOCTORAND:

Ing. Cătălin LUPU

Suceava, 2017

www.usv.ro



Investește în oameni !

FONDUL SOCIAL EUROPEAN

Proiect cofinanțat din Fondul Social EUROPEAN prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007 – 2013

Această lucrare a beneficiat de suport financiar prin proiectul

Performanță sustenabilă în cercetarea doctorală și post doctorală - PERFORM

Contract nr POSDRU 159/1.5/S/138963

Axa prioritară 1 - Educația și formarea profesională în sprijinul creșterii economice și dezvoltării societății bazate pe cunoaștere

Domeniul major de intervenție 1.5 - „Programe doctorale și postdoctorale în sprijinul cercetării”



Universitatea
Ștefan cel Mare
Suceava

DECIZIA D 138 / 5.09.2017

privind constituirea comisiei pentru susținerea publică a unei teze de doctorat

În conformitate cu prevederile H.G. nr. 26/12.01.2017 privind organizarea și funcționarea Ministerului Educației Naționale, Anexa 3, punctul 39, prin care se instituționalizează Universitatea Ștefan cel Mare din Suceava;

În conformitate cu HG 681 din 29.06.2011 - Codul Studiilor universitare de doctorat;
Având în vedere aprobarea conducerii Universității;

Rectorul Universității "Ștefan cel Mare" din Suceava emite prezenta decizie:

Art. 1 - Se numește comisia de doctorat pentru susținerea publică a tezei de doctorat în data de **28.09.2017**, cu titlul: **„CONTRIBUȚII PRIVIND RECUNOAȘTEREA PERSOANELOR DUPĂ IRIS ȘI AMPRENTĂ”**,

elaborată de **LUPU V. Cătălin**,
înmatriculat la data de 1.10.2013,
forma de învățământ: cu frecvență, cu taxă,
DOMENIUL: **Calculatoare și tehnologia informației**

PREȘEDINTE:

- Prof. univ. dr. ing. Adrian GRAUR, reprezentant IOSUD, Universitatea "Ștefan cel Mare" din Suceava;

CONDUCĂTOR ȘTIINȚIFIC:

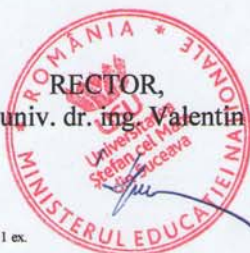
- Prof. univ. dr. ing. Vasile Gheorghiță GĂITAN, Universitatea "Ștefan cel Mare" din Suceava;

REFERENȚI:

1. Prof. univ. dr. ing. Florina UNGUREANU, Universitatea Tehnică "Gh. Asachi" din Iași;
2. Prof. univ. dr. ing. Mitică CRAUS, Universitatea Tehnică "Gh. Asachi" din Iași;
3. Prof. univ. dr. ing. Ștefan-Gheorghe PENTIUC, Universitatea "Ștefan cel Mare" din Suceava.

Art. 2. – Direcția Economică respectiv serviciul Secretariat - doctorat vor duce la îndeplinire dispozițiile prezentei decizii.

RECTOR,
Prof. univ. dr. ing. Valentin POPA



SECRETAR ȘEF UNIV.,
Jurist Maria MUSCĂ

C.Sk./C.Sk. / 1 ex.

Universitatea "Ștefan cel Mare" Suceava, Str. Universității nr. 13, 720 229 Suceava, România
Tel: +40 230 520 081, Fax: +40 230 520 080, Web: www.usv.ro

Introducere

Biometria reprezintă un termen derivat din cuvintele grecești *bios* (viață) și *metrikos* (măsură) și reprezintă mai multe metode automatizate utilizate în identificarea unei persoane folosind anumite caracteristici biometrice (geometria palmelor, amprenta digitală, irisul, retina, geometria feței, greutatea corpului, presiunea sanguină, etc.) sau comportamentale (timbrul vocal, configurația ADN, dinamica scrisului, scanarea semnături, dinamica acționării tastelor, etc.) ale acesteia, știut fiind faptul că unele dintre aceste caracteristici biometrice, de exemplu amprentele digitale sau irisul, ori comportamentale, de exemplu timbrul vocal, pot identifica în mod unic o persoană. Dată fiind această unicitate, informațiile biometrice pot fi folosite pentru proiectarea și implementarea unor tehnologii, echipamente și sisteme destinate determinării identității cu performanțe mult superioare celor existente.

Una dintre cele mai cunoscute caracteristici biometrice este reprezentată de amprenta digitală, savantul britanic Sir Francis Galton fiind primul care a propus utilizarea amprentei degetelor în scopul identificării încă din secolul al XIX-lea. Acesta a elaborat un studiu detaliat asupra amprentelor degetelor în care a prezentat și un sistem de clasificare bazat pe amprentele tuturor celor zece degete ale mâinilor, sistem ce stă și astăzi la baza schemelor de identificare aflate în uz. Amprentarea a fost introdusă ca metodă de identificare a persoanei în poliția britanică începând cu anul 1890 de către Sir Richard Edward Henry.

În termenii tehnologiei informației, biometria este asociată tehnologiilor și tehnicilor destinate securității și confirmării identității pe baza unor caracteristici biologice individuale și măsurabile ale persoanei. De exemplu, amprentele digitale, geometria mâinii, geometria feței, amprenta (codul) irisului sau a retinei, timbrul vocal pot fi utilizate în sisteme și scheme destinate accesului la un computer, într-o anumită încăpere și, de ce nu, la un cont bancar.

Identificarea automată a persoanei reprezintă procesul prin care un sistem biometric asociază o persoană unei identități specifice, acest lucru putându-se realiza în termenii verificării sau identificării. În cadrul procesului de verificare, sistemul numai autentifică o identitate pretinsă; cu alte cuvinte sistemul verifică dacă o persoană este cine pretinde că este. În cadrul identificării crește complexitatea procesului, sistemul determinând identitatea persoanei prin consultarea unei baze de date sau prin testarea unei rețele neuronale cu informații despre persoane, cu alte cuvinte, sistemul determină cine este persoana respectivă fără ca aceasta să precizeze un nume ori alte informații de identificare.

Proiectarea unui sistem de verificare este mult mai simplă decât a unui de recunoaștere a identității. Un sistem de verificare autentifică identitatea pretinsă de persoană prin compararea trăsăturilor biologice particulare furnizate de aceasta la un anumit moment cu măsurile acestor trăsături memorate anterior în sistem și asociate identității pretinse de persoană; de exemplu, amprenta degetului inelar a unei persoane ce pretinde a fi Popescu este comparată cu amprenta degetului inelar a lui Popescu memorată anterior într-o bază de date sau într-o rețea neuronală a sistemului. Spre deosebire de sistemul de verificare, sistemul de identificare sau recunoaștere are o complexitate procedurală mai crescută, trăsăturile biometrice furnizate de o persoană fiind comparate cu măsurile tuturor trăsăturilor biometrice similare stocate într-o bază de date sau într-o rețea neuronală. De exemplu, amprenta unei persoane ce dorește accesul într-o cameră cu destinație specială este comparată cu amprentele tuturor persoanelor autorizate să intre în acea încăpere. Un alt exemplu concludent îl constituie accesul într-un autoturism personal. Există sisteme anti-fraudă utilizate pentru protejarea împotriva furtului autoturismului sau a bunurilor aflate în interiorul său. Sistemul cuprinde sisteme senzoriale complexe (de tip web-cam) amplasate în interiorul/exteriorul mașinii, iar atunci când cineva dorește să pătrundă în interiorul autovehiculului, este verificat

dacă are acces să pătrundă sau nu; persoanele care au acces în acel autovehicul au codul irisului sau amprenta digitală memorate într-o bază de date; dacă persoana are codul în baza de date i se permite să deschidă ușile sau să pornească motorul, altfel se transmit frame-uri la Poliție, firme de pază sau la proprietarul autovehiculului și se poate interveni în timp util.

Nevoia pronunțată de a determina sau verifica identitatea persoanelor a dus la creșterea importanței cercetării în domeniul autentificării biometrice. Autentificarea biometrică reprezintă știința stabilirii unei identități, bazându-se pe atributele fizice sau comportamentale ale unui individ, dintre acestea făcând parte amprenta, fața, vocea, mersul, irisul, semnătura, geometria mâinii, urechea, etc. Devine din ce în ce mai evident faptul că o singură trăsătură biometrică (folosită într-un sistem unibiometric) nu este suficientă pentru a atinge anumite cereri importante ale sistemului – incluzând performanța de potrivire – impuse de multe aplicații de autentificare la scară largă. Sistemele multibiometrice vin să elimine oarecum neajunsurile întâmpinate de sistemele unibiometrice prin luarea măsurilor necesare pentru identificarea persoanelor de la multe surse biometrice. Aceste sisteme pot îmbunătăți în mod evident performanțele de recunoaștere ale unui sistem biometric, în același timp asigurând, de exemplu, deturnarea atacurilor asupra sistemelor sau reducerea ratei de eroare la înregistrare (failure-to-enroll rate - FER). Deși necesitățile de stocare, timpul de procesare și cerințele de calcul ale unui sistem multibiometric pot fi în mod semnificativ mai mari decât în cazul unui sistem unibiometric, avantajele menționate anterior reprezintă un motiv suficient de puternic pentru implementarea sistemelor multibiometrice în sisteme de autentificare la scară largă (de exemplu, pentru controlul pasagerilor la trecerea frontierei de stat) și în sisteme care necesită rate de acuratețe foarte mari (de exemplu, accesul într-o bază miliară securizată).

Domeniul multibiometricii a avut o creștere foarte rapidă și importantă în ultimii câțiva ani. Această creștere a fost alimentată și de către hotărâri ale guvernului american, care a stipulat utilizarea metodelor biometrice de recunoaștere pentru furnizarea unor funcții sociale foarte importante. Programul US-VISIT (United States Visitor and Immigration Status Indicator Technology) este un sistem de securizare a procesului de trecere a frontierei americane, care validează documentele de călătorie ale cetățenilor străini în Statele Unite. La începutul programului, amprente degetelor index de la ambele mâini erau folosite pentru a asocia o viză cu un individ care intră în Statele Unite. În prezent, toate cele zece degete sunt folosite, în acest fel fiind nevoie de dezvoltarea unui sistem mai fiabil de prelevare a datelor, precum și de algoritmi de fuzionare a caracteristicilor. Acest proces a început pe 29 noiembrie 2007, primul aeroport pe care s-au făcut astfel de teste fiind Washington Dulles International Airport. Organizația Aviației Civile Internaționale (International Civil Aviation Organization – ICAO) a recomandat ca statele sale membre să folosească documente de călătorie care pot fi citite de un dispozitiv electronic (Machine Readable Travel Documents – MRTD) care să încorporeze cel puțin fața ca identificator biometric (pot fi de asemenea folosite anumite combinații între față, amprentă și iris) pentru stabilirea identității deținătorului unui pașaport. Astfel, cercetarea în tehnologiile multibiometrice are posibilitatea să influențeze multe aplicații pe scară largă, civile sau comerciale.

Din punct de vedere academic, cercetarea în multibiometrie are diverse aspecte:

- identificarea surselor informației biometrice;
- determinarea tipurilor de informație care pot fuziona;
- designul unor metode optime de fuzionare;
- evaluarea și compararea diverselor metode de fuzionare;
- crearea de interfețe multimodale robuste care să faciliteze achiziția eficientă a datelor multibiometrice.

După evenimentele petrecute în New York în ziua de 11 septembrie 2001, sensul controlului accesului în sistem s-a schimbat radical, atât prin prisma *mijloacelor de exercitare*, cât și a *domeniilor de aplicare*. În privința mijloacelor, dominantă a fost discuția

de la sfârșitul anilor '90, dacă trebuie să se introducă sau nu sistemele de identificare biometrică a persoanelor, făcându-se asocierea cu luarea amprentelor digitale doar pentru elucidarea unor cazuri criminale. Opoziția cea mai puternică venea din partea sistemului bancar, dar nu numai. Alte instrumente păreau incomode sau periculoase și, ca atare, erau refuzate în serie. După data susmenționată lucrurile s-au schimbat radical în privința identificării biometrice.

Domeniile de aplicare s-au extins, totul venind din convingerea puternică a proprietarilor și administratorilor de sisteme, evidențiindu-se astfel și alte modalități de verificare a persoanelor ce doresc accesul în mai toate instituțiile prezidențiale, guvernamentale și altele de tip public sau privat, iar aeroporturile și-au extins zonele supuse unei atenții speciale.

Nici sistemele informaționale nu au rămas aceleași. Doar simpla trimitere la ceea ce au realizat mai multe firme importante pe linia securizării este destul de elocventă, căci aproape orice mișcare a personalului este sub control, apelându-se la dependența totală a acestuia de carduri speciale. Se poate spune că, în sistemele distribuite de prelucrare a datelor, dar și în cele centralizate, se impun sisteme performante de control al accesului. Se spune că „paza bună *alungă* primejdia rea”, ceea ce ar putea să evidențieze o bună înțelegere a *amenințărilor* la care este expus un sistem, a *vulnerabilităților* lui, dar și a *riscurilor* ce-i sunt asociate, îndeosebi pe linia infrastructurii sistemelor, de aici rezultând o bună identificare a *măsurilor preventive* de contracarare a lor.

Pe baza acestor provocări în domeniu și a experienței acumulate s-a elaborat prezenta teză de doctorat, în scopul dezvoltării de metode și aplicații noi pentru recunoașterea persoanelor după iris și amprentă.

Obiectivul principal al acestei teze de doctorat îl reprezintă îmbunătățirea metodelor existente de recunoaștere a persoanelor după iris și amprentă, precum și realizarea de aplicații în vederea validării practice a metodelor propuse. Domeniul este foarte vast și a fost cercetat timp îndelungat, dar totuși este de foarte mare actualitate, lucru care se poate vedea și din numărul mare de articole și cărți apărute pe aceste subiecte. Dacă în cazul recunoașterii persoanelor prin utilizarea amprente se poate vorbi de faptul că aceasta a fost studiată de mai bine de un secol, în ceea ce privește recunoașterea persoanelor după iris cercetarea metodelor de recunoaștere a persoanelor după acesta se poate spune că este abia la început, primul patent cu o complexă modelare matematică apărând destul de recent, în urmă cu aproximativ două decenii.

Obiectivul principal va fi susținut prin:

- studii și cercetări privind modalități noi de abordare a recunoașterii persoanelor după iris și amprentă;
- îmbunătățirea timpului necesar prelucrării imaginilor obținute de la un senzor sau dintr-o bază de date, în scopul extragerii de caracteristici utile, precum și a timpului pentru recunoașterea (identificarea sau verificarea) persoanelor;
- îmbunătățirea modalității de recunoaștere a persoanelor, prin utilizarea a două caracteristici biometrice, în loc de una singură cum se întâmplă în cele mai multe dintre cazuri.

Oportunitatea tezei de doctorat este dată de:

- evoluțiile tehnologice importante în ceea ce privește necesitatea securizării la un nivel superior a aplicațiilor de control acces, fie că este vorba despre accesul într-o locație sau la o anumită aplicație, de exemplu de internet banking;
- direcțiilor noi de cercetare din domeniul biometriei, vizibile atât la nivelul dezvoltării continue a senzorilor implicați în procesul de preluare a imaginilor ce

urmează a fi prelucrate, precum și a algoritmilor și metodelor propuse pentru recunoașterea persoanelor prin utilizarea caracteristicilor biometrice.

Teza de doctorat este structurată astfel: *Introducere*, cinci *capitole*, *Bibliografie* și trei *Anexe*. Structura capitolelor tezei este prezentată în continuare:

Capitolul I – „Stadiul actual al recunoașterii persoanelor după iris și amprentă” reprezintă o introducere în domeniul tehnologiilor biometrice. Principala contribuție este dată de prezentarea unitară și detaliată a noțiunilor de biometrie. Se prezintă funcționarea sistemelor biometrice, diferențele între verificare și autentificare, performanțele unui sistem biometric și aplicații ale biometriei. Au fost studiate și prezentate de asemenea câteva lucrări reprezentative pentru cele două metode biometrice propuse în teză, și anume recunoașterea persoanelor după iris și amprentă, fiind extrase principalele contribuții ale autorilor în acest domeniu.

În **capitolul II – „Contribuții privind recunoașterea persoanelor după iris”** s-au descris pentru început principalele etape parcurse în scopul recunoașterii persoanelor după iris, de la achiziția imaginii de la camera dedicată în acest sens până la obținerea codului irisului și potrivire. S-au luat pentru exemplificare 4 imagini din baza de date CASIA, care apoi au fost trecute prin toți pașii pentru a se obține codul irisului. Pentru fiecare pas s-au arătat rezultatele obținute prin aplicarea diverselor filtre sau tehnici asupra imaginilor. De asemenea, s-au studiat facilitățile oferite de camera pentru recunoaștere după iris Panasonic BM-ET100US precum și de camera UBKEY MirrorKem.

Capitolul III – „Contribuții privind recunoașterea persoanelor după amprenta digitală” cuprinde în partea de început pașii necesari pentru recunoașterea persoanelor după amprenta digitală. Din studierea metodelor propuse de către Nalini K. Ratha și Wu Zhi-Li, s-a propus o nouă schemă de principiu pentru recunoașterea persoanelor după amprentele digitale. Principalele avantaje preconizate sunt reprezentate de renunțarea la aplicarea transformatei Fourier rapide, folosirea filtrelor Gabor și a metodei Canny pentru detecția muchiilor. În scopul validării rezultatelor obținute, autorul a creat o aplicație în MatLab interactivă și în mod grafic, în care se pot vedea toate fazele prin care trece o amprentă digitală, de la încărcarea imaginii dintr-un fișier până la marcarea punctelor caracteristice. Finalul acestui capitol conține contribuțiile autorului în ceea ce privește potrivirea amprentelor, folosind teoria grafurilor pentru determinarea cuplajului maxim. S-a propus utilizarea unui algoritm euristic în acest scop, în locul celor clasici (algoritmul ungar (Kuhn) și algoritmul lui John D.C. Little), reducându-se astfel semnificativ timpul necesar recunoașterii persoanelor prin utilizarea amprentei digitale, prin scăderea complexității algoritmului de potrivire de la $O(n^4)$ la $O(n^2)$.

Capitolul IV – „Cercetări asupra unui sistem integrat pentru accesul la aplicații de internet/mobile banking folosind recunoașterea persoanelor după iris și amprentă” cuprinde studiul autorului asupra unui sistem integrat dezvoltat în mai multe limbaje de programare. Se folosesc inițial aplicații de tip standalone pentru asigurarea accesului la aplicații de internet banking, utilizând spre exemplificare o copie a site-ului de internet banking al Băncii Transilvania. Partea a doua a capitolului conține o aplicație realizată pe o placă de dezvoltare Arduino Mega 2560 și care are drept scop îmbunătățirea accesului la aplicații de internet banking, folosind atât recunoașterea persoanelor după amprenta digitală cât și după iris. Aplicația practică dezvoltată folosește contribuțiile prezentate anterior, în capitolele II și III.

Capitolul V – „Concluzii, contribuții și direcții viitoare de dezvoltare” conține concluziile generale ale tezei, precum și contribuțiile autorului în domeniul tezei de doctorat.

Capitolul se încheie cu prezentarea direcțiilor viitoare de dezvoltare a acestui domeniu foarte atractiv din punct de vedere al cercetării.

Teza de doctorat continuă cu prezentarea *Bibliografiei* care a stat la baza redactării acesteia.

Anexa 1 conține o descriere aprofundată a unor funcții dintr-o librărie a camerei pentru preluarea imaginii irisului.

Anexa 2 conține principalele funcții și algoritmi utilizați în recunoașterea persoanelor după amprenta digitală, subiect prezentat în *Capitolul 3*.

În *Anexa 3* s-a inclus codul sursă Arduino pentru funcționarea sistemului propus în cadrul *Capitolului 4*.

Cuprins

CAPITOLUL I. Stadiul actual al recunoașterii persoanelor după iris și amprentă.....	1
1.2. Funcționarea sistemelor biometrice	2
1.3. Verificarea și identificarea	2
1.4. Performanțele unui sistem biometric	3
1.5. Aplicații ale biometriei	3
1.6. Stadiul actual al cercetărilor referitoare la recunoașterea persoanelor după iris	3
1.6.1. Structura ochiului uman și a irisului	3
1.6.2. Echipamente de achiziție și de prelucrare a imaginilor	4
1.6.2.1. Importanța senzorilor	4
1.6.2.2. Dispozitive utilizate în vederea captării imaginii irisului	4
1.6.3. Studiul cercetărilor referitoare la utilizarea irisului uman în vederea recunoașterii persoanelor	6
1.6.3.1. Primul patent referitor la recunoașterea persoanelor după iris	6
1.6.3.2. Patentul de bază în identificarea matematică a persoanelor după iris	6
1.6.3.3. Lucrarea cercetătorului Richard Wildes referitoare la recunoașterea persoanelor după iris	6
1.6.3.4. Abordări și rezultate în recunoașterea persoanelor după iris, publicate în articole ce au fost studiate în cadrul programului de cercetare doctorală	6
1.7. Stadiul actual al recunoașterii persoanelor după amprenta digitală	6
1.7.1. Senzori utilizați în vederea preluării imaginilor brute ale amprentelor papilare	6
1.7.1.1 Tipuri de senzori utilizați	6
1.7.1.2. Importanța senzorilor pentru toate echipamentele și etapele următoare de achiziție și de prelucrare	7
1.7.2. Articole importante studiate și utilizate în cercetările ulterioare	7
1.8. Concluzii și contribuții	8
CAPITOLUL II. Contribuții privind recunoașterea persoanelor după iris.....	9
2.1. Introducere	9
2.2. Etape în recunoașterea persoanelor după iris	12
2.2.1. Preluarea imaginii de la cameră sau dintr-un fișier	13
2.2.2. Prelucrări grafice asupra imaginilor	14
2.2.3. Segmentarea imaginii	14
2.2.4. Normalizarea imaginii	14
2.2.5. Generarea codului iris	14
2.2.6. Potrivirea imaginilor	15
2.3. Dispozitive și metode pentru achiziția imaginii irisului	15
2.3.1. Dispozitive utilizate în vederea captării imaginii irisului	16
2.3.2. Utilizarea camerei pentru preluarea imaginilor irisului	16
2.3.2.2. Funcții din cadrul unei librării utilizate pentru preluarea imaginii irisului de la cameră	17
2.3.2.3. Librerie dinamică pentru utilizare în Visual Basic	17
2.4. Concluzii și contribuții	17
CAPITOLUL III. Contribuții privind recunoașterea persoanelor după amprenta digitală	19
3.1. Etape în recunoașterea persoanelor după amprenta digitală	19
3.1.2. Prelucrarea histogramei imaginilor (Egalizare histogramă)	20

3.1.3. Transformata Fourier Rapidă.....	20
3.1.4. Binarizarea adaptivă	20
3.1.5. Extragerea regiunii de interes	20
3.1.6. Subțiere	21
3.1.7. Eliminarea porilor și puncte singulare. Eliminarea punților sau “pinteni”	21
3.1.8. Extragerea caracteristicii amprentă.....	22
3.2. Contribuții privind adoptarea unei noi scheme de recunoaștere a persoanelor după amprenta digitală	23
3.2.1. Considerații teoretice	23
3.2.2. Aplicație software pentru obținerea punctelor caracteristice.....	26
3.2.3. Operatori pentru detectarea contururilor și a muchiilor dintr-o imagine a unei amprente.....	26
3.2.3.1. Metode pentru detecția muchiilor bazate pe filtrare urmată de aplicarea operatorilor diferențiali pentru amprentă digitală	26
3.2.3.2. Detecția contururilor din imagini ale amprentelor digitale prin aplicarea unor operatori în vederea detecției contururilor	28
3.3. Contribuții privind algoritmi utilizați pentru faza de potrivire.....	28
3.3.1. Potrivirea amprentelor digitale	28
3.3.2. Contribuții privind utilizarea grafurilor în faza de potrivire.....	29
3.3.2.1. Algoritmi pentru determinarea cuplajului maxim	29
3.3.2.1.1. Algoritmul ungar.....	29
3.3.2.1.2. Algoritmul lui Little.....	30
3.3.2.1.3. Procedeu euristic pentru determinarea cuplajului maxim într-un graf bipartit	30
3.4. Concluzii și contribuții	34
CAPITOLUL IV. Cercetări asupra unor sisteme integrate pentru accesul la aplicații de internet banking folosind recunoașterea persoanelor după iris și amprentă	35
4.1. Introducere.....	35
4.2. Aplicație pentru înregistrarea irisului utilizatorului de internet banking.....	36
4.3. Aplicație practică de acces la aplicația de internet banking	37
4.4. Aplicații practice pentru înregistrarea și recunoașterea persoanelor după amprenta digitală	38
4.4.1. Aplicație standalone pentru înregistrarea persoanelor în vederea asigurării accesului la aplicații de tip internet-banking.....	39
4.4.2. Aplicații și dispozitive pentru Android.....	41
4.5. Modulul Arduino Mega 2560 și senzori pentru înregistrarea utilizatorilor și pentru acordarea accesului la aplicații de internet banking	43
4.6. Concluzii și contribuții	47
CAPITOLUL V. Concluzii finale, contribuții și direcții viitoare de cercetare	49
5.1. Concluzii finale.....	49
5.2. Contribuții.....	50
5.3. Diseminarea rezultatelor	51
5.4. Direcții viitoare de cercetare privind tehnologiile biometrice	52
BIBLIOGRAFIE	53

CAPITOLUL I. Stadiul actual al recunoașterii persoanelor după iris și amprentă

În acest capitol se face o introducere în ceea ce privește recunoașterea persoanelor folosind metode biometrice, dintre care s-a insistat asupra celor două care fac obiectul tezei de doctorat, și anume irisul și amprenta.

Schemele tradiționale de autentificare sunt prezentate în figura 1.1.

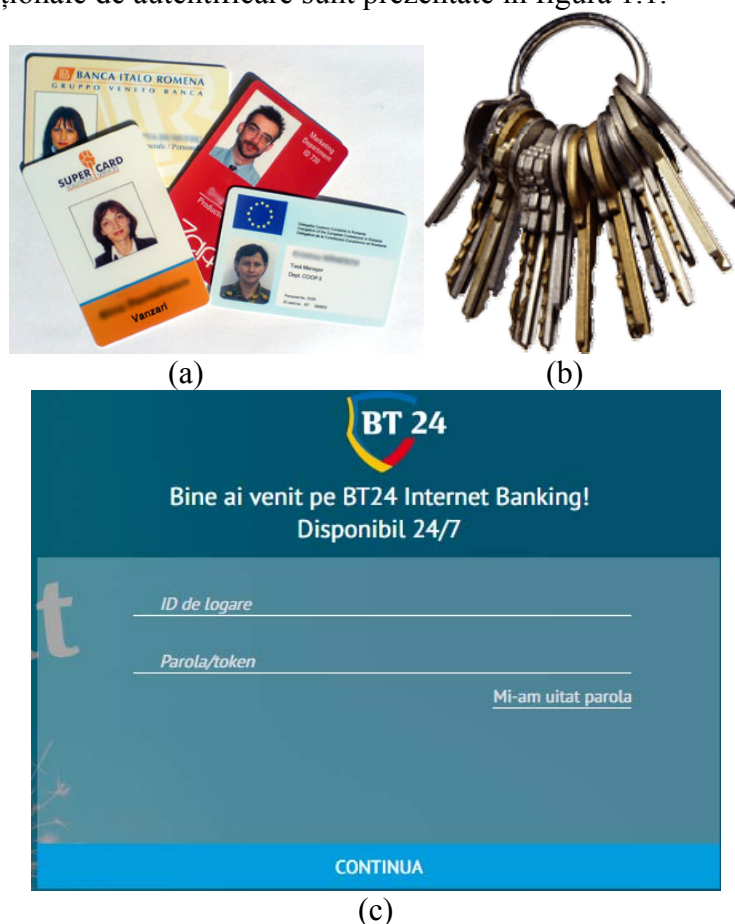


Figura 1.1. Scheme tradiționale de recunoaștere bazate pe (a) cartele de acces, (b) chei și (c) parole

Sistemele biometrice utilizează o mare varietate de caracteristici fizice sau comportamentale (după cum se poate remarca și din figura 1.2), între acestea regăsindu-se amprentele, fața, geometria mâinii sau a degetelor, irisul, retina, semnătura, mersul, amprenta palmară, urechea, structura de vene a mâinilor, mirosul sau ADN-ul. În literatura de specialitate, aceste caracteristici sunt adesea numite *trăsături*, *indicatori*, *identificatori* sau *modalități*. Deși sistemele biometrice au propriile limitări, totuși ele au un mare avantaj în fața metodelor de securitate tradiționale, în sensul că nu pot fi foarte ușor furate sau partajate.

Utilizarea trăsăturilor biologice pentru confirmarea identității unui individ nu reprezintă un concept nou. La sfârșitul secolului al XIX-lea, Alphonse Bertillon, un ofițer de poliție din Franța, a descoperit un sistem de identificare a persoanelor care asociază un set de măsurători antropometrice unui anumit individ.

Apariția procesării digitale a semnalelor a dus la dezvoltarea de sisteme automate în anii '60-'70, care erau capabile să proceseze date despre *amprenta digitală*, *vocea*, *geometria mâinii* și *fizionomia feței*.

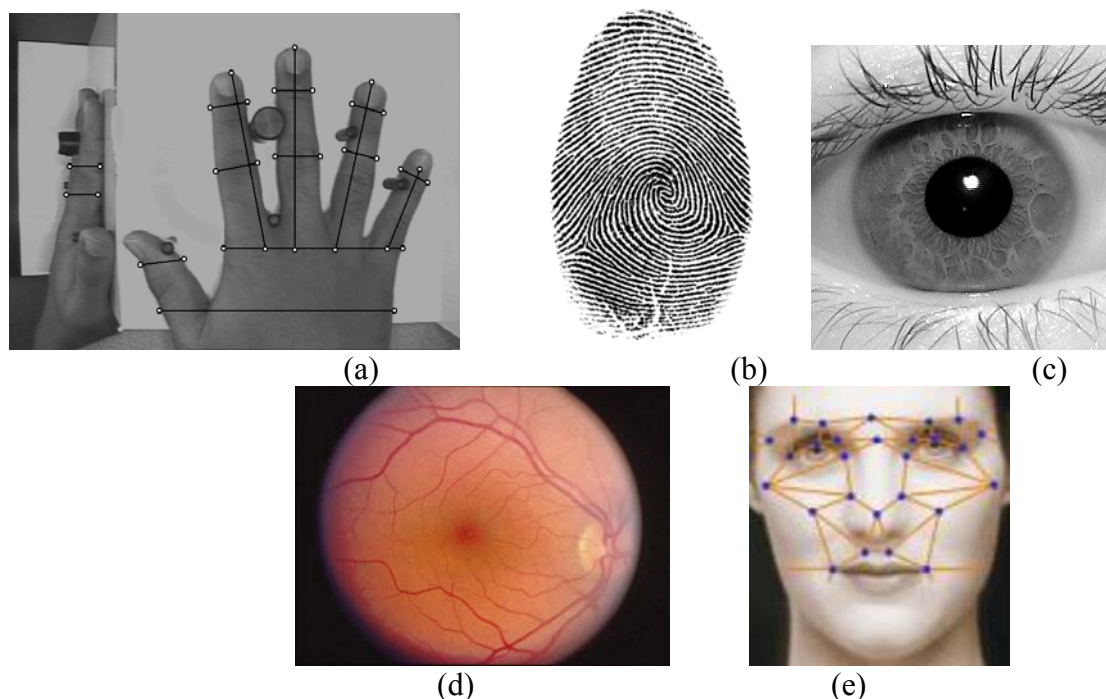


Figura 1.2. Metode de recunoaștere a persoanelor după (a) geometria mâinii, (b) amprentă, (c) iris, (d) retină și (e) fizionomia feței

Dezvoltarea foarte rapidă a sistemelor de calcul și îmbunătățirea performanțelor senzorilor de captare a informației biometrice, împreună cu progresul în domeniul recunoașterii formelor și a sistemelor de captare a imaginilor, au dus la apariția unor scheme sofisticate de procesare și potrivire a datelor biometrice a mai multor caracteristici, printre care irisul, retina, mersul și semnătura. Mai mult chiar, progresul în modelarea 3D conduce la o procesare a datelor biometrice tridimensionale, cum ar fi geometria mâinii, fizionomia feței și urechea.

1.2. Funcționarea sistemelor biometrice

Un sistem biometric reprezintă de fapt un sistem de recunoaștere a formelor care captează date biometrice de la o anumită persoană, extrage un set de caracteristici relevante din aceste date, compară acest set de trăsături cu setul sau seturile din baza de date și execută o acțiune bazată pe rezultatul comparării. De aceea, un sistem biometric general poate fi văzut ca având patru module principale: un modul referitor la senzor; un modul de evaluare a calității și de extragere a caracteristicilor; un modul de potrivire; și un modul al bazei de date. Fiecare dintre aceste module a fost prezentat în acest paragraf, informațiile reprezentând o sinteză a celor prezentate în cadrul lucrării [1], studiate în cadrul programului de cercetare doctorală.

Modulele sunt prezentate în acest paragraf al tezei de doctorat.

1.3. Verificarea și identificarea

Principala diferență este determinată de faptul că în cazul verificării se cunoaște

identitatea utilizatorului, dată printr-un nume de utilizator de exemplu, în acest fel realizându-se o comparație 1:1, între datele biometrice furnizate de către utilizator și cele stocate într-o bază de date. În cazul identificării, nu se cunoaște identitatea utilizatorului sistemului, realizându-se astfel o căutare în baza de date a datelor biometrice furnizate, rezultând astfel o comparație de tipul 1:N, unde N reprezintă numărul de șabloane existente în baza de date.

1.4. Performanțele unui sistem biometric

Variația observată în cadrul seturilor de caracteristici biometrice aparținând aceleiași individ se numește variație *intra-clasă*, iar variația dintre două seturi aparținând la doi indivizi diferiți se numește variație *inter-clasă*. Un set de caracteristici poate fi considerat util dacă se obține o variație intra-clasă foarte mică și o variație inter-clasă foarte mare.

În acest paragraf sunt prezentate principalele noțiuni referitoare la ratele de erori FAR, FRR, FTE.

1.5. Aplicații ale biometriei

Stabilirea identității unei persoane cu o foarte mare certitudine a devenit decisivă într-un foarte mare număr de aplicații din societatea noastră de astăzi, caracterizată prin interconectarea fără precedent. Întrebări de genul „Este acea persoană chiar cine pretinde că este?”, „Este această persoană autorizată să folosească acest dispozitiv sau această facilitate?”, sunt puse din ce în ce mai des în diferite scenarii, cum ar fi la emiterea unui permis de conducere în Statele Unite ale Americii sau la trecerea frontierei de stat. Nevoia unor tehnici foarte solide de autentificare a utilizatorilor este din ce în ce mai mare, având în vedere dezvoltările importante în domeniul rețelelor de calculatoare, a comunicațiilor și a mobilității. Astfel, tehnologiile biometrice sunt din ce în ce mai mult încorporate în multe aplicații. Aceste aplicații pot fi împărțite în trei mari grupuri:

1. **Aplicații comerciale**, cum ar fi autentificarea într-o rețea, securitatea datelor electronice, comerț electronic, accesul la Internet, folosirea unui ATM sau a unui card bancar, controlul accesului, utilizarea telefoanelor mobile, PDA-urilor, managementul înregistrărilor medicale, învățarea la distanță, etc;
2. **Aplicații guvernamentale**, cum ar fi emiterea unei cărți de identitate, managementul persoanelor din cadrul unei închisori, emiterea permisului de conducere, controlul la trecerea frontierei de stat, etc;
3. **Aplicații în criminalistică**, cum ar fi identificarea cadavrelor, investigațiile criminale, determinarea părinților pe baza ADN-ului, etc.

În continuarea paragrafului sunt prezentate câteva exemple de aplicații în care se folosește biometria pentru autentificare persoanelor.

1.6. Stadiul actual al cercetărilor referitoare la recunoașterea persoanelor după iris

În acest paragraf vor fi prezentate structura ochiului uman și a irisului, precum și echipamente utilizate în preluarea imaginilor irisului. Partea a doua a acestui paragraf este cea mai importantă, fiind prezentat un studiu asupra câtorva lucrări semnificative pentru recunoașterea persoanelor după iris.

1.6.1. Structura ochiului uman și a irisului

Irisul ochiului uman este o structură complexă care cuprinde mușchi, țesut conjunctiv,

vase capilare și cromatofore. La exterior prezintă o structură vizibilă cu variații radiale și unghiulare rezultând din brazde de contracție, fibre din collagen, filamente, vascularizație în serpentină, inele și pete de roșeață; luate împreună, acestea constituie o „amprentă digitală” distinctivă (individuală, personalizată). Imaginea optică mărită a unui iris uman, constituie de asemenea o semnătură biometrică plauzibilă pentru stabilirea sau confirmarea identității personale. Alte proprietăți ale irisului care se pretează acestui scop, și sunt mult superioare amprentelor digitale pentru sistemele automate de identificare, includ:

- imposibilitatea de a modifica prin intervenții chirurgicale structura sa, fără riscuri inacceptabile;
- protecția și izolarea sa inerentă de mediul fizic;
- răspunsul său fiziologic la lumină, care este ușor de monitorizat.

1.6.2. Echipamente de achiziție și de prelucrare a imaginilor

1.6.2.1. Importanța senzorilor

Recunoașterea persoanelor după iris se bazează pe analiza imaginii preluate de la un senzor. Se pot identifica avantajele majore pe care le au senzorii în prelucrarea și analiza irisului și anume:

- Imaginea preluată de către senzori poate fi prelucrată pe calculator. Există echipamente de preluare a imaginilor care conțin software specializat și metode de procesare a irisului, dintre care se pot aminti: modificarea contrastului, inversare a tonurilor de gri, colorarea artificială, realizarea de măsurători, etc.
- Calitatea imaginii: îmbunătățirea unei imagini într-un anumit sens predefinit; reconstituirea sau refacerea unei imagini degradate, prin utilizarea unor informații despre fenomenul de degradare; principalele surse de zgomot sunt: achiziția și transmisia imaginilor (camera CCD: zgomot influențat de nivelurile de iluminare și temperatura senzorului; transmisia imaginilor: interferențele din canalele de transmisie);
- Economia de timp reprezintă un alt avantaj esențial, mai ales în cazul sistemelor CCD (Change-Coupled Device) care permit afișarea imaginii imediat după expunere;
- Ecologic (neinvaziv pentru mediu sau individul supus procesului de recunoaștere).

1.6.2.2. Dispozitive utilizate în vederea captării imaginii irisului

Imaginea irisului poate fi captată de un aparat de fotografiat standard folosind deopotrivă lumina naturală și infraroșie și poate fi o procedură manuală sau una automată.

Aparatul de fotografiat poate fi poziționat la o distanță cuprinsă între 9 cm și un metru pentru a capta imaginea.

În procedura manuală, utilizatorul trebuie să ajusteze aparatul de fotografiat pentru a încadra irisul și trebuie să fie la o distanță între 15 cm până la 30 cm de aparatul de fotografiat. Acest proces este mult mai greu când se realizează manual și necesită o pregătire specială a utilizatorului pentru a avea succes.

Procedura automată folosește un set de aparate de fotografiat ce localizează automat fața și irisul. Îndată ce aparatul de fotografiat a localizat ochiul, sistemul de recunoaștere al irisului identifică apoi imaginea care ilustrează cel mai bine centrarea și claritatea irisului.

În aplicațiile realizate în această teză de doctorat, s-a folosit camera Panasonic BM-ET100US, care este prezentată în figura 1.3. Camera este formată din două obiective, cel de sus fiind folosit exclusiv pentru recunoașterea după iris, iar cel de jos poate fi folosit ca și webcam. Această cameră prezintă avantajul că se poate folosi, de asemenea, și pentru

recunoașterea facială a persoanei, prin folosirea webcam-ului. Astfel, această cameră este ideală pentru o recunoaștere multimodală a persoanei, după iris și după fizionomia feței.

Sub obiectivul webcam-ului se află o sursă de lumină în spectrul infraroșu apropiat, care se activează atunci când se citește imaginea irisului. Imaginea luată în infraroșu redă mult mai fidel detaliile necesare recunoașterii, deoarece culoarea irisului nu este importantă pentru recunoaștere. De asemenea, în cazul irișilor puternic colorați (spre negru), captarea imaginii folosind lumina naturală ar putea duce la reducerea semnificativă a calității detaliilor necesare unei recunoașteri cât mai exacte a imaginii irisului. De asemenea, trimiterea unui fascicul de lumină naturală sau – mai ales – artificială către iris poate duce la apariția de puncte albe de mari dimensiuni pe pupilă sau chiar pe iris, în acest fel reducându-se șansele unei recunoașteri corecte.

Pe lângă cameră, în pachet se mai găsește software-ul „PrivateID”, folosit pentru preluarea și recunoașterea imaginilor irisului.

De asemenea, în cadrul cercetărilor din cadrul tezei de doctorat s-a folosit camera UBKEY MirrorKem, care are avantajul că este de o generație mai nouă și are dimensiuni mult mai mici în comparație cu camera de mai sus. Camera poate fi integrată foarte simplu în diverse medii de programare, folosind SDK-ul oferit de producător. În figura 1.4 sunt prezentate trei imagini ale acestei camere. În partea de sus utilizatorul își poate vizualiza ochiul, iar partea de jos a camerei este reprezentat de LED-urile infraroșu utilizate în preluarea imaginii irisului.



Figura 1.3. Camera cu obiectiv pentru recunoaștere după iris (sus) și webcam (jos) Panasonic BM-ET100US

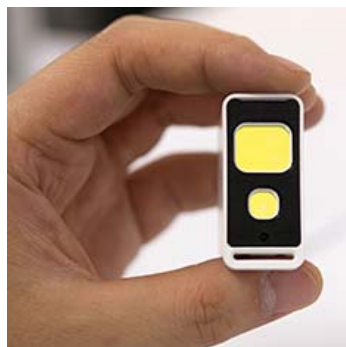


Figura 1.4. Camera UBKEY MirrorKem

1.6.3. Studiul cercetărilor referitoare la utilizarea irisului uman în vederea recunoașterii persoanelor

1.6.3.1. Primul patent referitor la recunoașterea persoanelor după iris

În anul 1987 s-a realizat de către cercetătorii Leonard Flom și Aran Safir patentul numărul 4.641.349 ([13]). Invenția are ca scop identificarea caracteristicilor ochiului uman pentru a recunoaște o persoană după caracteristicile irisului. Invenția are la bază „recunoașterea irisului”. În acest caz este mult mai ușor de a identifica caracteristicile ochiului decât prin scanarea retinei deoarece irisul și pupila sunt mult mai ușor de citit. Patentul este prezentat în detaliu în cadrul tezei.

1.6.3.2. Patentul de bază în identificarea matematică a persoanelor după iris

În anul 1994 a fost patentată lucrarea “*Biometric personal identification system based on iris analysis*” [14], realizată de către John Daugman, considerat părintele recunoașterii persoanelor după iris. Patentul are numărul 5291560, și a fost emis în data de 1 mai 1994. Principalele contribuții ale acestui patent sunt:

- Localizarea irisului este rezolvată folosind modelarea activă a conturilor;
- În privința reprezentării, Daugman propune aplicarea filtrelor Gabor.

Lucrarea reprezintă un punct important de pornire în recunoașterea persoanelor după iris și poate fi consultată în detaliu în pagina web aferentă patentului.

1.6.3.3. Lucrarea cercetătorului Richard Wildes referitoare la recunoașterea persoanelor după iris

Lucrarea *Iris Recognition: An Emerging Biometric Technology*, apare în anul 1997 și îl are ca autor pe Richard P. Wildes [16].

Principalele contribuții ale acestui articol sunt:

- Localizarea irisului este rezolvată folosind transformata Hough;
- În privința reprezentării, Wildes face uz de o aplicație a filtrelor gaussiene.

Principalele obiective ale acestui articol sunt legate de localizarea irisului utilizând transformata Hough, iar în privința reprezentării codului iris, Wildes face uz de o aplicație a filtrelor gaussiene.

1.6.3.4. Abordări și rezultate în recunoașterea persoanelor după iris, publicate în articole ce au fost studiate în cadrul programului de cercetare doctorală

În acest paragraf se prezintă un număr de 10 articole studiate în timpul cercetărilor efectuate în cadrul elaborării tezei.

1.7. Stadiul actual al recunoașterii persoanelor după amprenta digitală

În acest paragraf se prezintă principalii senzori utilizați în recunoașterea persoanelor după amprenta digitală, precum și articolele importante studiate în acest domeniu.

1.7.1. Senzori utilizați în vederea preluării imaginilor brute ale amprentelor papilare

1.7.1.1 Tipuri de senzori utilizați

Pentru preluarea amprentelor digitale ale unei persoane s-au dezvoltat mai multe tipuri

de senzori. Sensorii sunt de cele mai multe ori încorporați în diverse dispozitive periferice, cum ar fi tastatura sau mouse-ul. În figura 1.5 sunt prezentați mai multe tipuri de senzori.

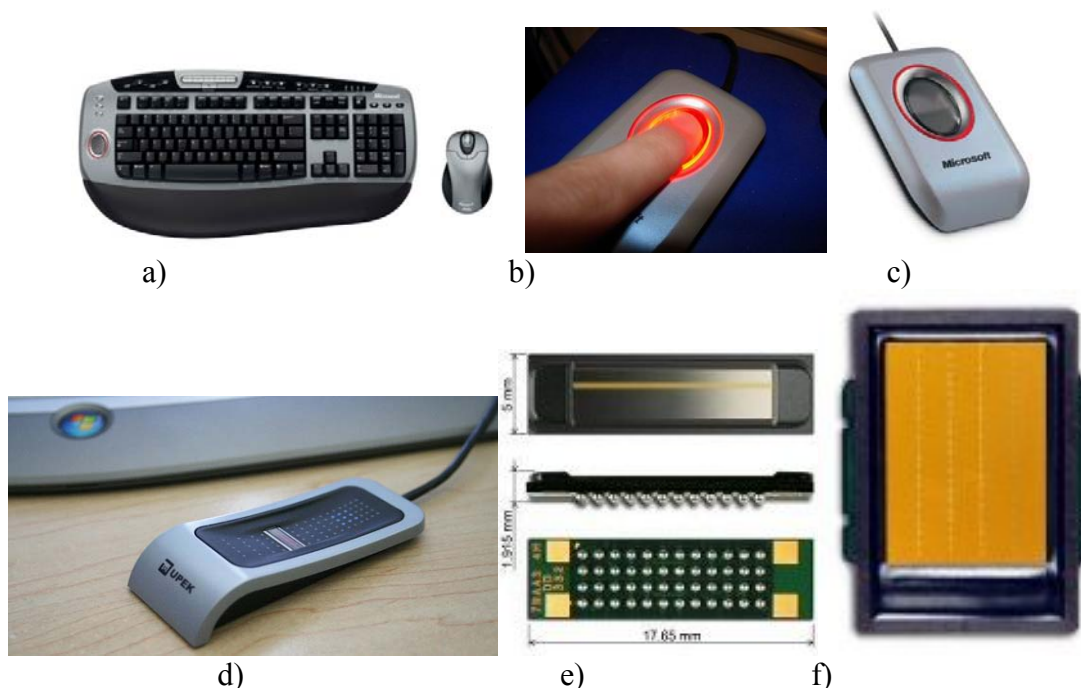


Figura 1.5. *Senzori pentru preluarea amprente digitale. a)-c) dispozitive Microsoft; d) senzor Upek; e) senzor de tip sweep; f) senzor capacitiv. Sursa: Internet*

În continuare se prezintă principalele tipuri de senzori: optici (FTIR, fibre optice, opto-electronici), siliconici sau care folosesc ultrasunete.

1.7.1.2. Importanța senzorilor pentru toate echipamentele și etapele următoare de achiziție și de prelucrare

Se pot identifica relativ ușor avantajele majore pe care le au senzorii în prelucrarea și analiza amprentelor digitale și anume:

- Imaginea preluată de către senzori poate fi prelucrată pe calculator. Există echipamente de preluare a imaginilor care conțin software specializat și metode de procesare a amprentelor digitale, dintre care putem aminti: modificarea contrastului, inversare a tonurilor de gri, colorarea artificială, realizarea de măsurători, etc.
- Calitatea imaginii: îmbunătățirea unei imagini într-un anumit sens predefinit; reconstituirea sau refacerea unei imagini degradate, prin utilizarea unor informații despre fenomenul de degradare; principalele surse de zgomot sunt: achiziția și transmisia imaginilor (camera CCD: zgomot influențat de nivelurile de iluminare și temperatura senzorului; transmisia imaginilor: interferențele din canalele de transmisie);
- Grad înalt de siguranță a sistemelor bazate pe senzori cu ultrasunete.
- Economia de timp reprezintă un alt avantaj esențial, mai ales în cazul sistemelor CCD (Change-Coupled Device) care permit afișarea imaginii imediat după expunere;
- Ecologic (neinvaziv pentru mediu). Utilizarea senzorilor optici, capacitivi sau cu ultrasunete nu necesită substanțe chimice cum erau folosite la dezvoltarea filmelor.

1.7.2. Articole importante studiate și utilizate în cercetările ulterioare

În acest paragraf au fost prezentate cronologic lucrările reprezentative din domeniul

recunoașterii amprentelor digitale. În același timp se va face o comparație a acestor lucrări, cu evidențierea îmbunătățirilor aduse pe parcursul evoluției acestei metode de identificare sau verificare a persoanelor.

În cadrul cercetărilor din cadrul tezei de doctorat, s-au studiat mai multe articole importante în domeniul recunoașterii persoanelor după amprenta digitală, dintre care două sunt reprezentative și au fost utilizate în vederea obținerii de noi rezultate:

- a) *“Adaptive flow orientation based feature extraction in fingerprint images”* ([33]), autori Nalini K. Ratha, Shaoyun Chen, Anil K. Jain, apărut în anul 1995;
- b) *„Fingerprint minutiae extraction from skeletonized binary images”* ([34]), autori Alessandro Farina, Zsolt M.Kovacs-Vajna, Alberto Leone, apărut în anul 1998.

De asemenea, s-au studiat alte articole, dintre care cele mai importante sunt prezentate în continuare.

Ca urmare a articolelor studiate, s-au publicat mai multe articole referitoare la recunoașterea persoanelor după amprenta digitală, printre care cele mai importante sunt [60], [61], [62] și [63].

1.8. Concluzii și contribuții

În acest capitol s-a realizat o introducere în domeniul recunoașterii persoanelor prin utilizarea tehnologiilor biometrice. La începutul capitolului s-a analizat funcționarea sistemelor biometrice, prin prezentarea modulelor componente ale acestora. În continuare s-a insistat pe diferențele între verificare și identificare, precum și pe performanțele sistemelor biometrice. Aplicațiile biometriei sunt foarte diverse și o parte dintre ele se regăsesc în cadrul acestui capitol.

Referitor la stadiul actual al recunoașterii persoanelor după iris, s-au studiat mai multe articole iar principalele contribuții ale acestora au fost redate în paragraful 1.6. De asemenea, au fost introduse informații despre structura ochiului uman și a irisului, precum și date despre senzorii utilizați în preluarea imaginilor. Partea a doua a acestui paragraf realizează o introducere în recunoașterea persoanelor după iris, plecând de la lucrarea de bază a cercetătorului britanic de la Universitatea din Cambridge, John Daugman, continuând cu o altă abordare a lui Richard Wildes și terminând cu o serie de articole foarte recente, care abordează diverse problematice referitoare la această modalitate de recunoaștere a persoanelor prin utilizarea irisului.

În ultima parte a capitolului se realizează o introducere în recunoașterea persoanelor după amprenta digitală. Acest subiect a fost studiat de foarte mult timp și de mulți cercetători. La fel ca și în cazul recunoașterii după iris, sunt prezentați principalii senzori utilizați în preluarea imaginilor amprentelor. În continuare se realizează o analiză asupra articolelor de referință din acest domeniu foarte vast al recunoașterii persoanelor după amprenta digitală.

Unele dintre articolele din acest capitol vor fi utilizate în dezvoltarea ulterioară a unor aplicații care vor fi prezentate în cadrul tezei de doctorat. De asemenea, acestea constituie un punct de plecare în abordarea domeniului foarte vast al recunoașterii persoanelor după iris și amprentă.

În primul capitol s-a elaborat un studiu aprofundat asupra articolelor importante în domeniul recunoașterii persoanelor după iris și amprentă, aceasta fiind **principala contribuție teoretică** rezultată.

CAPITOLUL II. Contribuții privind recunoașterea persoanelor după iris

2.1. Introducere

Irisul este considerat a fi unul dintre cele mai sigure caracteristici biometrice care poate fi utilizat în recunoașterea persoanelor. Începuturile utilizării irisului sunt destul de recente, începând cu un prim patent în acest domeniu, emis de către cercetătorii oftalmologi Leonard Flom și Aran Safir, care în anul 1987 au patentat un „Sistem de recunoaștere a irisului”, cu numărul de brevet US 4.641.349. Totuși, această invenție nu avea un fundament matematic, ideea fiind preluată de dr. John Daugman de la Universitatea din Cambridge. Acesta a reușit să folosească un operator integro-diferențial pentru determinarea conturilor exterioare și interioare ale irisului. De asemenea a propus utilizarea distanței Hamming pentru a determina autenticitatea unui iris în procesul de recunoaștere, după transformarea acestuia din coordonatele carteziane în coordonate polare și obținerea codului irisului respectiv. Prof. Daugman a patentat aceste descoperiri, fiindu-i emis patentul cu numărul US 5,291,560. Totuși, acest profesor, în prefața la cartea „Handbook of Iris Recognition” [62], face referire și la o altă lucrare mult mai veche a lui Alphonse Bertillon, apărută în anul 1892, și care se numește „Tableau des nuances de l’iris humain”. Preocupările autorului acestei lucrări includ mai multe modalități de identificare a criminalilor, el fiind cel care a propus un prim sistem de înregistrare a acestora prin metoda de măsurare a mai multor dimensiuni ale corpului uman (denumită „metoda antropometrică”).

Irisul reprezintă partea colorată a ochiului, care este un organ interior vizibil la exterior. Irisul se creează în timpul gestației și structura sa rămâne practic neschimbată pe tot parcursul vieții (cu excepția unor intervenții accidentale sau intenționate asupra sa). De la centru spre exterior, ochiul uman este compus din: pupilă, iris iar în exteriorul acestuia se află sclerotică, sau „albul ochiului”. În figura 2.1 se prezintă ochiul stâng al autorului, cu explicarea părților componente.

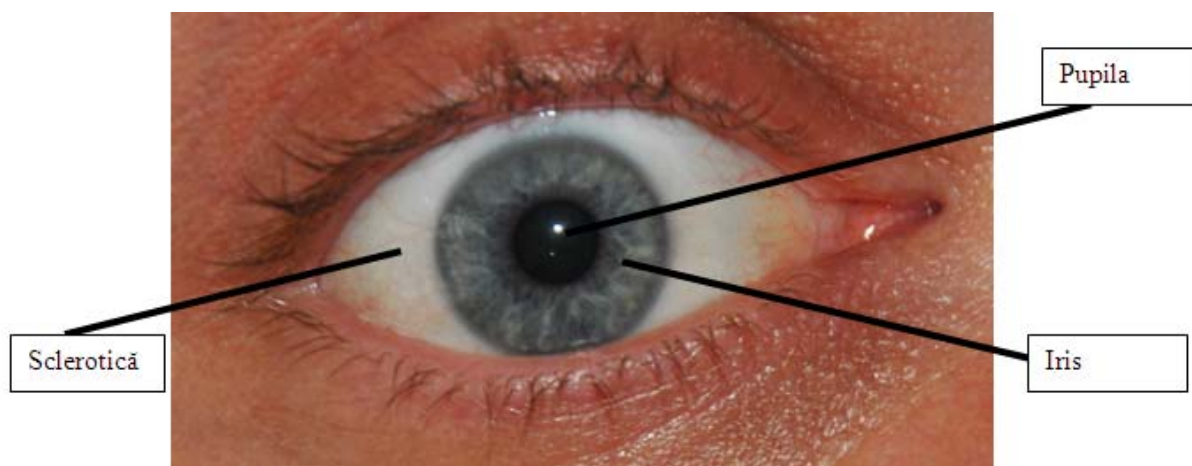


Figura 2.1. Componentele ochiului uman (fotografie proprie)

Se observă faptul că nu se poate captura doar imaginea irisului, ci se preia imaginea ochiului și a zonelor din jurul său (pleoape și gene), acestea putând să se suprapună peste zona de interes. De aceea unul dintre scopuri este extragerea unei cantități maxime de informație referitoare la iris.

Principiul care a stat la baza extragerii cu acuratețe a irisului se bazează pe variația de

culoare dintre pupilă și iris (pupila este neagră la un om sănătos) și dintre iris și sclerotică (care teoretic este mult mai deschisă la culoare decât irisul). Totuși, anumite boli pot influența aceste presupuneri inițiale:

- cataracta duce la opacifierea cristalinului, pupila devenind albicioasă; este mai dificil de determinat frontiera dintre iris și pupilă, mai ales la persoanele care au culoarea irisului foarte puțin pigmentat;
- conjunctivita colorează sclerotică în roșu, în acest fel fiind mai dificil de determinat frontiera exterioară a irisului;

În cazul formelor normale ale irișilor, în literatura de specialitate au fost propuse mai multe metode de extragere a caracteristicilor irisului, dintre cele mai importante sunt:

1. **Metoda lui John Daugman** – se bazează pe un operator integro-diferențial aplicat asupra intensităților imaginii; în figura 2.2 se prezintă o imagine emblematică referitoare la această metodă, preluată de pe site-ul profesorului Daugman (http://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html). Metoda este considerată ca fiind cea mai performantă dezvoltată până în momentul de față. În partea din stânga sus a imaginii este codul irisului obținut prin metoda sa, iar în imaginea principală se poate observa ochiul preluat de la o cameră, la care s-au determinat frontierele dinspre pupilă și sclerotică, precum și frontierele cu pleoapele de sus și jos. Informația utilă folosită în generarea IrisCode-ului din partea din stânga sus se află în interiorul celor 4 frontiere descrise mai sus. Aceste metode de determinare a frontierelor sunt prezentate și în patentul său, cu specificația că acesta a fost publicat fără revizuirea prealabilă a autorului, în acest fel conținând anumite greșeli de redactare, în special a formulelor din acesta.

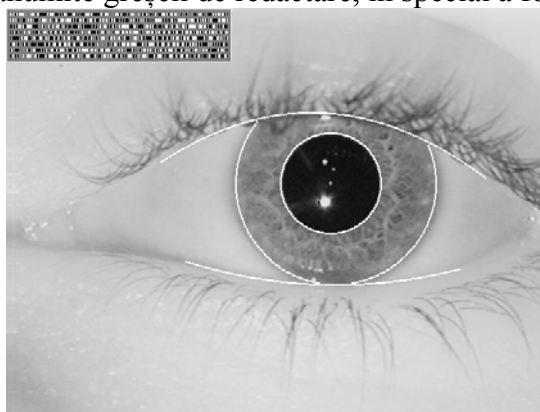


Figura 2.2. *Imaginea segmentată a irisului împreună cu IrisCode™-ul ([15])*

2. **Metoda lui Wildes** – se bazează pe articolul „Iris recognition: an emerging biometric technology” publicat în anul 1997 de către Richard P. Wildes. Metoda sa diferă de cea a lui John Daugman prin modul de căutare. A fost mai puțin studiată și aplicată în practică. În figura 2.3 este prezentată o imagine cu irisul localizat, din această lucrare.

O implementare practică o reprezintă lucrarea publicată de Libor Masek, redactată în anul 2003. Aceasta conține inclusiv un cod în MatLab, care va fi prezentat în acest capitol. Codul nu este criptat și este disponibil online fără taxă. Acesta a fost preluat inclusiv de Institutul Național pentru Standarde și Tehnologii (NIST), o instituție guvernamentală prestigioasă din Statele Unite ale Americii, fiind translatat din MatLab în C++, în cadrul aplicației VASIR – Video-based Automatic System for Iris Recognition (versiunea 2.2 beta a apărut în decembrie 2013). Altă implementare practică este reprezentată de aplicația „Iris Recognition System” de la firma Advanced Source Code (dezvoltată de Luigi Rosa). Autorul pune la dispoziție un demo într-o formă criptată, codul fiind de asemenea scris în MatLab. Și

această aplicație se bazează pe metoda lui Libor Masek, cu specificația că timpul de execuție a fost îmbunătățit cu 94% (adică de aproximativ 16 ori).

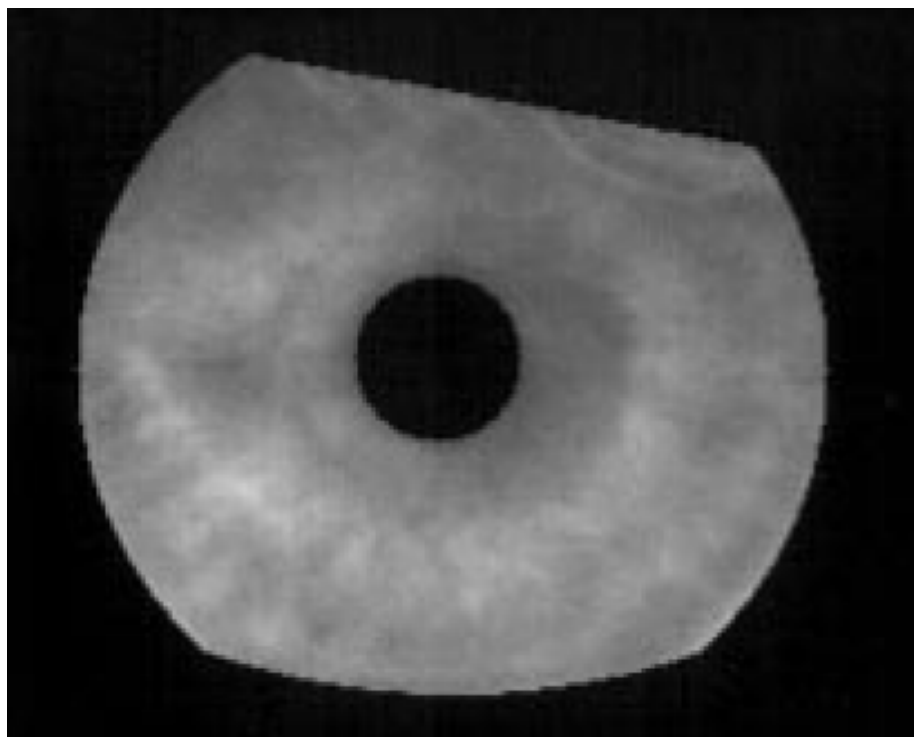


Figura 2.3. Localizarea irisului după metoda lui Wildes ([16])

În cadrul recunoașterii persoanelor după iris există mai multe provocări, printre care prelucrarea imaginilor obținute în condiții dificile sau în timp real, precum și a irișilor care sunt „protejați” de lentile de contact. Astfel imaginile capturate nu vor avea de obicei o calitate ridicată și vor fi necesari pași suplimentari în prelucrarea acestora. O altă provocare – valabilă de fapt pentru toate sistemele biometrice existente – o reprezintă determinarea autenticității irisului prezentat pentru prelucrare. Astfel, se va încerca eliminarea falsurilor (reprezentate de fotografii, unele foarte bine realizate, chiar în tehnologie de imprimare 3D) prin diverse teste, unele care vor necesita participarea efectivă a utilizatorului (de exemplu mișcarea ochiului într-o parte și în alta, în sus și în jos) sau nu (irisul uman are proprietatea de „hippus”, care înseamnă că se contractă sau se dilată de 1-2 ori pe secundă chiar și în condiții de iluminare constantă, iar un dispozitiv performant poate sesiza acest lucru). O altă provocare este reprezentată de faptul că trebuie preluată o imagine clară a unui obiect foarte mic (irisul are în cazul dilatării minime a pupilei o dimensiune de sub 2 cm) de la o distanță relativ mare și în condiții de mișcare, ceea ce duce la necesitatea utilizării unor dispozitive performante.

În subcapitolele următoare se vor prezenta câteva metode de preluare a imaginilor irisului în vederea extragerii unui șablon pentru stocarea acestuia într-o bază de date ce va fi utilizată în procesul de identificare sau verificare, precum și descrierea câtorva biblioteci necesare pentru acest lucru.

În figura 2.4 este prezentată o imagine a standului experimental realizat în vederea înregistrării sau recunoașterii unui utilizator. Acesta este un sistem multimodal, compus dintr-un mouse cu senzor de recunoaștere pentru amprentă și o cameră Panasonic BM-ET100US, prezentată în acest capitol.

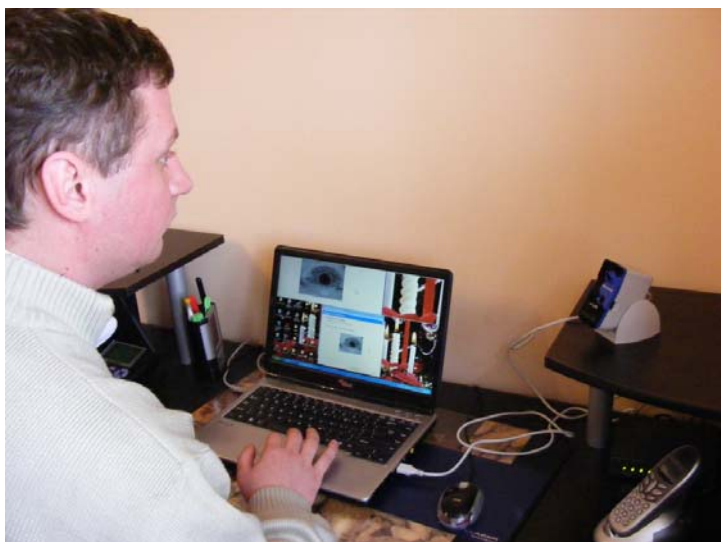


Figura 2.4. *Stand experimental. Preluare imagine ochi cu ajutorul unui senzor CCD de scanare a irisului și afișarea capturii pe ecran*

2.2. Etape în recunoașterea persoanelor după iris

În cazul unui sistem de recunoaștere a persoanelor după iris, se urmează pașii de mai jos, în ordinea în care sunt prezentați:

- **preluarea imaginii de la camera** pentru recunoașterea după iris, de exemplu Panasonic BM-ET100US sau UBKEY MirrorKem, sau încărcarea acesteia dintr-un fișier (de exemplu din baze de date cu iriși, cum ar fi CASIA (Chinese Academy of Sciences - Institute of Automation), MMU, UBIRIS, etc.);
- **prelucrări grafice**, care au ca scop îmbunătățirea imaginii preluate de la cameră sau din fișier; se realizează prin aplicarea a diverse filtre, prin egalizarea de histogramă sau prin alte metode de prelucrare a imaginilor;
- **segmentarea imaginii** – după obținerea unei imagini prelucrate cu un maxim de informații utile, aceasta va fi segmentată, în vederea obținerii centrului și a razei pupilei și a irisului;
- **normalizarea imaginii** – după segmentare, normalizarea regiunii irisului presupune încadrarea regiunii circulare într-un dreptunghi de dimensiune constantă pentru a putea fi comparat cu alte șabloane existente în baza de date sau într-o rețea neuronală;
- **codificare** – extragerea codului irisului în vederea înregistrării într-o bază de date sau pentru recunoaștere;
- **introducerea datelor într-o bază de date**;
- **potrivire** – în cazul identificării sau a verificării se va încerca să se determine dacă imaginea prezentată corespunde vreuneia din baza de date, pe baza unor comparații 1:1 (în cazul verificării, când se furnizează informații suplimentare despre utilizator – întrebarea poate fi pusă astfel: *Imaginea X prezentată corespunde utilizatorului Y ?*) sau 1:N (în cazul identificării, când se interoghează toată baza de date în vederea obținerii de date despre utilizatorul aferent imaginii prezentate – întrebarea se pune *Cine este utilizatorul care a prezentat imaginea irisului X ?*). În cazul înregistrării acest modul de potrivire poate lipsi; totuși, se poate face o verificare de tipul 1:N în baza de date pentru a se identifica dacă utilizatorul este deja înregistrat, eliminând astfel posibilitatea ca un singur utilizator să folosească credențiale diferite pentru autentificare.

În paragrafele următoare sunt prezentați detaliat acești pași. Se vor prezenta realizări ale cercetărilor proprii întreprinse, care s-au bazat într-o oarecare măsură pe îmbunătățirea metodei prezentate de Libor Masek.

2.2.1. Preluarea imaginii de la cameră sau dintr-un fișier

Pentru preluarea imaginii se poate folosi o aplicație de tip ActiveX integrată într-un script JavaScript în cadrul browserului Internet Explorer, explicată în partea a doua a capitolului și în Anexa 1. De asemenea, funcțiile ce vor fi prezentate în acest capitol pot fi folosite pentru capturarea imaginii ochiului și a irisului într-o aplicație standalone sau de tip librărie DLL, în vederea reutilizării acestuia în alte aplicații, după cum se va vedea în Capitolul IV.

În ceea ce privește preluarea imaginii dintr-un fișier stocat pe un hard disk local sau de rețea, aceasta poate fi realizată foarte simplu, orice mediu de programare permițând încărcarea celor mai diverse tipuri de fișiere (JPEG, BMP, PNG, TIF, etc.).

În capitolul IV se vor prezenta două aplicații complete care preiau imagini direct de la camera Panasonic BM-ET100US sau de la UBKEY MirrorKem, una pentru înregistrarea utilizatorilor și cealaltă pentru autentificarea la o aplicație de tip internet banking.

În figura 2.5 sunt prezentate 4 imagini din baza de date CASIA v1.0 (001_1_1.BMP, 001_1_2.BMP (imagini ale aceluiași iris), 019_1_1.BMP și 019_1_2.BMP (de asemenea, imagini ale aceluiași iris)), care vor fi folosite în pașii care vor urma. S-a preferat utilizarea unor imagini din această bază de date din cauza calității superioare celor preluate de la camera Panasonic. Totuși, în anumite articole se specifică faptul că marginile exterioare ale pupilei au fost înnegrite intenționat, pentru ca trecerea de culoare de la pupilă la iris să fie maximă.

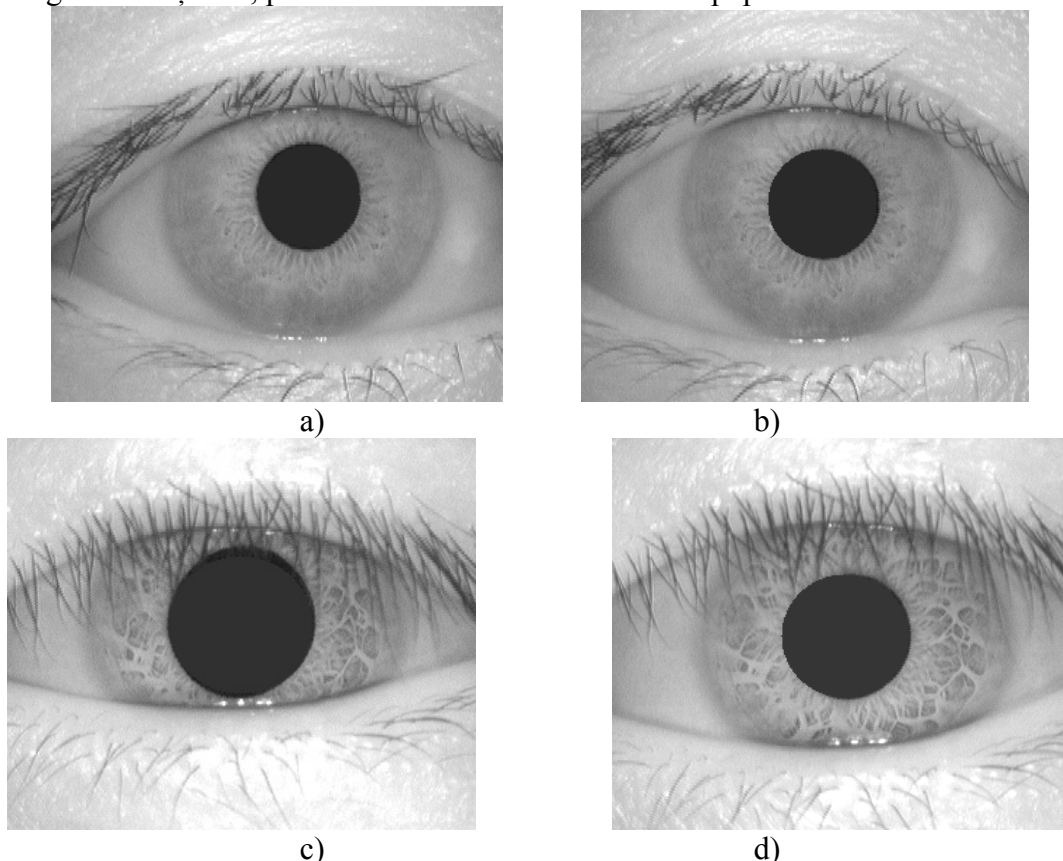


Figura 2.5. Imagini din baza de date CASIA utilizați în prelucrările următoare

2.2.2. Prelucrări grafice asupra imaginilor

În cadrul acestui paragraf se prezintă două metode clasice de îmbunătățire a calității imaginii obținute, și anume egalizarea de histogramă și filtrarea mediană. Scopul este prelucrarea imaginii în vederea obținerii uneia care are o cantitate maximă de informație ce urmează a fi extrasă în următorii pași.

2.2.3. Segmentarea imaginii

Scopul segmentării imaginii îl reprezintă extragerea caracteristicilor irisului și ale pupilei, cum ar fi centrul și raza unui cerc care le aproximează pe acestea. De asemenea izolează și regiunile cu zgomote din zona exterioară a irisului provocate de gene și pleoape. Regiunea irisului este aproximată de 2 cercuri, unul fiind granița dintre iris și sclerotică și cel de-al doilea, interior primului, reprezintă granița dintre iris și pupilă.

Principalele etape care trebuie realizate pentru a se ajunge la un iris segmentat sunt:

- I. Căutarea coordonatelor cercului care înfășoară irisul (linie, coloană, rază);
- II. Căutarea coordonatelor cercului care înfășoară pupila (linie, coloană, rază);
- III. Determinarea regiunii de deasupra pupilei (care are distanță minimă față de pupilă) care încadrează cel mai bine irisul (în regiune se găsesc și zgomote provocate de gene și pleoape);
- IV. Determinarea regiunii de sub pupilă (care are distanță minimă față de pupilă) care încadrează cel mai bine irisul (în regiune se găsesc și zgomote provocate de gene și pleoape).

Aceste faze sunt descrise în paragrafele următoare.

2.2.4. Normalizarea imaginii

Normalizarea regiunii irisului presupune încadrarea regiunii circulare într-un dreptunghi de dimensiune constantă pentru a putea fi comparat cu alte șabloane existente în baza de date sau într-o rețea neuronală. Toate punctele de pe raza radială sunt trecute în coordonate polare utilizând metoda Daugman Rubber Sheet [15]. Este determinată și zona (în coordonate polare) cu zgomote datorată prezenței pleoapelor și genelor în imaginea inițială.

2.2.5. Generarea codului iris

În acest pas se generează șablonul (template) codul iris pentru o imagine ochi (obținută după normalizare) și masca de zgomot corespunzătoare.

Pentru faza de generare cod sunt necesare următoarele operații:

- Convoluția regiunii normalizate cu un filtru Gabor 2-D;
- Creează șablonul iris;
- Calculul fazei. Calculul amplitudinii fazei (dacă amplitudinea este aproape zero, atunci faza semnalului nu mai are importanță și astfel această informație inutilă este marcată în masca de zgomot)

Scopul codificării este generarea unui șablon biometric după normalizarea regiunii irisului și de asemenea generează masca cu zgomote.

Wavelet-urile (formele de undă) sunt folosite pentru a descompune datele din regiunea irisului în componente care apar la rezoluții diferite. Au avantajul față de transformata Fourier prin faptul că datele de frecvență sunt localizate permițând potrivirea caracteristicilor ce apar la aceeași poziție și rezoluție. Un număr de filtre Wavelet este aplicat regiunii bidimensionale

a irisului. Rezultatul obținut în urma aplicării wavelet-urilor este apoi codat pentru a furniza o reprezentare compactă și distinctivă a modelului de iris.

Scopul utilizării filtrelor Gabor: Filtrele Gabor sunt capabile să furnizeze reprezentări optime ale semnalului în spațiu și frecvență. Un filtru Gabor este construit prin modularea unei unde sinusoidale / cosinusoidale cu o gaussiană. Astfel se poate furniza o localizare optimă atât în spațiu cât și în frecvență, de vreme ce unda sinusoidală este perfect localizată în frecvență, dar nu este localizată în spațiu. Componenta pară simetrică a unui filtru Gabor va avea o componentă continuă dacă lărgimea de bandă este mai mare de o octavă, aceasta constituind un dezavantaj. Totuși o componentă continuă zero poate fi obținută pentru orice lărgime de bandă folosind un filtru Gabor care este Gaussian pe o scară logaritmică, filtru cunoscut sub numele de LOG – Gabor.

2.2.6. Potrivirea imaginilor

Scopul îl reprezintă potrivirea imaginilor iris din două șabloane, unul generat și altul care se găsește într-o bază de date sau într-o rețea neuronală

Operațiile care se execută sunt:

- Apelare program calcul_distanță_Hamming dintre două șabloane iris;
- Comparare a fiecărei secvențe din primul șablon, cu o secvență generată din al doilea șablon, secvență obținută prin deplasarea spre dreapta cu o poziție a secvenței din șablonul 2;
- Reținerea celei mai mici distanțe Hamming dintre cele două secvențe ale șabloanelor de test;
- Acceptare / respingere cod iris

Recunoașterea sau identificarea persoanelor după iris rămâne una dintre cele mai sigure metode existente în prezent, în principal din cauza stabilității caracteristicilor și a componenței total aleatoare a acestora. În comparație cu recunoașterea după amprentă, această metodă este total neinvazivă și mult mai sigură din cauza unicității caracteristicilor irisului. Totuși, metoda este pretabilă în cele mai multe cazuri pentru controlul accesului în diverse spații sau pentru recunoașterea persoanelor care dețin un pașaport biometric. Metoda nu poate fi folosită însă în criminalistică, deoarece caracteristicile irișilor nu rămân la locul săvârșirii unor infracțiuni, cum se întâmplă cu amprente digitale sau cu ADN-ul.

2.3. Dispozitive și metode pentru achiziția imaginii irisului

Se pot identifica avantajele majore pe care le au senzorii în prelucrarea și analiza irisului și anume:

- Imaginea preluată de către senzori poate fi prelucrată pe calculator. Există echipamente de preluare a imaginilor care conțin software specializat și metode de procesare a irisului, dintre care se pot aminti: modificarea contrastului, inversare a tonurilor de gri, colorarea artificială, realizarea de măsurători, etc.
- Calitatea imaginii: îmbunătățirea unei imagini într-un anumit sens predefinit; reconstituirea sau refacerea unei imagini degradate, prin utilizarea unor informații despre fenomenul de degradare; principalele surse de zgomot sunt: achiziția și transmisia imaginilor (camera CCD: zgomot influențat de nivelurile de iluminare și temperatura senzorului; transmisia imaginilor: interferențele din canalele de transmisie);
- Grad înalt de siguranță a sistemelor;

- Economia de timp reprezintă un alt avantaj esențial, mai ales în cazul sistemelor CCD (Charge-Coupled Device) care permit afișarea imaginii imediat după expunere;
- Ecologic (neinvaziv pentru mediu). Utilizarea senzorilor optici, capacitivi sau cu ultrasunete nu necesită substanțe chimice cum erau folosite la dezvoltarea filmelor.

2.3.1. Dispozitive utilizate în vederea captării imaginii irisului

În aplicațiile realizate în această teză de doctorat, s-au folosit camera Panasonic BM-ET100US (care este prezentată în figura 2.6 a) și UBKEY MirrorKem (figura 2.6 b). Camera Panasonic este formată din două obiective, cel de sus fiind folosit exclusiv pentru recunoașterea după iris, iar cel de jos poate fi folosit ca și webcam. Această cameră prezintă avantajul că se poate folosi, de asemenea, și pentru recunoașterea facială a persoanei, prin folosirea webcam-ului. Astfel, această cameră este ideală pentru o recunoaștere multimodală a persoanei, după iris și după fizionomia feței.

Sub obiectivul webcam-ului se află o sursă de lumină în spectrul infraroșu apropiat, care se activează atunci când se citește imaginea irisului. Imaginea luată în infraroșu redă mult mai fidel detaliile necesare recunoașterii, deoarece culoarea irisului nu este importantă pentru recunoaștere. De asemenea, în cazul irișilor puternic colorați (spre negru), captarea imaginii folosind lumina naturală ar putea duce la reducerea semnificativă a calității detaliilor necesare unei recunoașteri cât mai exacte a imaginii irisului. De asemenea, trimiterea unui fascicul de lumină naturală sau – mai ales – artificială către iris poate duce la apariția de puncte albe de mari dimensiuni pe pupilă sau chiar pe iris, în acest fel reducându-se șansele unei recunoașteri corecte.

Pe lângă cameră, în pachet se mai găsește software-ul „PrivateID 3.2”, folosit pentru preluarea și recunoașterea imaginilor irisului, precum și aplicația „SecureSuite 3.51”. Aplicația PrivateID 3.2 va fi prezentată în continuare.



a)



b)

Figura 2.6. (a) Camera cu obiectiv pentru recunoaștere după iris (sus) și webcam (jos) Panasonic BM-ET100US; (b) Camera UBKEY MirrorKem

2.3.2. Utilizarea camerei pentru preluarea imaginilor irisului

Aplicația PrivateID 3.2 este inclusă pe CD-ul cu care vine camera Panasonic Authenticam. Are rolul principal de a asigura captarea imaginii irisului sau a feței, folosind

unul dintre cele două obiective disponibile.

În cadrul pachetului sunt incluse mai multe librării DLL, ale căror funcții exportate pot fi utilizate în capturarea imaginii irisului sau a feței. În continuare se vor prezenta două librării, una care este un ActiveX și poate fi apelată direct din cadrul unei aplicații scrise în JavaScript în browser-ul Internet Explorer (celelalte browsere nu acceptă obiecte ActiveX), iar cealaltă poate fi utilizată în cadrul unor aplicații dezvoltate în Microsoft Visual Studio.

2.3.2.2. Funcții din cadrul unei librării utilizate pentru preluarea imaginii irisului de la cameră

Librăria **ClientCoreAPI.DLL** conține mai multe funcții, care sunt documentate în cadrul documentului „Private ID™ API Developer’s Guide” publicat de către producătorul camerei Panasonic, cu numărul de document 101920DOC. Această documentație poate fi descărcată de la adresa <http://www.multibiometrics.ro/apis/privateidapi.pdf>. O implementare a acestei librării pentru apelarea acestor funcții în Java se regăsește în fișierul **ClientCoreAPI_JNIStub.dll**.

Funcția *ClCaptureIrisNonce* este prezentată în Anexa 1.

Apelul acestei funcții duce la apariția pe ecran a unei ferestre pentru a vizualiza imaginea ochiului. De asemenea, LED-urile de infraroșu din partea de jos a camerei sunt aprinse (cel din stânga și cel din dreapta). Utilizatorul vizualizează în interiorul obiectivului de sus al camerei un cerc de culoare portocalie în cazul în care irisul nu este depistat sau nu este focalizat corespunzător. Utilizatorul trebuie să stea la o distanță de aproximativ lungimea antebrațului (acest lucru s-a determinat prin cercetarea momentelor în care focalizarea este optimă – producătorul recomandă o distanță de 19-21 inch de la obiectivul camerei până la iris) și trebuie să-și deplaseze fața astfel încât culoarea cercului să se schimbe în culoarea verde. În acest moment mișcările vor fi din ce în ce mai lente, în vederea focalizării și preluării irisului. Atunci când criteriile de performanță ale imaginii stabilite de producătorul camerei sunt îndeplinite se preia imaginea finală a irisului, iar utilizatorul își poate da seama de acest lucru prin faptul că led-ul de infraroșu din mijloc se aprinde, intensitatea acestuia fiind mult mai mare decât a celor de pe extremități. De asemenea, se aude și un sunet asemănător cu cel al declanșării unui aparat foto. Se preferă preluarea imaginilor în infraroșu deoarece în cazul irișilor foarte închiși la culoare fotografierea acestora în lumină vizibilă nu ar determina captarea de imagini optime pentru recunoașterea persoanelor după iris.

2.3.2.3. Librărie dinamică pentru utilizare în Visual Basic

În cadrul cercetărilor s-a creat o aplicație simplă de tip DLL care exportă funcțiile prezentate anterior în vederea folosirii acestora în cadrul unor aplicații Visual Basic.

Funcțiile discutate anterior sunt declarate ca „__cdecl”. Mediul de programare Visual Basic nu permite accesarea directă a acestor tipuri de funcții, ci doar a celor care sunt declarate cu „__stdcall”.

Imaginile capturate folosind orice aplicație prezentată în acest capitol pot fi folosite în capitolul IV, în vederea prelucrării și a extragerii caracteristicilor.

2.4. Concluzii și contribuții

Recunoașterea persoanelor după iris reprezintă un domeniu relativ nou și în care cercetările continuă într-un ritm foarte alert. Prima parte a acestui capitol face o scurtă introducere în acest domeniu, prin menționarea celor mai importante contribuții ale autorilor

John Daugman, Richard Wildes și Wu Zhi-Li. Capitolul continuă cu descrierea etapelor care sunt parcurse pentru îndeplinirea dezideratului propus, plecând de la preluarea imaginii ochiului de la o cameră sau dintr-un fișier. Următorii pași presupun efectuarea de prelucrări grafice asupra acestora în vederea îmbunătățirii calității caracteristicilor de extras. Se continuă cu segmentarea și normalizarea imaginii, iar în cele din urmă se obține codul iris care poate fi folosit pentru stocarea într-o bază de date sau pentru faza de potrivire, care este analizată în continuarea capitolului. Succesiunea pașilor parcurși și descriși în prima parte a capitolului reprezintă o **contribuție practică**, ce va fi utilizată în dezvoltarea ulterioară de aplicații pentru recunoașterea persoanelor după caracteristicile irisului.

Partea a doua a capitolului conține date și informații importante despre dispozitivele pentru preluarea imaginii irisului, insistându-se pe funcțiile oferite de către camera Panasonic BM-ET100US, ce a fost folosită în cadrul cercetărilor din cadrul tezei de doctorat. În timpul cercetărilor s-au descoperit facilități ale acestei camere nedocumentate de către producător, cum ar fi faptul că imaginile preluate pot fi stocate în fișiere de tip bitmap într-un folder de pe calculatorul pe care aceasta a fost instalată. O parte din funcții sunt descrise detaliat în cadrul Anexei 1. O parte din acest capitol a fost publicată în articolele [62] și [65]. Această parte a capitolului conține o **contribuție practică** reprezentată de posibilitatea de utilizare la un nivel superior a facilităților oferite de camera Panasonic BM-ET100US.

CAPITOLUL III. Contribuții privind recunoașterea persoanelor după amprenta digitală

Acest capitol cuprinde rezultatele obținute în domeniul recunoașterii persoanelor după amprenta digitală. Partea de început a capitolului conține etapele parcurse pentru recunoașterea persoanelor după amprentă, pentru fiecare etapă arătând și rezultatele obținute folosind mediul de programare MatLab. Partea a doua a capitolului conține contribuțiile autorului în ceea ce privește recunoașterea persoanelor după amprentă, cu un accent deosebit pe faza de potrivire, unde se va introduce o metodă euristică de parcurgere a grafurilor bipartite, în acest fel scăzându-se timpul necesar potrivirii, prin scăderea ordinului de complexitate a algoritmului utilizat, prin comparație cu alte abordări ale unor cercetători din domeniu.

3.1. Etape în recunoașterea persoanelor după amprenta digitală

Recunoașterea persoanelor după amprenta digitală presupune parcurgerea mai multor etape, într-o anumită ordine prestabilită. Astfel, din studierea referințelor bibliografice, s-a ajuns la următoarea succesiune de pași:

1. Încărcare imagine;
2. Prelucrarea histogramei imaginilor (egalizare histogramă);
3. Aplicarea transformatei Fourier Rapide – FFT;
4. Binarizare adaptivă;
5. Extragere regiune de interes;
6. Subțiere (scheletizare);
7. Eliminare pori și puncte singulare;
8. Eliminare punți și piteni;
9. Extragere puncte caracteristice amprentă;
10. Eliminare puncte caracteristice false;
11. Salvare imagine pentru potrivire;
12. Potrivire (matching).

În subparagrafele următoare a fost analizat fiecare dintre acești pași, evidențiindu-se rezultatele proprii obținute prin aplicarea lor pe un număr de trei amprente din cadrul bazei de date FVC2002, prezentate în figura 3.1.



Figura 3.1. Exemple de imagini de test (din [45])

3.1.2. Prelucrarea histogramei imaginilor (Egalizare histogramă)

Modificarea nivelurilor de gri are ca scop scoaterea în evidență a anumitor trăsături prin schimbarea contrastului imaginii. După localizarea pixelilor modificați, se pot distinge:

- a. corectarea nivelului de gri dependent de poziția pixelului în imagine;
- b. modificarea scalei nivelului de gri.

După faza de obținere a histogramei cumulative normalizate se trece la faza de egalizare de histogramă. Plecând de la imaginile din figura 3.1, aplicând algoritmi de histogramă cumulativă normalizată și al algoritmului de egalizare de histogramă se obțin imaginile care au contrastul accentuat.

Deci scopul final al egalizării histogramei este acela de a îmbunătăți imaginea preluată.

3.1.3. Transformata Fourier Rapidă

Scopul utilizării Transformata Fourier Rapidă (TFR) constă în îmbunătățirea imaginii, și anume o localizare bună în frecvență și orientare. Imaginea îmbunătățită după aplicarea transformatei Fourier constă în corectarea punctelor false din fiecare linie (pori) din amprentă și eliminarea punctelor singulare dintre linii [47].

3.1.4. Binarizarea adaptivă

Binarizarea imaginii [48] înseamnă transformarea a imaginii unei amprente reprezentată prin tonuri de gri pe 8 biți într-o imagine nouă reprezentată alb/negru (valoarea 0 pentru creste și valoarea 1 pentru adâncituri). Algoritmul este prezentat în Anexa 2.3.

3.1.5. Extragerea regiunii de interes

În vederea extragerii regiunii de interes se face prin aplicarea unor operatori morfologici, dintre care cei mai folosiți sunt erodarea și dilatarea. Erodarea presupune ca fiecare pixel care este aproximativ la fel ca și fundalul este transformat în fundal. Dilatarea presupune ca fiecare pixel care este în contact cu obiectul să fie asimilat obiectului respectiv. Se vor crea doi operatori morfologici M1 (erodare urmată de dilatare) – utilizat pentru eliminarea insulelor din obiect și M2 (dilatare urmată de erodare) pentru eliminarea insulelor din fundal. Rezultatele aplicării celor doi operatori morfologici sunt prezentate în figura 3.2. Algoritmul pentru extragerea regiunii de interes este descris în Anexa 2.4.

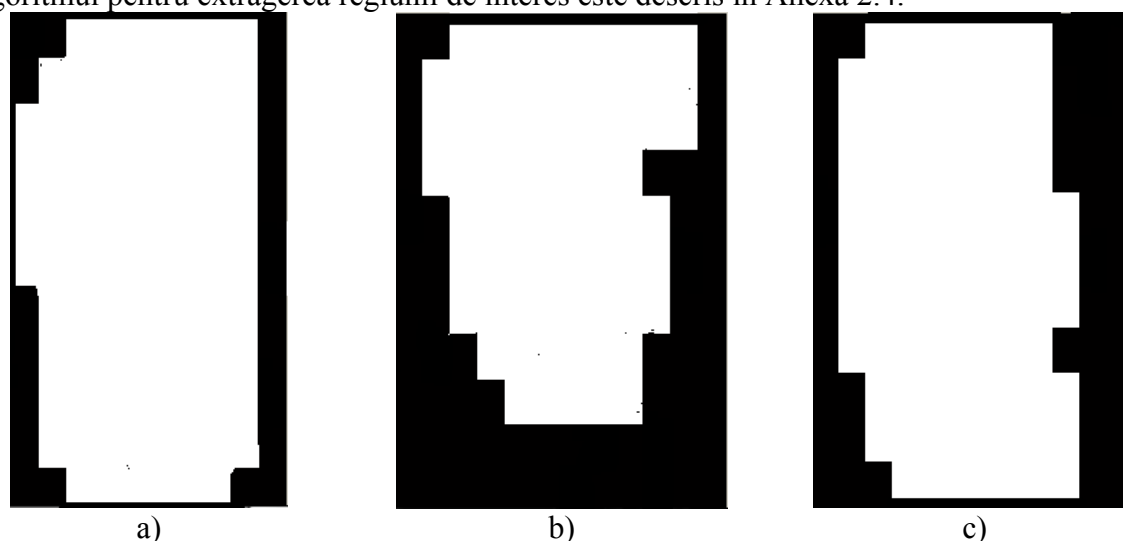


Figura 3.2. Regiunea de interes pentru amprente de test

Pentru operațiile ce vor urma, informațiile utile se vor lua din această regiune demarcată. Regiunea de interes din figura 3.2 este obținută în urma aplicării algoritmului de mai sus și reprezintă zona cu cele mai multe caracteristici biometrice din cadrul amprente digitale.

3.1.6. Subțiere

Subțierea reprezintă operația prin care sunt eliminați pixelii din cadrul regiunii de interes, astfel încât fiecare creastă papilară să aibă dimensiunea de un pixel. Operația de subțiere folosește o matrice de 3x3 cu elemente având valorile 0 sau 1. Algoritmul se poate implementa prin utilizarea a două șabloane, precum și a celor obținute prin rotirea lor la 90°. În fiecare iterație se efectuează operația de subțiere mai întâi cu șablonul 1 și apoi cu șablonul 2, apoi cu celelalte 6 obținute prin rotația lor cu 90°.

Rezultatele obținute după aplicarea algoritmului de subțiere sunt prezentate în figura 3.3.

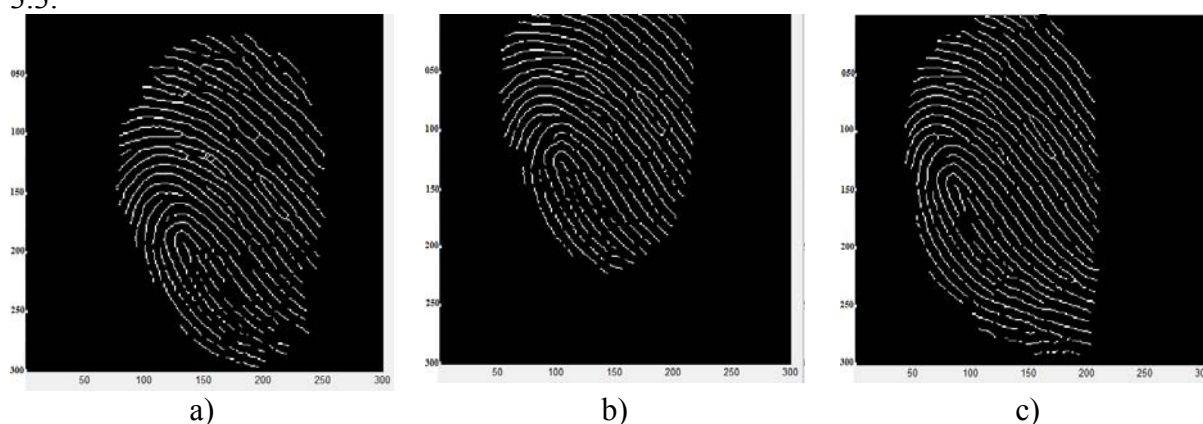


Figura 3.3. Vizualizarea imaginilor obținute după operația de subțiere (pentru amprente de test)

3.1.7. Eliminare pori și puncte singulare. Eliminare punți sau “pinteni”

Punctele care sunt singulare sau punctele care se află între creste se elimină. S-a folosit secvența Matlab din Anexa 2, paragraful A2.5.

În figura 3.4 se prezintă imaginea primei amprente de test, din care au fost eliminate punțile și pintenii și ”spini”.

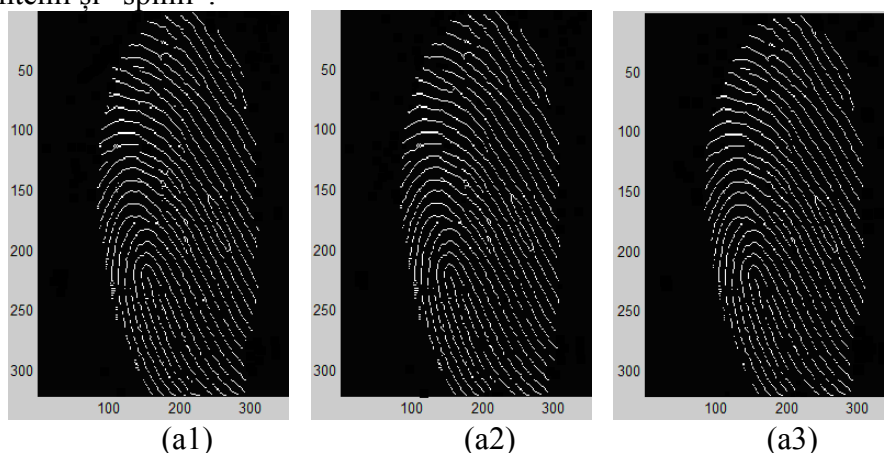


Figura 3.4. a1) Imaginea primei amprente de test scheletizată; a2) Imaginea fără ”punți” și ”pinteni”; a3) imaginea fără „spini”

3.1.8. Extragere caracteristici amprentă

Rezultatele sunt prezentate în figurile 3.5 X1 și 3.5 X2, unde $X \in \{1,2,3\}$.

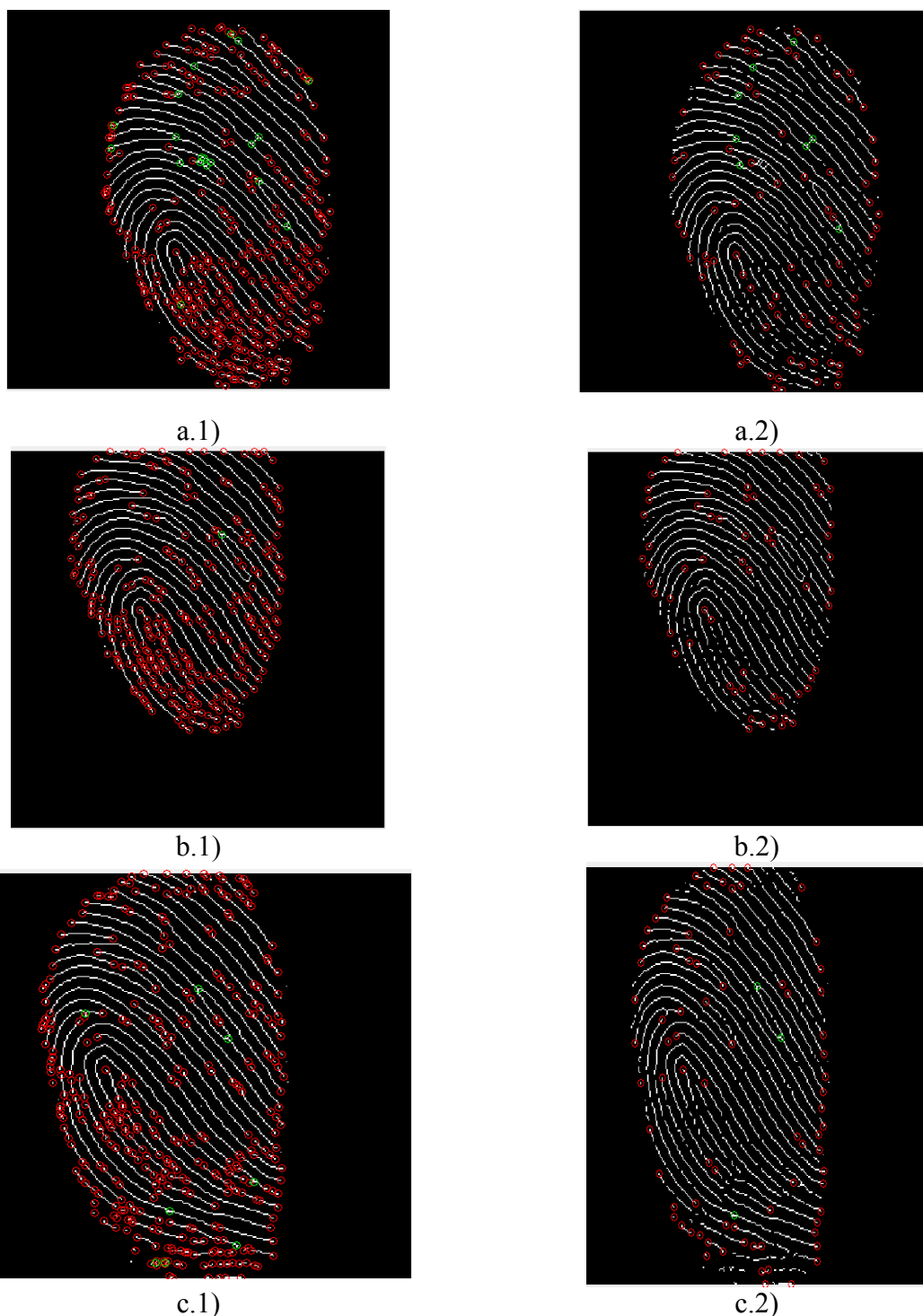
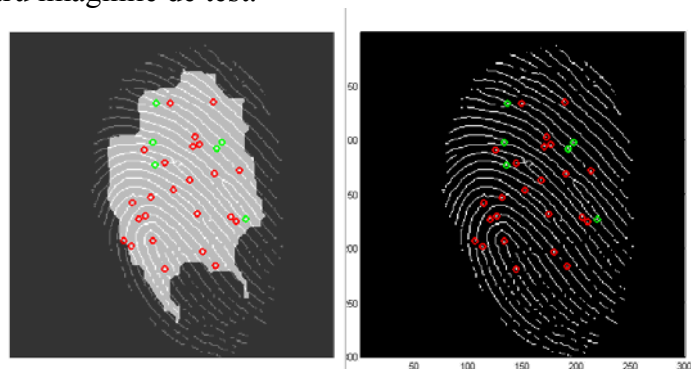


Figura 3.5. X.1) Extragerea tuturor caracteristicilor; X.2) Imaginea obținută după eliminarea caracteristicilor false, unde $X=\{a,b,c\}$, pentru imaginile de test (folosind [46])

Se observă faptul că numărul de puncte de interes (în special terminații) din regiunile de margine ale ampreței nu au fost eliminate în totalitate, acest lucru realizându-se printr-o alegere corectă a regiunii de interes, după cum este descris în continuare.

În figura 3.6 sunt reprezentate punctele caracteristice încadrate într-o regiune compactă (partea stângă), respectiv punctele caracteristice finale reprezentate pe imaginea subțiată (partea dreaptă) pentru imaginile de test.



Terminații:

X	Y	Gradient
144	60	2.36
150	66	0.00
172	97	2.09
127	109	0.00
146	120	-0.52
191	131	1.57
132	152	3.14
115	157	-2.36
211	157	2.09
215	162	-0.79
133	192	-0.79
114	197	-1.57
180	202	2.09
139	208	1.57
211	214	2.09
192	215	-1.57
167	225	1.57
163	232	2.36
168	239	-1.05
190	241	2.09
215	243	2.36
194	246	-0.52
158	249	2.62

Bifurcații:

X	Y	Gradient1	Gradient2	Gradient3
135	67	-2.36	1.05	0.79
133	101	2.36	-2.62	-0.52
198	101	2.36	-2.36	-0.79
192	107	2.36	0.79	-0.79
136	122	3.14	1.57	-0.52
220	172	3.14	1.57	-0.52

Figura 3.6. Rezultate finale. Punctele caracteristice încadrate într-o regiune compactă (partea stângă); punctele caracteristice finale reprezentate pe imaginea subțiată (partea dreaptă); coordonatele punctelor caracteristice și gradientii pentru terminații / bifurcații (în partea de jos a figurii) pentru prima imagine de test

Eliminarea punctelor care se află pe marginile amprente și delimitarea punctelor utile necesare pentru faza de potrivire (obținerea coordonatelor carteziene a punctelor caracteristice (bifurcații și terminații))

Programul MatLab care realizează obținerea regiunii de interes cu punctele caracteristice reale ce vor fi folosite pentru faza de potrivire (a regiunii albe) este descris în Anexa 2, paragraful A2.6.

3.2. Contribuții privind adoptarea unei noi scheme de recunoaștere a persoanelor după amprenta digitală

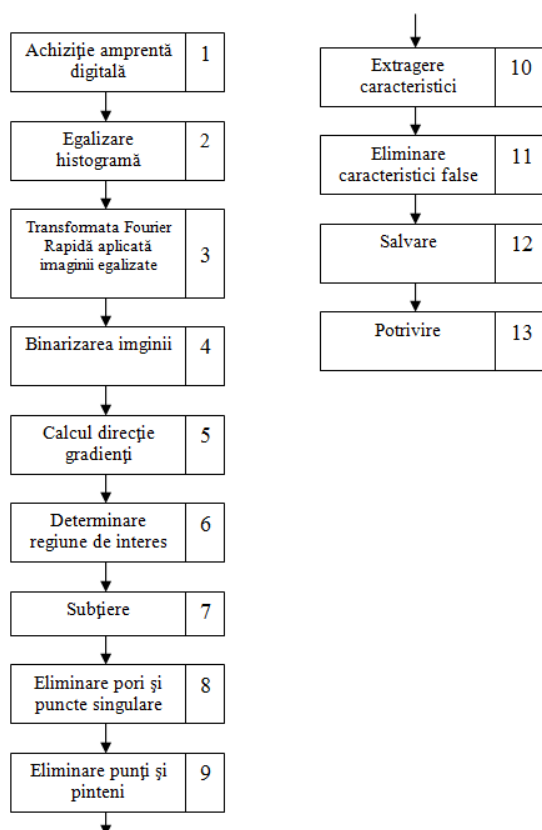
3.2.1. Considerații teoretice

Avându-se în vedere concluziile rezultate din analiza stadiului actual al identificării persoanelor, bazat pe amprenta digitală, respectiv schemele bloc prezentate în [33] și [46]

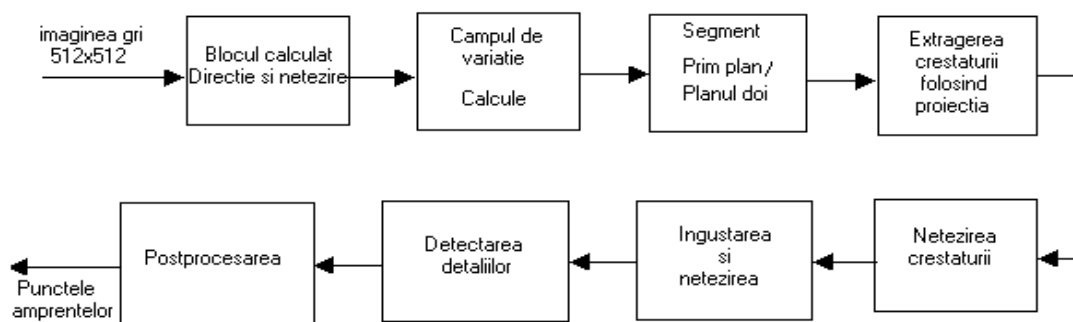
(figura 3.7 a, b) s-a propus adoptarea acestei scheme principale (figura 3.7 c), în vederea realizării cercetărilor teoretice și experimentale dezvoltate în lucrare.

Avantajele metodei propuse sunt:

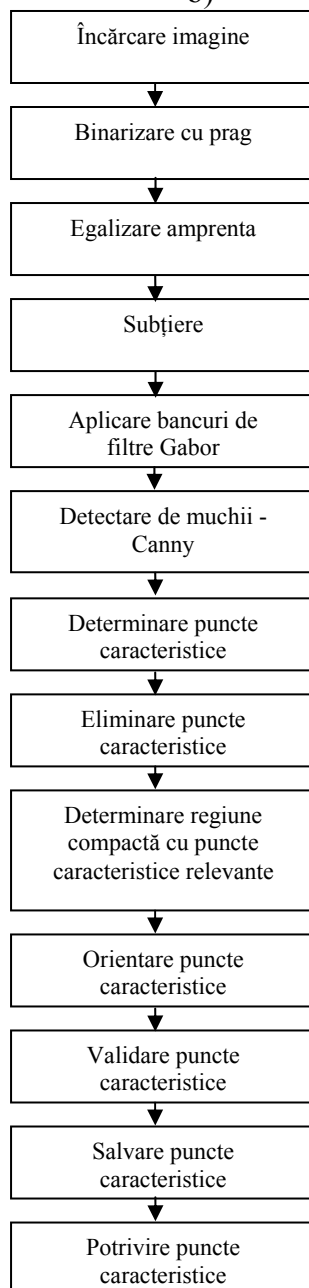
- 1) S-a renunțat la transformata Fourier rapidă pentru calculul disparității punctelor în imagine, deoarece transformata Fourier folosește întreaga imagine pentru calcularea rezultatelor pe când fereastra Gaussiană din filtrele Gabor limitează atenția către o regiune mai mică din imagine.
- 2) Transformata Fourier folosește o fereastră de dimensiune fixă pentru fiecare frecvență, filtrul Gabor folosește o fereastră care se mărește și se micșorează după cum se modifică frecvența de reglare w . La frecvențe înalte lărgimea ferestrei va fi mică asigurând faptul că doar pixelii apropiați vor fi folosiți pentru a calcula ieșirea filtrului. La frecvențe joase fereastra se va lărgi, necesitând mai multe date din semnalul original.
- 3) Determinarea regiunii de interes (faza 6 din schema bloc prezentată în [46]) nu se mai calculează după aplicarea Transformatei Fourier, ci se calculează înainte de a aplica imaginii egalizate filtrele Gabor.
- 4) Calculul regiunii de interes poate fi realizat utilizând algoritmi opționali precum “Divide et Impera” sau programarea dinamică. Regiunea de interes reprezintă zona în care sunt punctele care caracterizează amprenta digitală, eliminând punctele care nu fac parte din amprentă.
- 5) Aplicarea metodei CANNY se folosește pentru detectarea muchiilor, are avantajul pentru evaluarea performanțelor. Sunt luate în considerare trei elemente:
 - detectarea propriu-zisă a muchiei;
 - precizia localizării ei;
 - unicitatea răspunsului (pentru a evita corpurile de dublare a muchiilor deconectate).



a)



b)



c)

Figura 3.7. Schema bloc pentru prelucrarea unei amprente digitale a) model propus în lucrarea [46] b) model propus în lucrarea [33] c) Schema bloc a sistemului integrat prezentat de autor

3.2.2. Aplicație software pentru obținerea punctelor caracteristice

În cadrul cercetărilor din cadrul tezei de doctorat, s-a elaborat o aplicație în MatLab care reprezintă o implementare practică a pașilor propuși în schema de mai sus. Pentru fiecare pas parcurs s-au prezentat rezultatele obținute. Succesiunea fazelor prin care trece o amprentă digitală pentru a extrage punctele de interes este următoarea:

1. Încărcare imagine (prezentată în figura 3.8);
2. Binarizare imagine;
3. Egalizare;
4. Subțiere;
5. Aplicarea bancurilor de filtre Gabor asupra imaginii;
6. Aplicarea operatorului Canny pentru detectarea de muchii și prelungirea prin histereză a punctelor caracteristice;
7. Determinare puncte caracteristice;
8. Eliminarea punctelor caracteristice false;
9. Determinarea regiunii compacte de interes;
10. Orientare puncte caracteristice;
11. Validare puncte caracteristice;
12. Faza de export puncte caracteristice;
13. Imaginea ecran a aplicației unde este prezentată amprenta originală și amprenta cu punctele caracteristice marcate;
14. Imaginea ecran a aplicației unde este prezentată amprenta subțiată și amprenta cu punctele caracteristice marcate.

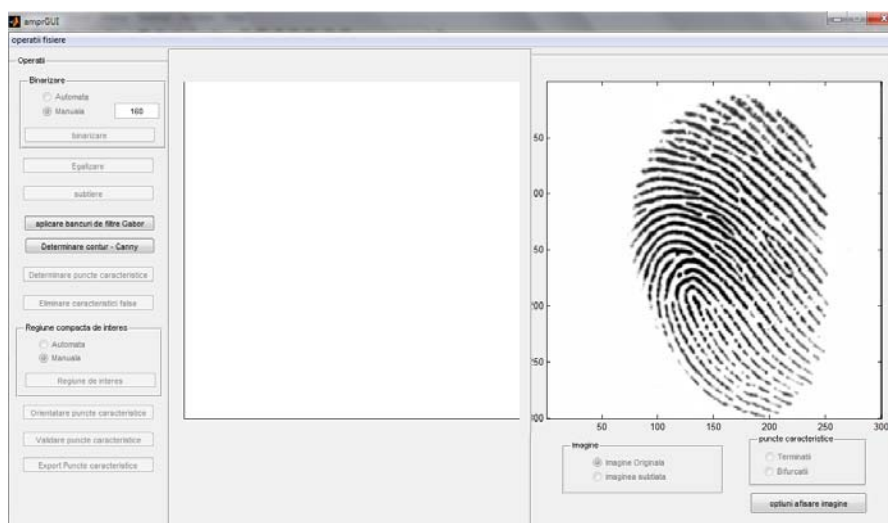


Figura 3.8. Imaginea aplicației după faza de încărcare imagine

3.2.3. Operatori pentru detectarea conturilor și a muchiilor dintr-o imagine a unei amprente

3.2.3.1. Metode pentru detecția muchiilor bazate pe filtrare urmată de aplicarea operatorilor diferențiali pentru amprentă digitală

Prin detectarea muchiilor se înțelege o tehnică de care încearcă să identifice locurile cu variații rapide a intensităților. Fiecare tehnică este caracterizată printr-un set de operatori numiți și detectori de muchii.

Detectarea corectă a muchiilor este o problemă foarte importantă în orice sistem

biometric. Procesul de detectare a muchiiilor servește la simplificarea analizei imaginilor prin reducerea puternică a volumului de date cu păstrarea informațiilor structurale utile despre conturile imaginilor preluate de la amprente digitale. Majoritatea modulelor componente ale sistemelor biometrice depind direct sau indirect de performanțele detectorului de muchii folosit.

După principiul folosit pentru detecția muchiiilor se clasifică în:

- Metode bazate pe aplicarea operatorilor diferențiali;
- Metode bazate pe filtrare urmată de aplicarea operatorilor diferențiali;
- Metode bazate pe aproximarea prin suprafețe unidimensionale având un profil asemănător muchiei;
- Metoda reziduurilor.

După modul de execuție al operațiilor de derivare și filtrare metodele se clasifică în:

- Metode care lucrează cu suprafețe discrete, folosind aproximarea discretă a operatorilor diferențiali prin diferențe finite;
- Metode care lucrează cu suprafețe approximate printr-o funcție continuă și folosesc forma analitică a operatorilor diferențiali.

Tehnicile de detecție a muchiiilor au două etape distincte:

- Marcarea tuturor punctelor caracterizate prin variații rapide ale intensităților;
- Selectarea punctelor de muchie.

a. Metode bazate pe aplicarea operatorilor diferențiali

Metodele bazate pe aplicarea operatorilor diferențiali constau în folosirea diferențierii pentru scoaterea în evidență a punctelor în care există variații rapide a intensității, urmată de aplicarea unui prag pentru eliminarea punctelor ne semnificative. Variațiile rapide de intensitate pot fi accentuate într-o manieră izotropă sau anizotropă folosind operatori derivativi de ordin par respectiv impar.

Principalele dezavantaje sunt date de variațiile de intensitate care pot fi detectate prin diferențiere, dar în cazul semnalelor zgomotoase diferențierea este periculoasă datorită efectului ei de amplificare a frecvențelor înalte. În concluzie semnalul necesită o filtrare prealabilă. Pe de altă parte operația de filtrare este periculoasă deoarece odată cu zgomotul poate elimina și semnal util. Problema de bază a detectorilor de muchii este de a sesiza dacă într-o vecinătate dată există sau nu o variație a semnalului. Dacă operatorul lucrează pe o vecinătate prea mare el poate să se suprapună peste mai mult decât o muchie sau peste o muchie a unei forme complexe, prin urmare răspunsul poate fi eronat. Dacă se lucrează pe o vecinătate prea mică estimarea parametrilor nu este fiabilă. Este necesară corelarea dimensiunilor operatorilor cu dimensiunile detaliilor unite din imagine.

Un alt dezavantaj constă în necesitatea unui pas suplimentar, în general neluat în considerare în evaluarea metodei, constând în subțierea muchiiilor și eliminarea punctelor cu variații ne semnificative.

De aceea voi prezenta în continuare metode bazate pe filtrare urmată de aplicarea operatorilor diferențiali.

b. Metode bazate pe filtrare urmată de aplicarea operatorilor diferențiali

Se pune problema proiectării unui detector de muchii optim. Canny încercă să găsească filtrul care are cele mai bune performanțe, în raport cu următoarele criterii:

- Detecție corectă: Trebuie să existe o probabilitate scăzută de nemarcare a unui

punct real de muchie și o probabilitate scăzută de marcarea a unui punct fals de muchie. Aceste probabilități sunt funcții monoton crescătoare ale raportului semnal – zgomot. Acest criteriu corespunde maximizării raportului semnal – zgomot.

- Localizare corectă: Punctele marcate ca puncte de muchie trebuie să fie cât mai apropiate de punctul real.
- **Un singur răspuns la o singură muchie:** Acest criteriu a fost introdus pentru că forma matematică a primului criteriu nu sesizează situația răspunsurilor multiple. El a dat o formă matematică a celor trei criterii, a găsit filtrul care le maximizează, având o expresie complicată și a arătat că derivata întâi a Gaussianului se apropie foarte mult de acesta. Un rezultat similar se poate obține cu derivata a doua a Gaussianului.

3.2.3.2. Detecția contururilor din imagini ale amprentelor digitale prin aplicarea unor operatori în vederea detecției contururilor

Acest paragraf conține rezultatele experimentale obținute prin aplicarea mai multor operatori asupra unei imagini de test, în vederea detecției contururilor din cadrul acesteia. Din aplicarea operatorilor se determină avantajele și dezavantajele aplicării acestora.

Modificările sau discontinuitățile de intensitate (amplitudine) dintr-o imagine constituie caracteristici fundamentale care pot indica prezența unor obiecte într-o imagine [51]. La operatorii prezentați mai jos, intensitățile se înlocuiesc cu sumele obținute prin convoluția imaginii procesate cu măștile corespunzătoare. Operatorii sunt descriși în lucrarea [41].

Operatorii prezentați mai sus au făcut obiectul articolului [63], iar principala concluzie care se poate trage este că alegerea unuia optim reprezintă o adevărată provocare, în special dacă se ia în calcul timpul necesar aplicării acestuia și calitatea caracteristicilor obținute.

Rezultatele aplicării filtrelor sunt prezentate în continuarea paragrafului.

3.3. Contribuții privind algoritmi utilizați pentru faza de potrivire

3.3.1. Potrivirea amprentelor digitale

Dându-se două seturi de puncte caracteristice pentru două amprente digitale, algoritmul de potrivire a punctelor caracteristice încearcă să găsească dacă setul de puncte din amprenta de intrare corespunde cu setul de puncte din amprenta de ieșire. Algoritmul de potrivire constă din doi pași:

1. alinierea terminațiilor și bifurcațiilor;
2. potrivirea punctelor caracteristice aliniate

După cum se poate observa, potrivirea reprezintă un proces foarte important în recunoașterea persoanelor după amprenta digitală. Amprenta este în continuare folosită la identificarea persoanelor, deoarece, în cazul unor infracțiuni, aceasta rămâne la locul la care s-a produs evenimentul, putând fi prelevată și apoi comparată cu amprente dintr-o bază de date, în vederea încercării de stabilire a vinovatului. Alături de ADN, amprenta păstrează o importantă forță probatoare în criminalistică. De asemenea, este pretabilă a se utiliza și pentru accesul persoanelor în zonele securizate.

Pentru faza de potrivire a două amprente digitale există mai mulți algoritmi, dar cei mai folosiți sunt cei care utilizează potrivirea grafurilor. Potrivirea grafurilor este abordarea cea mai directă a problemei punerii în corespondență. Se bazează pe folosirea grafurilor relaționale atributate pentru reprezentarea atât a scenei cât și a obiectelor model. Metoda

constă în căutarea de sub-grafuri izomorfe între cele două reprezentări. Sau mai precis se caută cuplajul maxim între două grafuri date.

3.3.2. Contribuții privind utilizarea grafurilor în faza de potrivire

În lucrarea [56] se prezintă mai multe noțiuni de teoria grafurilor, ce pot fi utilizate în problema recunoașterii persoanelor după amprenta digitală.

3.3.2.1. Algoritmi pentru determinarea cuplajului maxim

Problemele de repartiție sunt probleme în care se urmărește asemănarea unei amprente digitale cu o amprentă digitală din baza de date, iar rezolvarea acestei probleme constă în determinarea cuplajului maxim (adică determinarea a cât mai multor puncte caracteristice care sunt identice între cele două amprente digitale (potrivirea este inexactă)). Se va lucra în coordonate polare, pentru ca un anumit punct să nu mai fie fix.

Determinarea cuplajului maxim se face cu ajutorul mai multor algoritmi, și anume:

- algoritmul ungar (Kuhn);
- algoritmul lui Little;
- un algoritm euristic

3.3.2.1.1. Algoritmul ungar

Algoritmul ungar este prezentat în lucrarea [57] și presupune parcurgerea următorilor pași:

1. Se formează o matrice C pătratică de ordinul p dacă $p > q$ (se folosesc atâtea coloane cu elemente de 0 până când $p = q$) și de ordinul q dacă $q > p$ (se creează atâtea linii cu elemente egale cu 0 până când $p = q$).
2. Obținerea de zerouri. Se scade minorantul fiecărei linii din toate elementele liniei respective, obținând astfel cel puțin câte un 0 pe fiecare linie a matricei C . Dacă în urma acestei operații există coloane care nu conțin 0, se scade minorantul fiecărei coloane în cauză din toate elementele coloanei respective. Se obține astfel cel puțin câte un 0 pe fiecare linie și coloană a matricei C .
3. În matricea C_1 obținută din matricea C după parcurgerea etapei a doua se caută un cuplaj maxim prin operația de încadrare și barare de zerouri, astfel:
 - a. se încadrează un 0 situat pe linia cu cele mai puține zerouri și se barează (taie) toate celelalte zerouri așezate pe linia și coloana zeroului încadrat;
 - b. se repetă această operație până când toate zerourile matricei C_1 au fost încadrate sau barate. Dacă se obține câte un 0 încadrat pe fiecare linie și coloană, s-a obținut cuplajul maxim. În caz contrar se trece la etapa 4.
4. Căutarea unui cuplaj maxim printr-o marcare a liniilor și coloanelor, astfel:
 - a. se marchează liniile care nu conțin nici un 0 încadrat;
 - b. se marchează coloanele care conțin zerouri tăiate pe liniile deja marcate;
 - c. se marchează liniile care conțin un 0 încadrat pe coloanele deja marcate;
 - d. se repetă aceste operații până când nu mai este posibil să se obțină alte linii sau coloane marcate.
5. În matricea C_1 se taie toate liniile nemarcate și coloanele marcate. Minorantul elementelor rămase netăiate se adaugă elementelor dublu tăiate, se scade din elementele netăiate, lăsând neschimbate elementele simplu tăiate. Se obține astfel o nouă matrice C_2 .
6. Pe matricea C_2 se repetă procedeul de încadrare și tăiere a zerourilor. Se procedează în continuare așa cum s-a arătat mai sus, până când se obține câte un 0

încadrat pe fiecare linie și coloană, deci s-a obținut un cuplaj maxim. Soluția optimă poate să nu fie unică.

Complexitatea acestui algoritm este $O(n^4)$.

3.3.2.1.2. Algoritmul lui Little

În lucrarea [58] se prezintă algoritmul lui Little:

Fie $T = (t_{ij})_{i,j=1}^n$ matricea timpilor.

Algoritmul lui Little presupune parcurgerea următorilor pași:

1. Se determină matricea T_R efectuând operațiile:
 - 1.1. Se scade din fiecare linie cel mai mic element. Mai precis, pentru $i = \overline{1, n}$, se scade din elementele liniei "i" elementul $t_{i\alpha} = \min_{j=1, n} \{t_{ij}\}$.
 - 1.2. Se scade din fiecare coloană cel mai mic element. Mai precis, pentru $j = \overline{1, n}$ se scade din elementele coloanei "j" elementul $t_{\beta j} = \min_{i=1, n} \{t_{ij} - t_{i\alpha}\}$.

2. Se determină constanta de reducere:

$$h = \sum_{i=1}^n t_{i\alpha} + \sum_{j=1}^n t_{\beta j}$$

3. Se va construi un arbore. Fiecărui nod x i se asociază o margine $\omega(x)$. Nodul inițial este E (mulțimea permutărilor definite pe $\{1, 2, \dots, n\}$ și se va pune $\omega(E)=h$;
4. Etapa 4 constă din:
 - 4.1. Pentru fiecare element $t_{ij}=0$ din T_R se calculează:

$$\theta_{ij} = \min_{q \neq j} t_{iq} + \min_{i \neq p} t_{pj}$$

- 4.2. Se determină $\theta_{ke} = \max(\theta_{ij})$;
- 4.3. Se asociază lui E două noduri: E_{ke} și $\overline{E_{ke}}$. De asemenea, se va pune
- 4.4. Se construiește matricea $T(E_{kl})$ obținută din T_R prin suprapunerea liniei k și a coloanei l . Se aplică acestei matrici etapele 1 și 2 și se determină $T_R(E_{kl})$ și constanta de reducere h_{kl} . Se va pune

$$\omega(\overline{E_{ke}}) = \omega(E) + \theta_{ke}$$

$$\omega(E_{kl}) = \omega(E) + h_{kl}$$

5. Dacă s-a obținut o matrice de tipul (1,1) algoritmul s-a încheiat. În caz contrar ramificarea se continuă din acel nod cu marginea cea mai mică. În cazul mai multor noduri se alege un nod de tip E_{kl} . Dacă s-a ales un nod de tip E_{kl} se trece la etapa 4. Dacă s-a ales un nod de tip $\overline{E_{kl}}$ atunci pentru a evita afectarea (k,l) se pune în matricea nodului precedent $t_{kl}=\infty$ și se trece la etapa 4.

3.3.2.1.3. Procedeu euristic pentru determinarea cuplajului maxim într-un graf bipartit

Modelul matematic al acestui procedeu euristic este următorul:

Punerea problemei

Dându-se mulțimile de indici $I'=\{1, 2, \dots, m\}$, $I''=\{1, 2, \dots, n\}$ și o mulțime $L \subset I' \times I''$, se

atașează fiecărei perechi $(i, k) \in L$ o constantă v_{ik} și o variabilă ξ_k^i , cu valori din $\{0,1\}$. Se cere să se găsească pentru variabilele ξ_k^i valorile care satisfac condițiile:

1. $\sum_{k=1}^n \xi_k^i \leq 1, i=1, 2, \dots, m$
2. $\sum_{i=1}^m \xi_k^i \leq 1, k=1, 2, \dots, n$
3. $\sum_{(i,k) \in L} \xi_k^i = \min(m,n)$
4. $\sum_{(i,k) \in L} v_{ik} \xi_k^i$ să fie minimă

L definește o anumită relație între I' și I'' , care se presupune prestocastică și surjectivă.

Așa cum a fost enunțată, problema afectării este o problemă de programare liniară; aceasta va fi abordată însă cu ajutorul grafurilor.

Mulțimile de puncte

$$X = \{x_i \mid i \in I'\}; Y = \{y_k \mid k \in I''\}$$

formează împreună cu relația dată de L , un graf simplu, căruia i se notează cu U mulțimea arcelor:

$$(i,k) \in L \Leftrightarrow (x_i, y_k) \in U$$

Fiecărui arc $(x_i, y_k) \in U$ îi este atașat un număr v_{ik} , iar din condiția 1 rezultă că dintre numerele v_{ik} atribuite arcelor incidente exterior în $x_i (\forall i \in I')$ cel mult unul poate să intre în suma 4, căci celelalte arce nu pot fi decât $\xi=0$. Analog, condiția 2 arată că doar cel mult unul dintre numerele atribuite arcelor incidente interior în $y_k (\forall k \in I'')$ poate participa la formarea sumei 4. Așadar, soluția căutată se situează pe arcele unui cuplaj în graful simplu $G=(X,Y,U)$.

Pe de altă parte, din condiția 3 reiese că:

- a) Dacă $m < n$, numărul arcelor cuplajului este m , deci cuplajul este al lui X în Y , deci este maximal;
- b) Dacă $m > n$, numărul arcelor cuplajului este n , deci cuplajul este al lui Y în X , el fiind maximal;
- c) Dacă $m=n$, cuplajul este al lui X pe Y , deci este maximal și în acest caz.

Așadar, graful simplu G care modelează problema afectării se bucură de proprietatea că în el avem $Q(G) = \min(m, n) = \min(\#X, \#Y)$.

Problema afectării revine la alegerea, dintre cuplajele maximale existente într-un astfel de graf, a celor pentru care suma numerelor v_{ik} atașate arcelor lor să fie minimă.

Dacă, în locul condiției 4, s-ar cere ca

$$\sum_{(i,k) \in L} v_{ik} \xi_k^i \text{ să fie maximă,}$$

problema s-ar reduce la cea precedentă, punând

$$V = \max_{(i,k) \in L} v_{ik} \text{ și } t_{ik} = V - v_{ik}$$

Atunci avem

$$\sum_{(i,k) \in L} v_{ik} \xi_k^i = V \cdot \sum_{(i,k) \in L} \xi_k^i - \sum_{(i,k) \in L} t_{ik} \xi_k^i = V \cdot \min(m,n) - \sum_{(i,k) \in L} t_{ik} \xi_k^i$$

deci

$$\max \sum_{(i,k) \in L} t_{ik} \xi_k^i = V \cdot \min(m,n) - \min \sum_{(i,k) \in L} t_{ik} \xi_k^i$$

Așadar, problema de maxim se poate transforma într-una de minim și reciproc.

Observație. În practică este mai comod să se recurgă la transformarea

$$V_k = \max_i v_{ik} \text{ și } t_{ik} = V_k - v_{ik} \quad (\forall k \in I'') \text{ când } m \geq n$$

sau

$$V_i = \max_k v_{ik} \text{ și } t_{ik} = V_i - v_{ik} \quad (\forall i \in I') \text{ când } m \leq n$$

spre a se obține direct zerourile coloanelor (liniilor) matricei $\|t_{ik}\|$, cum se va de vedea, mai departe, într-un exemplu. Este ușor de verificat că și în acest caz problema de maxim se transformă într-una de minim.

Numerele v_{ik} pot fi considerate toate nenegative, căci, dacă n-ar fi, s-ar putea pune

$$v_0 = -\min_{(i,k) \in L} v_{ik} \quad (v_0 > 0) \text{ și } \theta_{ik} = v_0 + v_{ik} \quad (\theta_{ik} \geq 0)$$

Rezultă că

$$\sum_{(i,k) \in L} v_{ik} \xi_k^i = \sum_{(i,k) \in L} \theta_{ik} \xi_k^i - v_0 \cdot \min(m, n)$$

deci optimul (maximul sau minimul) are loc, pentru ambele sume, cu aceleași perechi $(i,k) \in L$.

În practică, problema afectării se întâlnește de multe ori sub forma particulară în care $m = n$. Atunci luând $I' = I'' = I = \{1, 2, \dots, n\}$ și subînțelegând condiția $Q(G) = n$ pe care graful o îndeplinește în acest caz, condițiile 1-4 se reduc la următoarele trei:

- a) $\sum_{k \in I} \xi_k^i = 1, \quad (\forall i)$
- b) $\sum_{i \in I} \xi_k^i = 1, \quad (\forall k)$
- c) $\sum_{(i,k) \in L} v_{ik} \xi_k^i$ să fie minimă

Într-adevăr, într-un graf simplu în care $\# X = \# Y$ și cuplajul maximal este al lui X pe Y , condițiile 1 și 2 se transformă în egalități.

Toate cele ce preced rămân valabile și în acest caz particular, în care s-a încadrat și chestiunea redistribuirii sarcinilor, de mai sus.

Există diferite metode pentru soluționarea problemei afectării. Se poate, de exemplu, folosi metoda „Branch and Bound”, după cum se poate observa în continuare.

Algoritmul euristic propus pentru soluționarea problemei afectării este următorul:

1. Se împart în prealabil arcele grafului simplu ce modelează problema (a se vedea punerea problemei și transformarea ei într-o problemă de cuplaje în grafuri) în clase având același v_{ik} . Clasele se ordonează după v_{ik} crescător și în interiorul fiecăruia se articulează arcele adiacente.
2. Se ia un arc din prima clasă și se exclud ambele sale extremități din toate clasele următoare, deoarece arcele cuplajului nu pot fi adiacente. Se continuă, după v_{ik} crescător, alegerea arcelor cu ambele extremități intacte, excluzând apoi aceste extremități din clasele următoare, până se formează un cuplaj maxim W_0^j cu n arce, dacă $n \times n$ este ordinul matricei $\|v_{ik}\|$.
3. Se calculează $S_j = \sum_{(x_i, y_k) \in W_0^j} v_{ik}$ pentru fiecare W_0^j astfel obținut și se rețin cele mai mici sume.

Observație. De obicei sunt suficiente câteva încercări pentru obținerea soluției. La aplicarea corectă, acest procedeu nu poate omite niciuna dintre soluțiile pe care la admite problema.

Pentru calcul complexității algoritmului, în cazul unei astfel de reprezentări a grafurilor în memorie, s-a încercat depistarea cazului cel mai defavorabil care poate să apară. Algoritmul poate fi descris astfel:

```

Lista[i]={element[1],..., element[L[i]]
pentru fiecare Lista[i] din multimea de K liste {Lista[1], ..., Lista[K]}
    pentru fiecare element[j] din Lista[i] de L[i] elemente
        alfa1: proceseaza perechea element[j]
        alfa2: daca s-a construit cuplajul, se opreste algoritmul
    sfarsit pentru
sfarsit pentru

```

Acest algoritm parcurge secvența $\alpha_1 + \alpha_2$, în cel mai defavorabil caz, pentru *toate* elementele ale *tuturor* listelor, adică de *exact* $n \times n$ ori. Prin urmare, $\text{COMPLEXIT}(\text{algoritm}) = O(n \times n \times (\text{COMPLEXIT}(\alpha_1) + \text{COMPLEXIT}(\alpha_2)))$.

La nivelul secvenței *alfa1*, se decide dacă se pune în cuplaj muchia, parcurgând cuplajul parțial construit. Parcurgerea acestei liste de muchii alese până în acest moment ar fi, în mod normal de $O(n)$, la o parcurgere liniară, $O(\log(n))$ dacă se introduce un index de sortare și se face căutare binară pentru decizie, sau chiar $O(1)$, dacă se folosește cu un vector caracteristic pentru o mulțime de noduri (parțială), adică o căutare directă.

Legat de complexitatea lui *alfa2*, verificarea terminării construcției cuplajului se face prin parcurgere completă, în acest caz complexitatea fiind $O(n)$ sau eventual se poate folosi căutarea/sortarea directă, caz în care complexitatea este $O(1)$. Se poate de asemenea introduce o modalitate de reținere a pasului anterior de verificare și a modificării aduse, în acest caz complexitatea fiind $O(\log(n))$ sau chiar $O(1)$.

Ca o concluzie, se poate considera că

$$\text{COMPLEXITATE}(\alpha_1) = \text{COMPLEXITATE}(\alpha_2) = O(1),$$

deci

$$\text{COMPLEXITATE}(\text{algoritm}) = O(n \times n).$$

În acest fel se poate observa foarte ușor faptul că s-a redus complexitatea algoritmului de la $O(n^4)$ în cazul metodei ungare la doar $O(n^2)$ pentru algoritmul euristic propus.

Experimental s-a folosit acest algoritm pentru potrivirea amprentelor digitale. Din comparațiile cu metodele propuse anterior, s-a determinat o îmbunătățire substanțială a timpului de recunoaștere a unei amprente digitale. În tabelul 3.2 sunt prezentate rezultatele obținute prin utilizarea acestui algoritm, în comparație cu aplicarea algoritmului ungar sau a algoritmului lui Little.

Tabelul 3.2. Comparație între algoritmul ungar și algoritmul euristic

Dimensiunea matricei	Timpul de calcul al metodei ungare (secunde)	Timpul de calcul al algoritmului euristic propus de autor (secunde)
4×4	0,063	0,041
5×5	0,078	0,059
7×7	0,214	0,130
8×8	0,255	0,135
9×9	0,485	0,171
10×10	0,795	0,235

50×50	38	7,431
100×100	44	8,256
200×200	85	9,159

Abordarea rezolvării problemei de afectare prin utilizarea unui algoritm euristic a dus la rezultate ale comparării amprentelor digitale cu un consum de timp și calcul mult diminuate. Acest algoritm poate fi folosit cu succes în aplicații care necesită un timp foarte mic de răspuns, cum ar fi în cazul identificării persoanelor înregistrate într-o bază de date cu un număr foarte mare de amprente.

3.4. Concluzii și contribuții

Acest capitol conține principalele contribuții ale autorului în ceea ce privește recunoașterea persoanelor după amprenta digitală.

Principalele **contribuții teoretice** sunt:

- adoptarea unei noi scheme de recunoaștere a persoanelor după amprentă, după analizarea altor două metode propuse de autori;
- s-a propus un algoritm euristic pentru potrivirea amprentelor digitale folosind grafurile, prin aceasta reducându-se semnificativ timpul de execuție, datorită scăderii ordinului de complexitate;
- propunerea unei metode de determinare a punctului de referință pentru alinierea punctelor caracteristice.

Dintre **contribuțiile practice**, cele mai importante sunt următoarele:

- analiza succesiunii pașilor parcurși în vederea recunoașterii persoanelor după amprenta digitală poate fi utilizată în dezvoltarea ulterioară de aplicații în acest domeniu;
- realizarea unei aplicații în mediul de programare MatLab, plecând de la schema propusă în cadrul tezei și utilizată în scopul validării practice a contribuției teoretice;
- aplicarea mai multor operatori asupra primei imagini de test, în vederea vizualizării diferențelor între ei și pentru alegerea celui optim în fiecare caz.

CAPITOLUL IV. Cercetări asupra unor sisteme integrate pentru accesul la aplicații de internet banking folosind recunoașterea persoanelor după iris și amprentă

4.1. Introducere

Serviciile de internet banking au devenit unele dintre cele mai importante aplicații din Internet, fiind furnizate de majoritatea băncilor de pe întregul mapamond. Acestea au fost introduse la începutul anilor 1980 și sunt într-o creștere exponențială. Cele mai multe bănci furnizează aceste tipuri de servicii clienților lor cu scopul reducerii tranzacțiilor clasice care presupun prezentarea fizică la sediul băncii.

Majoritatea salariilor sunt plătite într-un cont bancar și astfel beneficiarul poate avea un control asupra finanțelor proprii prin utilizarea serviciilor de internet banking, direct de pe calculatorul personal de acasă, nefiind necesară prezența fizică la sediul băncii sau la alți furnizori de servicii pentru efectuarea de plăți.

Securitatea în ceea ce privește autentificarea la serviciile de online banking poate varia de la combinația clasică de utilizator și parolă statică (care în ultimul timp a fost abandonată) până la tehnici mult mai avansate, care utilizează un nume de utilizator și o parolă generată dinamic de către un dispozitiv de tip digipass sau primită prin SMS (OTP – One Time Password – o parolă care poate fi utilizată o singură dată, pentru o perioadă limitată de timp (de exemplu 30 secunde)).

Principala problemă identificată este faptul că dispozitivele digipass pot fi pierdute, furate sau indisponibile (determinate de plasarea în alt loc decât cel din care se dorește accesarea serviciului sau pot apărea probleme de funcționare necorespunzătoare din cauza unei baterii descărcate, de exemplu). Același lucru se întâmplă și în cazul primirii parolei OTP prin SMS, în acest caz telefonul putând fi descărcat sau într-o zonă fără semnal corespunzător.

De aceea s-a identificat posibilitatea de utilizare a unei caracteristici biometrice pe lângă numele de utilizatori. Utilizarea unei caracteristici biometrice bine alese, care să confere un grad ridicat de disponibilitate și o rată de erori cât mai mică, va duce la creșterea siguranței în autentificarea la aceste tipuri de servicii.

Schematic, în figura 4.1 este prezentată o aplicație de internet banking, atât din punctul de vedere al utilizatorului, cât și pentru lucrătorul bancar. În partea din stânga a schemei se prezintă interfața utilizatorului serviciului de online banking. Acesta se va autentifica folosind un nume de utilizator, o parolă generată de un digipass (acest pas poate lipsi, dacă se folosește irisul) și un iris deja înregistrat în baza de date a băncii. Se folosește numele de utilizator pentru a realiza o *verificare* (o căutare de tipul 1:1) în baza de date, în acest fel timpul de răspuns fiind mult mai scurt decât în cazul unei *identificări* (ce presupune o căutare 1:N a irisului în baza de date). După autentificare utilizatorul poate realiza diverse operațiuni, cum ar fi inițierea unei plăți sau constituirea/lichidarea unor depozite.

În cazul efectuării de plăți, după introducerea datelor referitoare la codul IBAN, sumă și detalii, utilizatorul va trebui să semneze electronic ordinul de plată constituit. Acest lucru se va realiza prin utilizarea unui digipass (la fel, poate lipsi acest tip de semnătură) și imaginea irisului său, care se găsește deja în baza de date a băncii.

Din punctul de vedere al lucrătorului băncii, acesta se va autentifica la aplicația proprie (se poate folosi și aici autentificarea cu caracteristici biometrice și chiar este implementată în anumite bănci), după care va putea efectua operațiuni asupra conturilor utilizatorului. De exemplu, poate crea un nou cont bancar, în acest caz fiind necesară parcurgerea mai multor

etape, începând de la introducerea datelor de identificare a utilizatorului serviciului de internet banking, continuând cu asignarea unui digipass și înregistrarea irisului utilizatorului în baza de date.

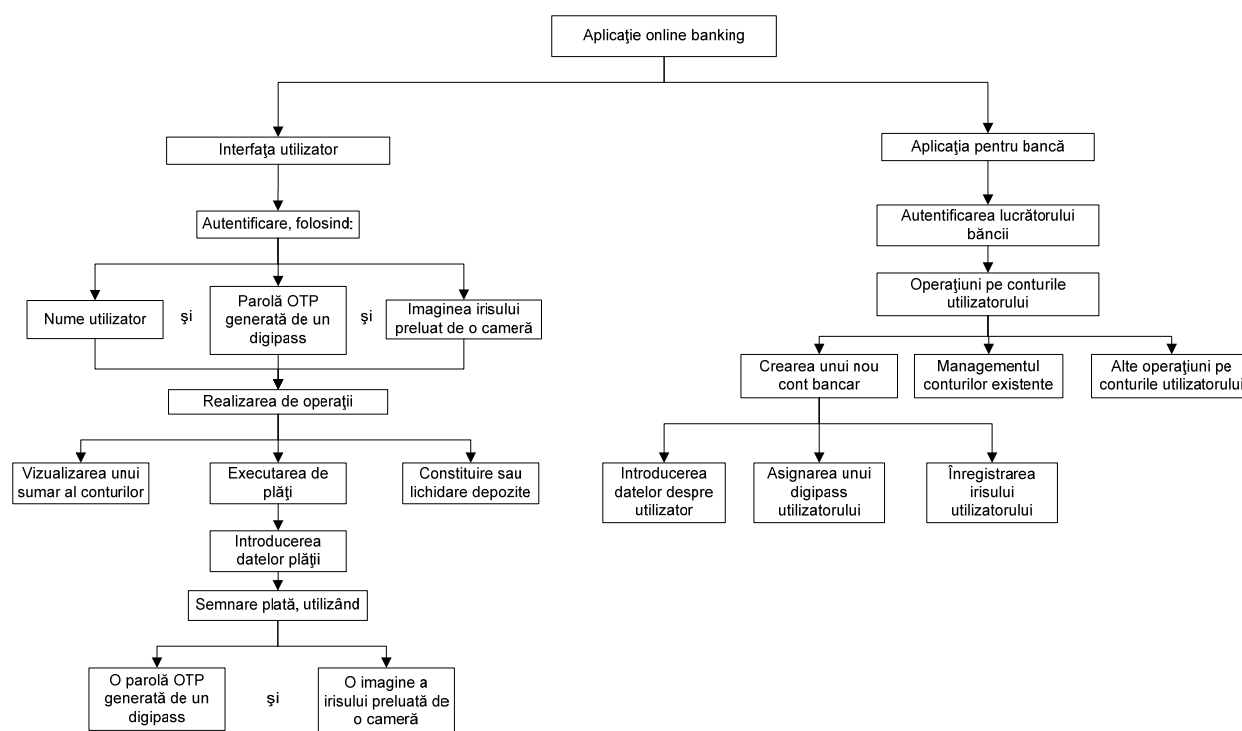


Figura 4.1. Schema accesului la aplicația de online banking

În subcapitolele următoare se vor prezenta două aplicații, una pentru înregistrarea irisului utilizatorului într-o bază de date și cealaltă pentru simularea accesului la aplicația de internet banking al Băncii Transilvania.

4.2. Aplicație pentru înregistrarea irisului utilizatorului de internet banking

În cadrul cercetărilor s-a realizat o aplicație pentru înregistrarea irisului utilizatorului într-o bază de date. Aplicația este disponibilă la adresa <http://multibiometrics.ro/iris/enroll/>. La deschiderea aplicației se afișează pagina de start, care conține un buton și șase celule dintr-un tabel în care se vor afișa imaginile preluate de la camera Panasonic BM-ET100US.

La apăsarea butonului se va începe preluarea efectivă a imaginii irisului, folosind funcțiile și procedeele oferite de cameră. În figura 4.2 este rezultatul final al preluării imaginilor.

Aplicația este scrisă în limbajul HTML, folosind un script JavaScript pentru accesarea obiectelor de tip ActiveX. În cadrul fișierului „index.html” se descriu toate elementele din pagina afișată și de asemenea se va maximiza fereastra browser-ului (se simulează apăsarea tastei F11, ceea ce duce la afișarea paginii din Internet Explorer în modul full-screen).

La apăsarea butonului din pagină se execută funcția mainProgram(), care presupune parcurgerea următorilor pași:

1. Se testează dacă există folderul „c:\camtest\log” (în care se vor stoca imaginile), iar dacă nu există se va crea;

2. Se modifică regiștrii Windows pentru a se activa opțiunea „LogImages” (va avea valoarea 1, conform celor prezentate în capitolul 2);
3. Cele 6 celule pentru vizualizarea imaginilor preluate sunt inițializate cu o imagine standard, care conține textul „Waiting for iris image ...”;
4. Se apelează funcția createEnrollFolders, care are rolul de a crea un folder cu denumirea „C:\camtest\log\iris_enroll_ZZ.LL.YYYY-HHMMSS, unde ZZ este ziua curentă, LL – luna, YYYY – anul, HH – ora, MM – minutul și SS – secunda; în cadrul acestui folder se creează 6 foldere cu denumirea iris1 ... iris6 (în care vor fi stocate imaginile de la cele 6 prelevări) și un alt folder cu denumirea found_files în care se mută fișierele găsite în „c:\camtest\log” în momentul rulării aplicației;
5. Se execută o instrucțiune “for” pentru a prelua cele 6 imagini ale irisului; pentru fiecare preluare se apelează funcția doPrivateID, rezultatul fiind în variabila “img”; după preluarea cu succes se modifică imaginea corespunzătoare din cadrul paginii, folosind proprietatea document.getElementById(imgNo).src;
6. Se solicită apăsarea butonului OK pentru preluarea următoarei imagini sau Cancel pentru a finaliza operațiunea de preluare;
7. Când au fost preluate toate cele 6 imagini se afișează un mesaj prin care se anunță finalizarea procesului de preluare.

În cercetările viitoare se va implementa un alt obiect de tip ActiveX de către autor, în vederea procesării imaginilor, obținerea de IrisCode-uri, compararea două câte două a imaginilor și înregistrarea în baza de date.

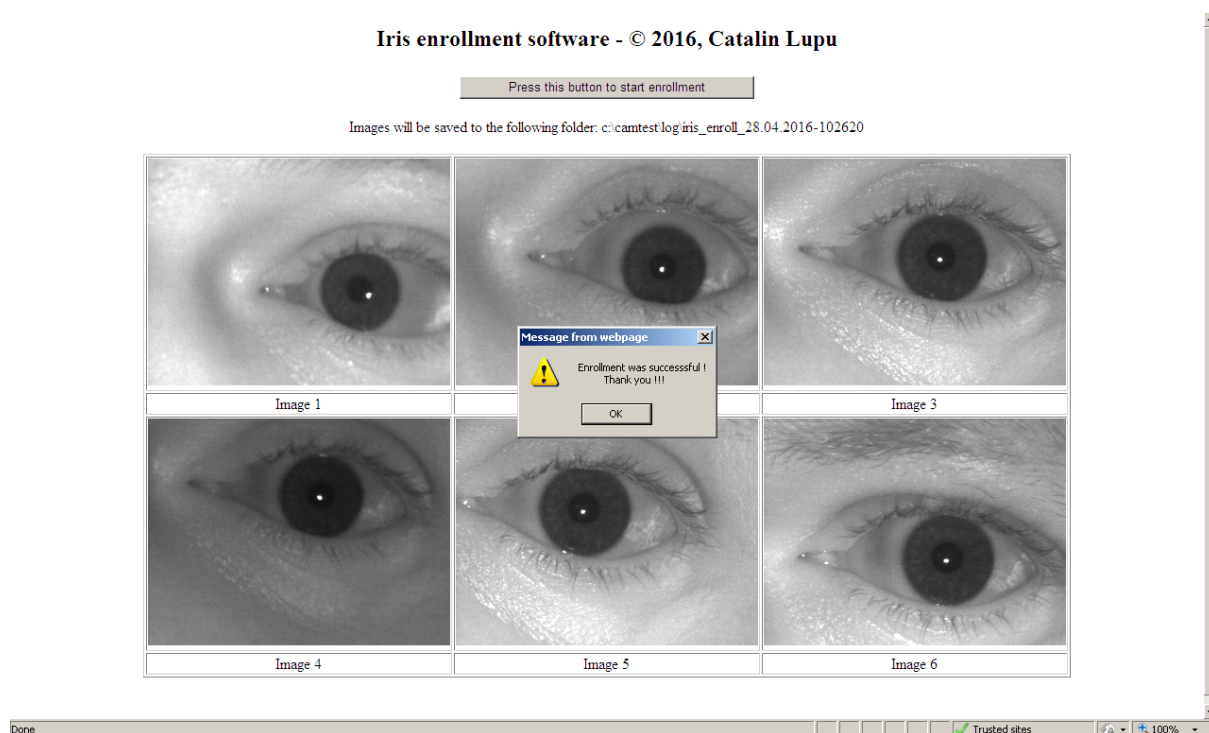


Figura 4.2. Finalizarea procesului de preluare a irișilor

4.3. Aplicație practică de acces la aplicația de internet banking

În cele ce urmează se va prezenta o aplicație pentru simularea accesului la aplicațiile de internet banking. În acest scop s-a salvat pagina <https://ib.btrl.ro/BT24/bfo/channel/web/>

`loginframe.jsp?locale=RO` și a fost modificată pentru ca la apăsarea butonului OK să se preia și irisul utilizatorului.

Pagina modificată a fost postată pe site-ul propriu, la adresa <http://www.multibiometrics.ro/bt24/> și este folosită doar în interesul cercetării, neînregistrând nicio dată din cele introduse (nu are aceleași funcționalități ca aplicațiile rău-voitoare, de tip phishing).

În figura 4.6 se prezintă pagina principală a aplicației de pe site-ul propriu. Utilizatorul introduce ID-ul de logare și parola generată de un dispozitiv digipass. Având în vedere caracterul strict de prezentare a unor facilități, în aceste câmpuri se poate introduce orice valoare, în momentul de față. După introducerea acestor date, la apăsarea butonului OK se afișează fereastra pentru previzualizarea imaginii preluate de la camera Panasonic BM-ET100US. Acest lucru se poate vedea în figura 4.3. După preluarea unei imagini a ochiului se va deschide o nouă pagină, salvată de asemenea din aplicația de internet banking a Băncii Transilvania. Aceasta este similară cu cea deschisă după conectarea la serviciul oferit de bancă, fiind de asemenea o „clonă” a paginii originale. Ca și în cazul paginii anterioare, aceasta doar afișează ceva, fără a prelua sau stoca date.

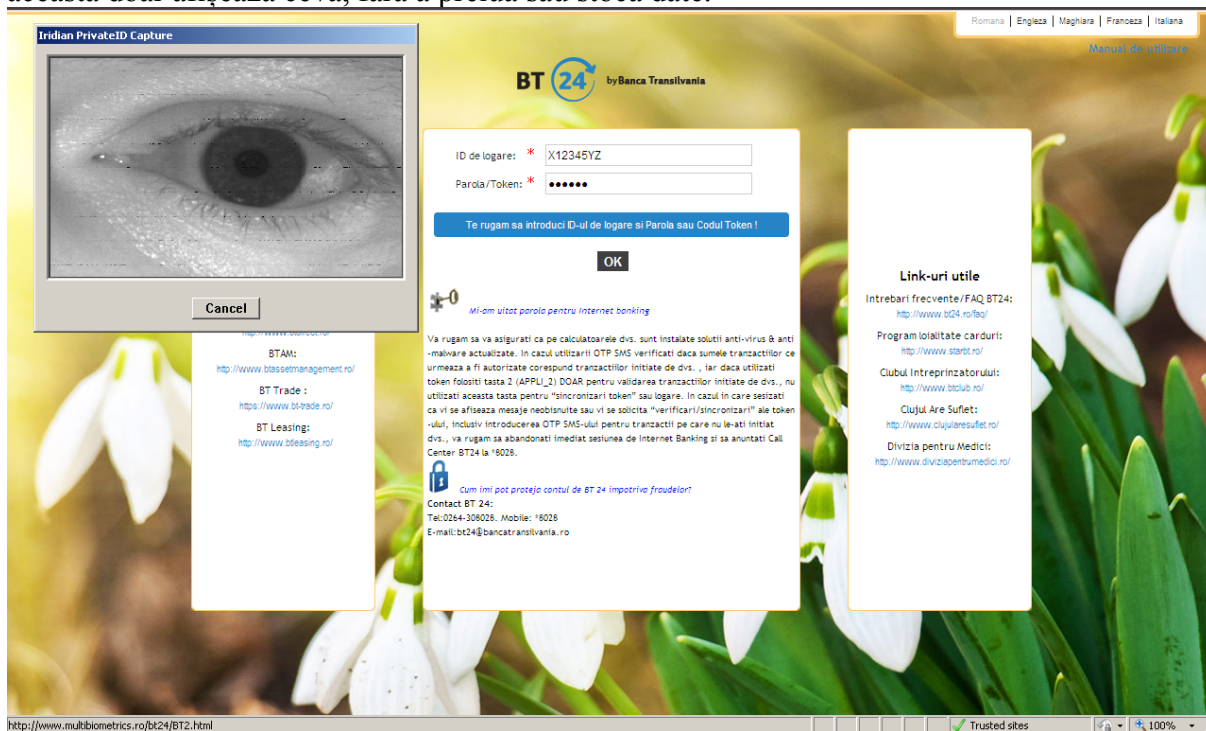


Figura 4.3. Pagina după apăsarea butonului OK, cu afișarea ferestrei de vizualizare a imaginii preluate de la camera

Aplicațiile prezentate mai sus vor fi dezvoltate și pe viitor, pentru a realiza toți pașii care trebuie parcurși de la preluarea imaginii irisului și obținerea unui cod al irisului ce poate fi folosit pentru căutări în baza de date.

4.4. Aplicații practice pentru înregistrarea și recunoașterea persoanelor după amprenta digitală

În acest subcapitol se vor prezenta trei aplicații din diferite domenii de activitate, astfel:

- o aplicație pentru înregistrarea persoanelor în vederea utilizării ulterioare a unei aplicații de tip internet-banking;
- aplicații și dispozitive destinate dispozitivelor smartphone care nu au inclus un senzor de amprentă, pentru acordarea accesului la ecranul principal al acestuia;

- un modul Arduino MEGA 2560 și mai mulți senzori cuplați la acesta, pentru acordarea accesului la o aplicație de internet banking;

4.4.1. Aplicație standalone pentru înregistrarea persoanelor în vederea asigurării accesului la aplicații de tip internet-banking

Aplicația a fost realizată în Visual Studio 2008. Pentru această aplicație s-a folosit un senzor de amprentă Microsoft Fingerprint Scanner.

Senzorul de amprentă este cel din figura 4.4.



Figura 4.4. Senzorul de amprentă folosit în aplicație

Pentru a asigura interfața între dispozitiv și sistemul de operare, s-a folosit pachetul oferit de firma Griaule Biometrics. La instalarea acestei aplicații se modifică driverul oferit de către producătorul dispozitivului cu unul furnizat de acest software, în vederea comunicării mai facile între aplicație și dispozitiv. După instalarea aplicației se poate folosi un obiect creat special pentru mediul de programare Visual Studio, în vederea comunicării dintre aplicație și dispozitivul de citire al amprenteii. Acest obiect se regăsește în figura 4.5 și se poate vedea în partea de dreapta sus a formei, iar o parte din proprietățile acestuia în partea dreaptă.

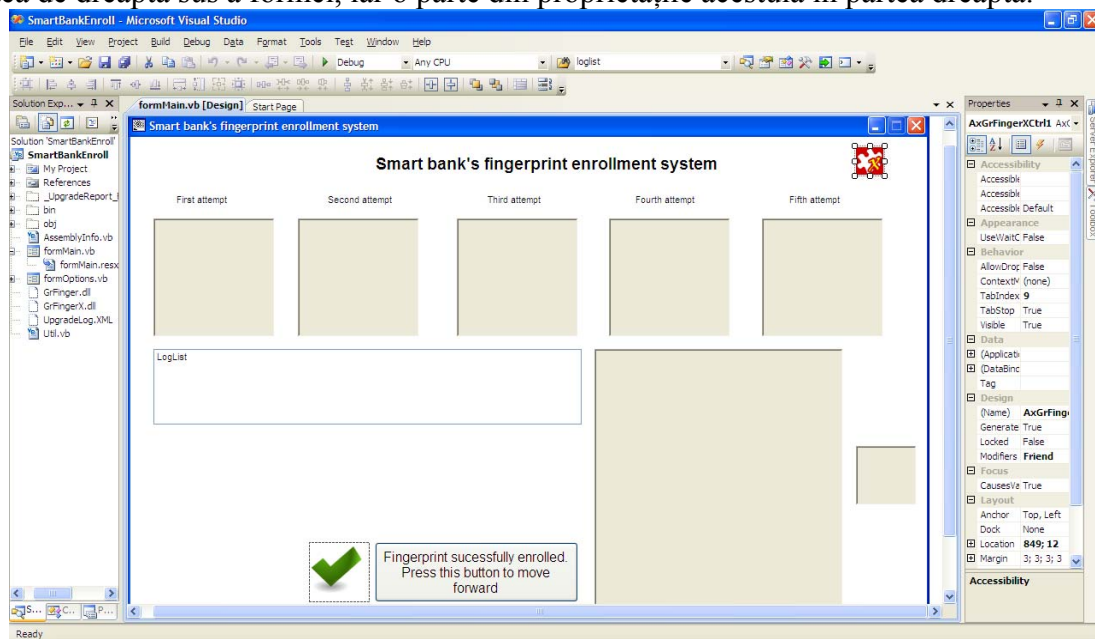


Figura 4.5. Pagina mediului de programare Visual Studio 2008, cu aplicația de înregistrare a persoanelor

Această aplicație a fost prezentată la conferința internațională ECAI 2015 (Electronics, Computers and Artificial Intelligence, 25-27 iunie 2015, București), articolul fiind indexat în IEEE Xplore și Thomson-Reuters Web of Science (ISI).

Ideea presupune preluarea a cinci amprente ale aceluiași deget, verificarea tuturor amprentelor, atât din punct de vedere al acurateții informației utile ce se poate extrage cât și prin verificarea între ele, două câte două, pentru a se determina dacă aparțin aceluiași deget.

La rularea aplicației, se afișează fereastra din figura 4.6:

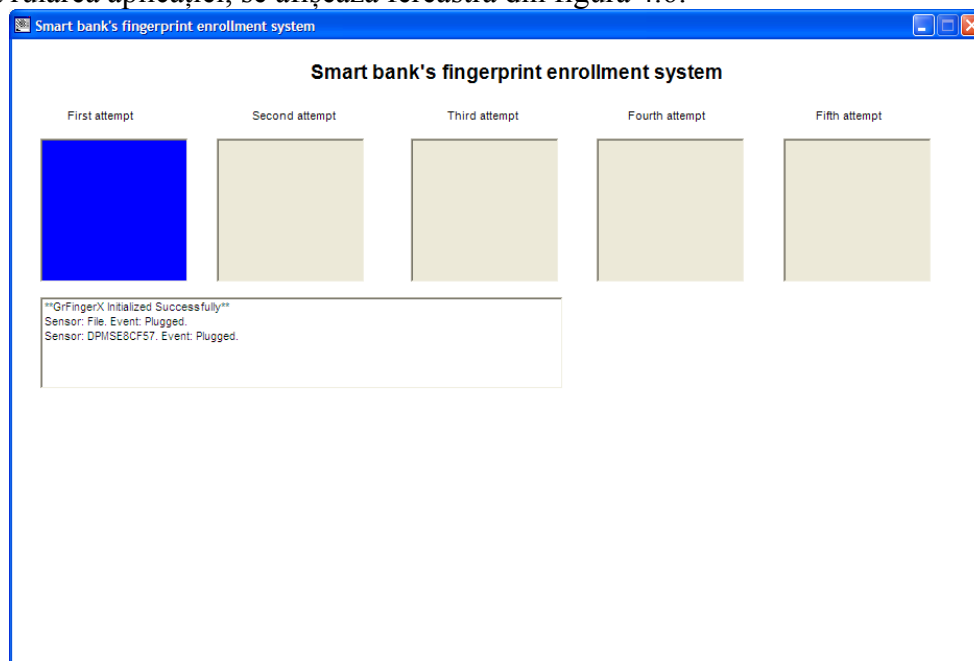


Figura 4.6. Pagina principală a aplicației, înainte de preluarea primei amprente

După ce senzorul sesizează prezența unui deget, scanează amprenta acestuia și o afișează în partea din dreapta jos a ferestrei, după cum se poate observa și în figura 4.7.

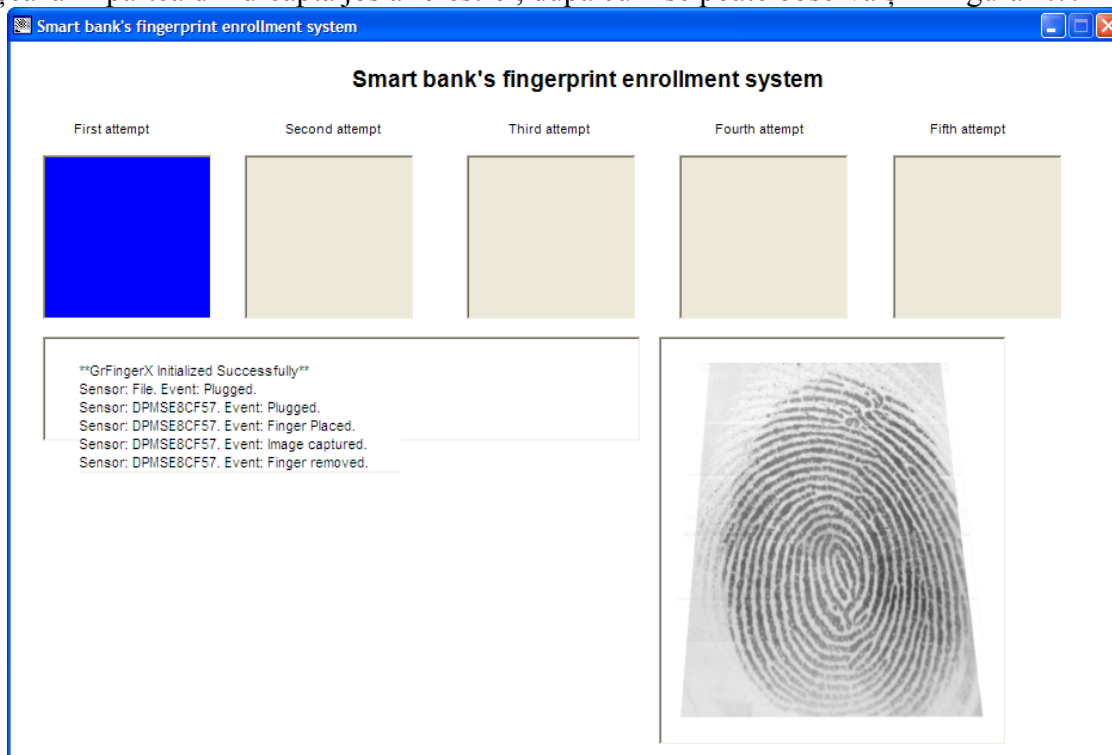


Figura 4.7. Afișarea imaginii preluate de la senzor

După ce sunt preluate cele 5 impresiuni ale amprentelor, acestea sunt verificate și în cazul în care verificarea este reușită se va afișa un buton în partea din stânga jos, după cum se poate observa în figura 4.8.

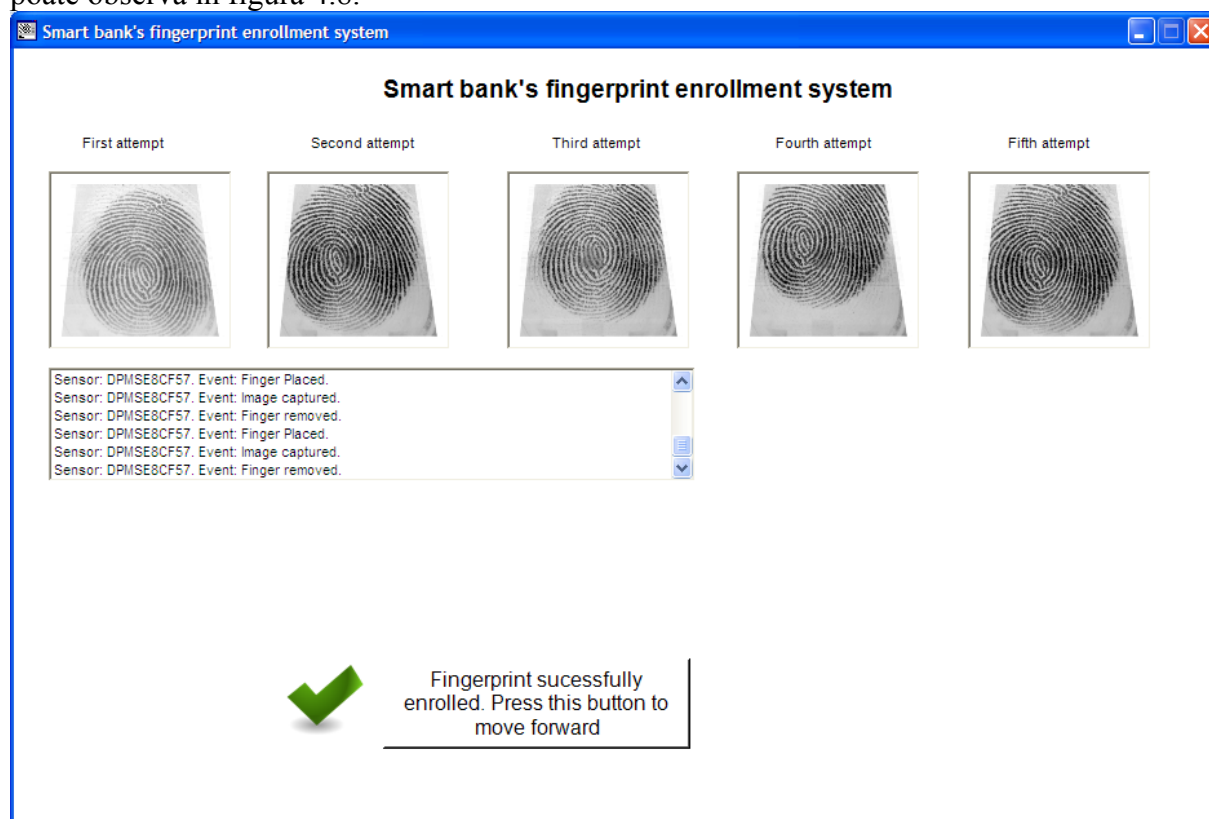


Figura 4.8. Fereastra de achiziție a imaginilor după terminarea preluării acestora

De asemenea, se poate observa faptul că aplicația furnizează și un log cu evenimentele apărute în timpul funcționării.

4.4.2. Aplicații și dispozitive pentru Android

Din punctul de vedere al aplicațiilor disponibile pentru sistemul de operare Android instalat pe smart-phone-uri sau pe tablete, problema identificării sau verificării persoanelor cu ajutorul amprentei digitale poate fi privit din trei puncte de vedere:

- anumite dispozitive vin dotate din fabrică cu un senzor de amprentă, ceea ce include și faptul că dispun inclusiv de software-ul necesar pentru recunoașterea utilizatorului;
- în cazul în care dispozitivul nu dispune de așa ceva, se pot imagina cel puțin două scenarii în acest sens:
 - se poate utiliza un software specializat care folosește imaginile amprentelor preluate de la camera din spate a telefonului pentru identificare (ICE Unlock, prezentată mai jos);
 - se poate atașa un dispozitiv de tip dongle pe portul de microUSB al dispozitivului, în vederea preluării amprentei și transmiterii acesteia către dispozitiv în scopul de a fi utilizată de o aplicație pentru recunoașterea persoanelor după amprentă; o altă idee ar fi transmiterea informației prin bluetooth sau NFC.

Din aceste scenarii prezentate, cel mai ieftin și care nu necesită cumpărarea unui dispozitiv specializat, este reprezentat de aplicația ICE Unlock Fingerprint Scanner, dezvoltată de firma Diamond Fortress Technologies, care folosește tehnologia Onyx.

La instalarea aplicației se cere configurarea unui PIN, care va fi folosit în cazul în care camera din spate și blitzul integrat nu sunt disponibile (de exemplu în cazul descărcării bateriei, când toate facilitățile sunt reduse la minimum). După configurarea PIN-ului, se cere alegerea unui deget pentru care se va stoca amprenta. După alegerea degetului, se va intra în modul de înregistrare a utilizatorului (enrollment).

După ce sunt preluate 5 imagini ale amprentelor, se mai ia o imagine suplimentară pentru verificare cu acestea. Dacă verificarea atinge un prag satisfăcător, atunci înregistrarea este considerată terminată.

În figurile 4.9 și 4.10 sunt prezentate două capturi de ecran din timpul funcționării aplicației, prima referindu-se la procesul de achiziție a imaginii amprentei utilizatorului iar a doua la amprente supuse verificării.

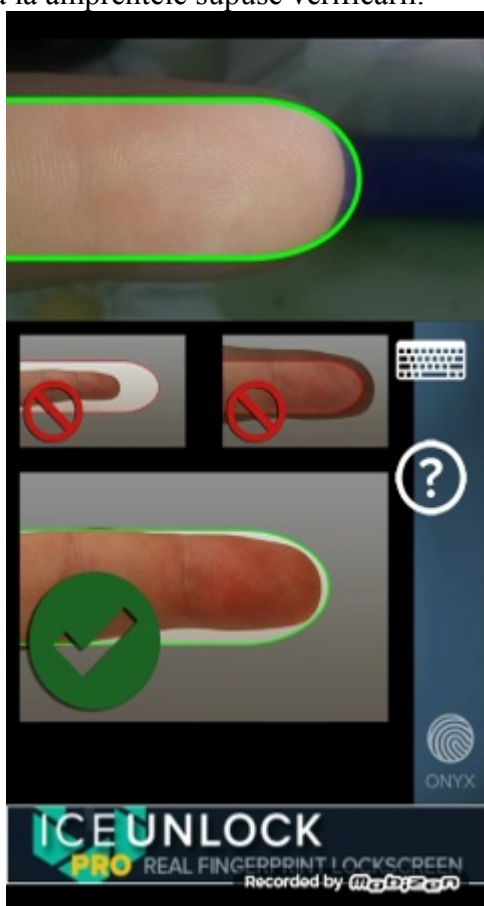


Figura 4.9. Funcționare aplicației



Figura 4.10. Verificarea amprentelor

O altă posibilitate de folosire a amprentei pentru autentificarea pe dispozitive de tip Android îl reprezintă achiziționarea unui dispozitiv de tip dongle, cum ar fi cel prezentat în figura 4.11.



Figura 4.11. Dispozitiv dongle pentru conectarea la dispozitive Android prin microUSB

Dezavantajele evidente sunt reprezentate de faptul că utilizatorul trebuie să achiziționeze un dispozitiv în plus și de faptul că acesta trebuie conectat la portul microUSB al dispozitivului, în acest fel creând dezavantaje în ceea ce privește utilizarea bateriei și faptul că trebuie să fie tot timpul în posesia utilizatorului în cazul în care nu este conectat.

O soluție practică ce va fi avută în vedere în cercetările viitoare este reprezentată de un astfel de dispozitiv, dar care să transmită informația prin bluetooth sau NFC.

4.5. Modulul Arduino Mega 2560 și senzori pentru înregistrarea utilizatorilor și pentru acordarea accesului la aplicații de internet banking

Sistemul folosește un modul Arduino Mega 2560, la care este conectată mai mulți senzori, ce vor fi detaliați în continuare. Acest sistem își propune sporirea securității pentru accesul la aplicații de internet banking. Astfel, se pornește de la ideea unui token care generează un anumit cod format din 6 cifre, după introducerea unui PIN stabilit de utilizator. Acest lucru este utilizat și în cadrul acestui proiect, dar pe lângă generarea unui cod OTP (One Time Password) se mai adaugă și recunoașterea persoanelor după iris și amprentă.

Schema de principiu a acestui sistem este prezentată în figura 4.12.

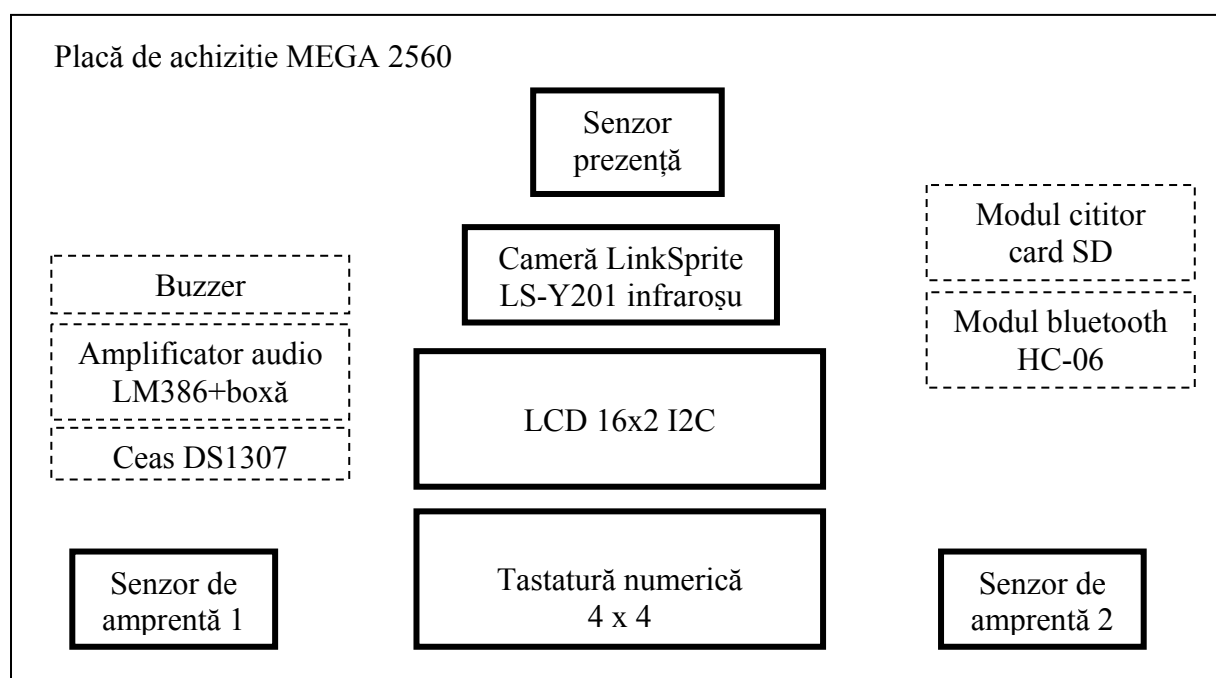


Figura 4.12. Schema de principiu a sistemului propus

Dispozitivele utilizate pentru realizarea proiectului sunt prezentate în figura 4.13. Pornind de la schema de mai sus, se pot identifica foarte ușor componentele din această figură. Figura conține dispozitivele utilizate neconectate la placa de dezvoltare Arduino Mega 2560.

În figura 4.14 sunt senzorii conectați pe un breadboard ce interacționează cu placa de dezvoltare. S-a ales utilizarea unui breadboard din cauza numărului mare de senzori, care necesită fiecare o alimentare. De asemenea, doi dintre senzori folosesc pentru conectare doar doi pini în afară de alimentare, tehnologie denumită I2C (sau IIC – Inter-Integrated Circuit).

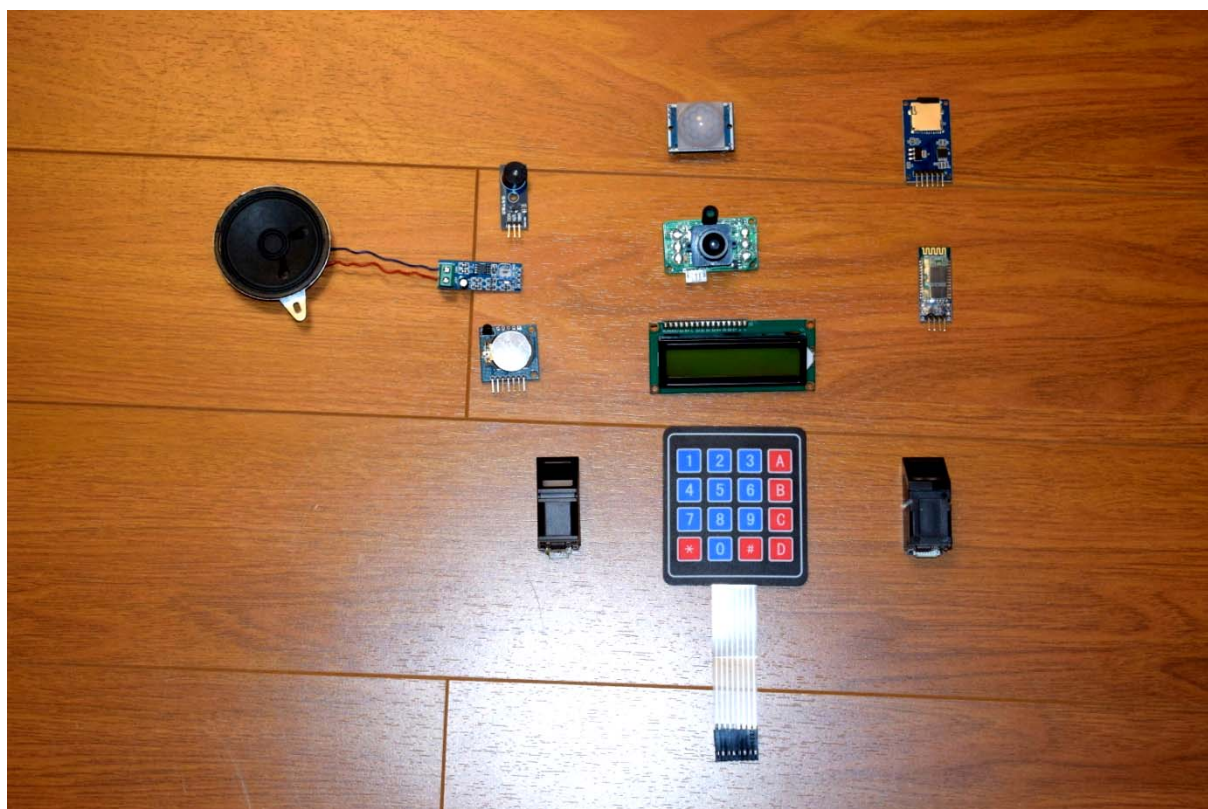


Figura 4.13. Senzorii utilizați, înainte de conectare

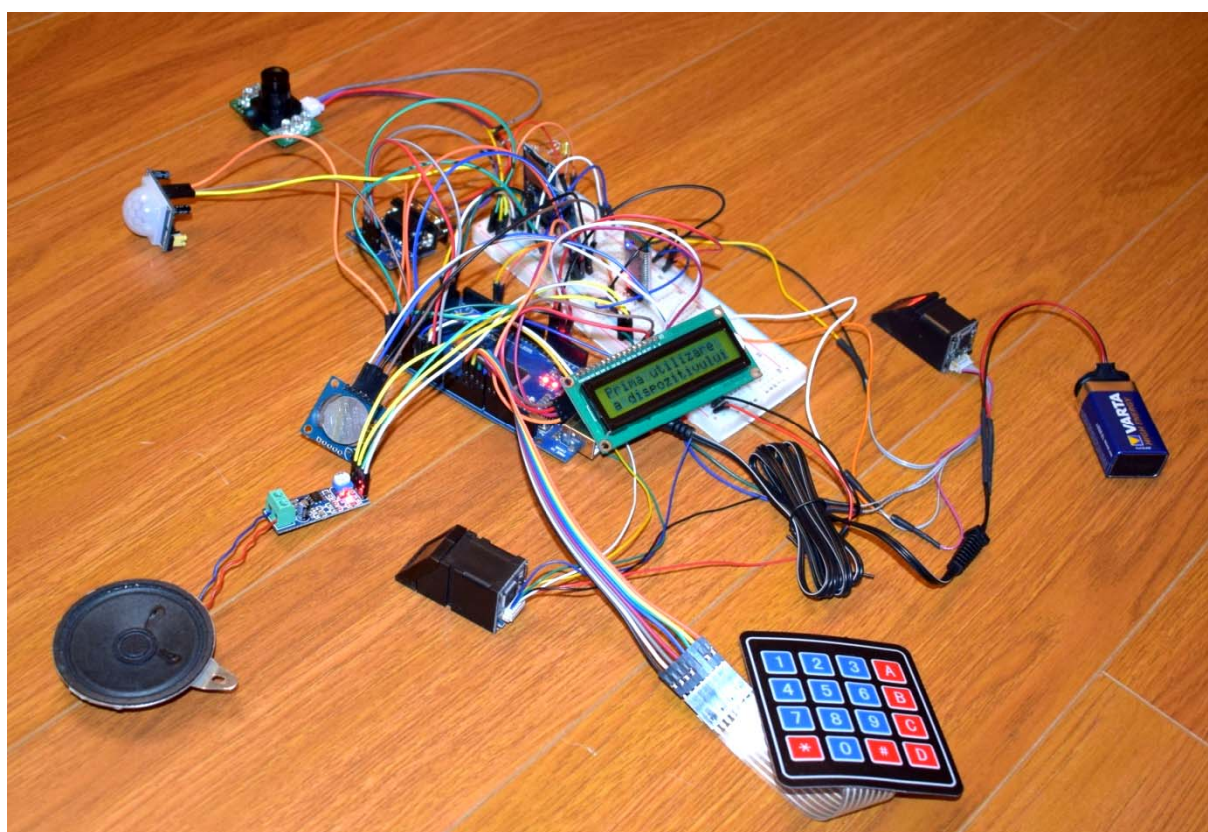


Figura 4.14. Senzorii conectați la modulul de dezvoltare Arduino Mega 2560

În continuarea capitolului sunt fi prezentați senzorii care alcătuiesc sistemul.

Utilizarea modului Arduino Mega 2560 și a senzorilor conectați la acesta pentru înregistrarea sau acordarea accesului utilizatorilor la aplicații de internet banking este prezentată în continuarea capitolului

În schema logică din figura 4.15 se prezintă etapele parcurse pentru inițializarea comunicației între modulul de dezvoltare Arduino Mega 2560 și senzorii care sunt conectați la acesta.

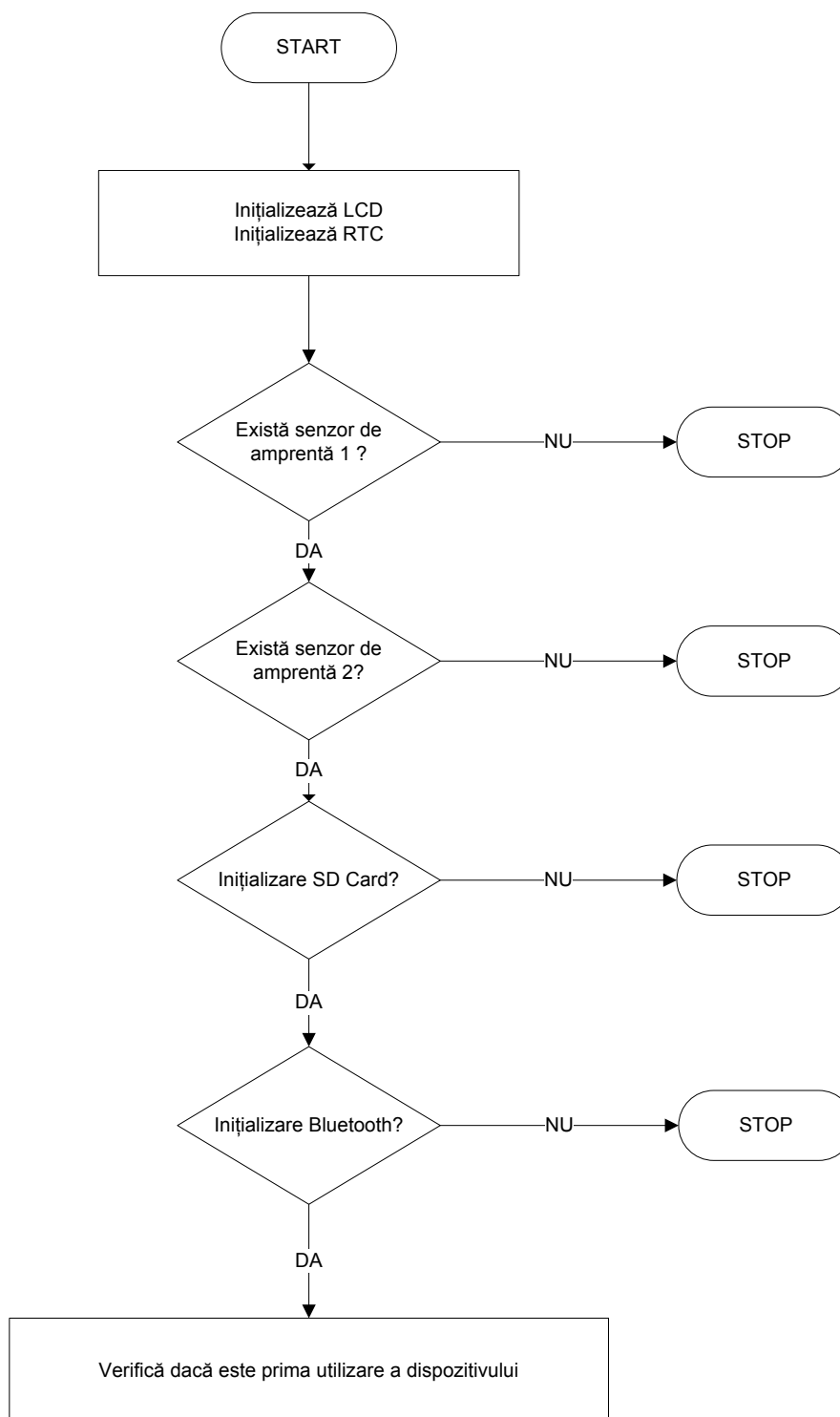


Figura 4.15. Schema logică de inițializare a aplicației

În cazul primei utilizări a dispozitivului (determinată prin citirea valorii 1 de la poziția 2003 din EEPROM) se va trece la înregistrarea utilizatorului, conform schemei logice din figura 4.16.

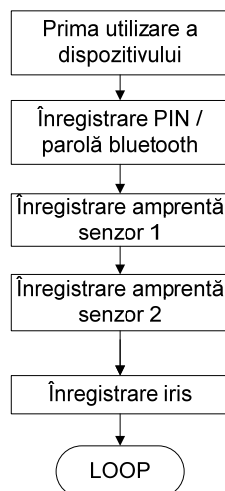


Figura 4.16. Schema logică pentru prima utilizare a dispozitivului

Scenariul de înregistrare este următorul:

- funcționarul de la bancă se conectează la aplicația de înregistrare a dispozitivului de pe serverul băncii;
- se realizează comunicația prin bluetooth cu dispozitivul;
- se stabilește o parolă din 4 cifre pentru PIN și pentru comunicația cu bluetooth;
- se înregistrează amprenta de pe senzorul 1 apoi de pe senzorul 2;
- se înregistrează irisul folosind camera LinkSprite LS-Y201;
- funcționarul se deconectează de la bluetooth și de la aplicația de înregistrare și configurează telefonul clientului pentru realizarea conexiunii prin bluetooth.

În urma înregistrării sau în cazul în care nu este prima utilizare a dispozitivului, se intră în bucla LOOP, unde se așteaptă evenimente de la portul serial, bluetooth sau tastatură. La primirea unui eveniment pe oricare dintre aceste căi, se procesează evenimentul respectiv. În cazul în care dispozitivul nu este utilizat pentru 5 minute, acesta va intra în stand-by. Schema logică a acestui proces este prezentată în figura 4.17.

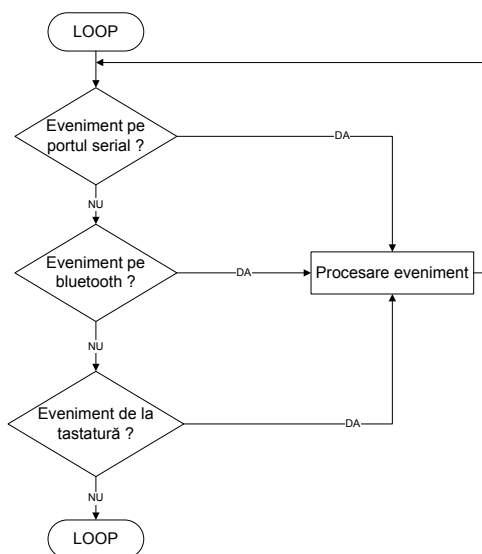


Figura 4.17. Așteptarea evenimentelor în bucla LOOP

Pentru procesarea evenimentelor se folosește schema logică din figura 4.18:

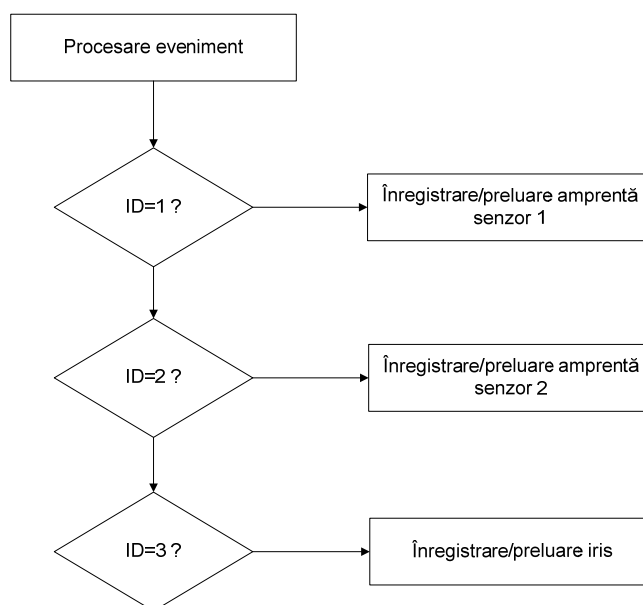


Figura 4.18. *Procesarea evenimentelor*

Securitatea sistemului este asigurată de mai multe verificări, printre care cele mai importante ar fi:

- se verifică adresa MAC a dispozitivului bluetooth cu cea înregistrată în baza de date;
- se citesc anumite valori din memoria EEPROM, de la adrese prestabilite, pentru a se observa dacă sunt identice cu cheia privată a utilizatorului stocată pe server.

O parte importantă a cercetărilor din acest capitol a fost publicată în articolele [59], [60], [64]-[66].

4.6. Concluzii și contribuții

Acest capitol conține principalele studii ale autorului tezei asupra sistemelor integrate ce pot fi utilizate în vederea securizării accesului la aplicații de internet banking. În acest domeniu nevoia de securizare a accesului utilizatorilor sau a angajaților băncii reprezintă un obiectiv foarte important, având în vedere faptul că tentativele de fraudare sunt foarte frecvente, iar în cazul în care se reușește acest lucru consecințele pot fi foarte importante.

În scopul securizării accesului la aplicații de internet banking, am adus următoarele contribuții practice:

- folosind funcțiile prezentate în Capitolul 2, s-a realizat o aplicație pentru înregistrarea irisului utilizatorului care dorește să fie înregistrat într-o aplicație de internet banking;
- pagina de autentificare în sistemul de internet banking al Băncii Transilvania a fost „clonată”, adăugându-se un modul de identificare a utilizatorului prin intermediul irisului; în acest scop s-au utilizat, de asemenea, funcții discutate în Capitolul 2;
- s-a realizat o aplicație standalone pentru înregistrarea utilizatorilor prin utilizarea amprente digitale, folosind mediul de programare Visual Studio; în realizarea aplicației s-au folosit informațiile prezentate în Capitolul 3;

- s-a dezvoltat o aplicație complexă, folosind modulul Arduino Mega 2560 și mai mulți senzori atașați la acesta, printre care doi senzori de amprentă, o cameră pentru preluarea imaginilor în infraroșu, o tastatură și un modul bluetooth ce permite comunicarea între acest dispozitiv și un dispozitiv mobil sau un sistem desktop/laptop. Aplicația dezvoltată poate fi utilizată pentru înregistrarea sau autentificarea la un sistem de internet banking, prin introducerea caracteristicilor biometrice reprezentate de iris și amprentă, pe lângă modalitățile clasice de autentificare, bazate pe nume de utilizator și o parolă generată de un token. Aplicația și dispozitivul au doar rolul de a prelua irisul sau amprenta, acestea fiind transmise prin bluetooth în vederea prelucrării pe un dispozitiv mobil sau de tip laptop. Analiza și extragerea caracteristicilor biometrice nu se poate face pe dispozitivul Arduino Mega 2560 din cauza frecvenței mici a procesorului (12 MHz) și a spațiului relativ foarte mic al memoriei. Prelucrarea imaginilor obținute de la dispozitiv se poate face utilizând informațiile din cadrul Capitolelor 2 și 3.

CAPITOLUL V. Concluzii finale, contribuții și direcții viitoare de cercetare

5.1. Concluzii finale

În cadrul cercetărilor efectuate în cadrul tezei s-au analizat soluțiile disponibile pentru recunoașterea persoanelor după iris și amprentă, atât din punctul de vedere al senzorilor utilizați cât și în ceea ce privește algoritmi folosiți.

Studiarea referințelor bibliografice a reprezentat un adevărat ajutor în înțelegerea provocărilor din acest domeniu, precum și pentru a face diferența între diversele abordări în ceea ce privește recunoașterea persoanelor după iris și amprentă.

Pentru a ajunge la obiectivul studiului, s-a analizat mai întâi stadiul actual privind tehnologiile biometrice. S-a efectuat un studiu amplu asupra recunoașterii persoanelor după iris și amprentă. Astfel, în [Capitolul I](#) s-a realizat o introducere în domeniul recunoașterii persoanelor prin utilizarea tehnologiilor biometrice. La începutul capitolului s-a analizat funcționarea sistemelor biometrice, prin prezentarea modulelor componente ale acestora. În continuare s-a insistat pe diferențele între verificare și identificare, precum și pe performanțele sistemelor biometrice. Aplicațiile biometriei sunt foarte diverse și o parte dintre ele se regăsesc în cadrul acestui capitol.

Referitor la stadiul actual al recunoașterii persoanelor după iris, s-au studiat mai multe articole iar principalele contribuții ale acestora au fost redate în paragraful 1.6. De asemenea, au fost introduse informații despre structura ochiului uman și a irisului, precum și date despre senzorii utilizați în preluarea imaginilor. Partea a doua a acestui paragraf realizează o introducere în recunoașterea persoanelor după iris, plecând de la lucrarea de bază a cercetătorului britanic de la Universitatea din Cambridge, John Daugman, continuând cu o altă abordare a lui Richard Wildes și terminând cu o serie de articole foarte recente, care abordează diverse problematice referitoare la această modalitate de recunoaștere a persoanelor prin utilizarea irisului.

În ultima parte a capitolului se realizează o introducere în recunoașterea persoanelor după amprenta digitală. Acest subiect a fost studiat de foarte mult timp și de mulți cercetători. La fel ca și în cazul recunoașterii după iris, sunt prezentați principalii senzori utilizați în preluarea imaginilor amprentelor. În continuare se realizează o analiză asupra articolelor de referință din acest domeniu foarte vast al recunoașterii persoanelor după amprenta digitală.

Unele dintre articolele din acest capitol vor fi utilizate în dezvoltarea ulterioară a unor aplicații care vor fi prezentate în cadrul tezei de doctorat. De asemenea, acestea constituie un punct de plecare în abordarea domeniului foarte vast al recunoașterii persoanelor după iris și amprentă.

În [Capitolul II](#) s-a studiat recunoașterea persoanelor după iris, care reprezintă un domeniu relativ nou și în care cercetările continuă într-un ritm foarte alert. Prima parte a acestui capitol face o scurtă introducere în acest domeniu, prin menționarea celor mai importante contribuții ale autorilor John Daugman, Richard Wildes și Wu Zhi-Li. Capitolul continuă cu descrierea etapelor care sunt parcurse pentru îndeplinirea dezideratului propus, plecând de la preluarea imaginii ochiului de la o cameră sau dintr-un fișier. Următorii pași presupun efectuarea de prelucrări grafice asupra acestora în vederea îmbunătățirii calității caracteristicilor de extras. Se continuă cu segmentarea și normalizarea imaginii, iar în cele din urmă se obține codul iris care poate fi folosit pentru stocarea într-o bază de date sau pentru faza de potrivire, care este analizată în continuarea capitolului. Succesiunea pașilor parcurși a fost descrisă în prima parte a capitolului și va fi utilizată în dezvoltarea ulterioară de aplicații pentru recunoașterea persoanelor după caracteristicile irisului.

Partea a doua a capitolului conține date și informații importante despre dispozitivele pentru preluarea imaginii irisului, insistându-se pe funcțiile oferite de către camera Panasonic BM-ET100US, ce a fost folosită în cadrul cercetărilor din cadrul tezei de doctorat. În timpul cercetărilor s-au descoperit facilități ale acestei camere nedocumentate de către producător, cum ar fi faptul că imaginile preluate pot fi stocate în fișiere de tip bitmap într-un folder de pe calculatorul pe care aceasta a fost instalată. O parte din funcții sunt descrise detaliat în cadrul Anexei 1. O parte din acest capitol a fost publicată în articolele [62] și [65]. Această parte a capitolului poate duce la posibilitatea de utilizare la un nivel superior a facilităților oferite de camera Panasonic BM-ET100US.

În **Capitolul III** sunt descriși la început principalii pași parcurși în recunoașterea persoanelor după amprenta digitală. Partea a doua a capitolului conține o propunere de adoptare a unei noi scheme pentru acest scop. S-a propus o nouă schemă de recunoaștere, urmată de implementarea acesteia în cadrul unei aplicații MatLab. Ultima parte a capitolului conține principalele contribuții în ceea ce privește utilizarea teoriei grafurilor pentru potrivirea amprentelor digitale.

Capitolul IV conține principalele studii ale autorului tezei asupra sistemelor integrate ce pot fi utilizate în vederea securizării accesului la aplicații de internet banking. În acest domeniu nevoia de securizare a accesului utilizatorilor sau a angajaților băncii reprezintă un obiectiv foarte important, având în vedere faptul că tentativele de fraudare sunt foarte frecvente, iar în cazul în care se reușește acest lucru consecințele pot fi foarte importante.

În continuare vor fi prezentate principalele contribuții aduse de autor în domeniul cercetat în cadrul tezei de doctorat.

5.2. Contribuții

În această lucrare au fost prezentate metode și sisteme pentru identificarea și recunoașterea persoanelor, după iris (**Capitolul II**) și amprenta digitală (**Capitolul III**). În continuare se va prezenta, pentru fiecare capitol în parte, contribuțiile autorului la dezvoltarea acestui domeniu de actualitate. Rezultatele au fost valorificate prin publicarea a 10 articole pe tema tezei de doctorat (ca prim sau unic autor), în cadrul a diverse conferințe și publicații. Dintre aceste articole, două sunt indexate în baza de date Thomson Web of Science (ISI).

Principalele **contribuții teoretice** prezentate în această teză sunt:

- elaborarea unui studiu aprofundat asupra articolelor importante în domeniul recunoașterii persoanelor după iris și amprentă, în cadrul prezentării stadiului actual al cercetărilor din acest domeniu;
- s-a propus adoptarea unei noi scheme de recunoaștere a persoanelor după amprentă, după analizarea altor două metode propuse de autori;
- s-a propus un algoritm euristic pentru potrivirea amprentelor digitale folosind grafurile, prin aceasta reducându-se semnificativ timpul de execuție, datorită scăderii ordinului de complexitate;
- propunerea unei metode de determinare a punctului de referință pentru alinierea punctelor caracteristice ale amprente digitale.

Dintre **contribuțiile practice**, cele mai importante sunt:

- analiza succesiunii pașilor parcurși și descriși în prima parte a **Capitolelor 2 și 3**, ce poate fi utilizată în dezvoltarea ulterioară de aplicații pentru recunoașterea persoanelor după caracteristicile irisului sau ale amprente digitale;
- prin analizarea funcțiilor puse la dispoziție de către producătorul camerei Panasonic BM-ET100US și nedocumentate s-a ajuns la posibilitatea de utilizare la un nivel

- superior a facilităților oferite de cameră;
- în urma cercetărilor efectuate, s-a realizat o aplicație în mediul de programare MatLab, plecând de la schema propusă în cadrul tezei și utilizată în scopul validării practice a contribuției teoretice;
 - analizarea rezultatelor aplicării mai multor operatori asupra unei imagini de test a amprente digitale, în vederea vizualizării diferențelor între ei și pentru alegerea celui optim în fiecare caz.
 - folosind funcțiile prezentate în [Capitolul 2](#), s-a realizat o aplicație pentru înregistrarea irisului utilizatorului care dorește să fie înregistrat într-o aplicație de internet banking;
 - pagina de autentificare în sistemul de internet banking al Băncii Transilvania a fost „clonată”, adăugându-se un modul de identificare a utilizatorului prin intermediul irisului; în acest scop s-au utilizat, de asemenea, funcții discutate în [Capitolul 2](#);
 - ca urmare a cercetărilor din cadrul tezei s-a realizat o aplicație standalone pentru înregistrarea utilizatorilor prin utilizarea amprente digitale, folosind mediul de programare Visual Studio; în realizarea aplicației s-au folosit informațiile prezentate în [Capitolul 3](#);
 - în urma cercetărilor întreprinse s-a dezvoltat o aplicație complexă, folosind modulul Arduino Mega 2560 și mai mulți senzori atașați la acesta, printre care doi senzori de amprentă, o cameră pentru preluarea imaginilor în infraroșu, o tastatură și un modul bluetooth ce permite comunicarea între acest dispozitiv și un dispozitiv mobil sau un sistem desktop/laptop. Aplicația dezvoltată poate fi utilizată pentru înregistrarea sau autentificarea la un sistem de internet banking, prin introducerea caracteristicilor biometrice reprezentate de iris și amprentă, pe lângă modalitățile clasice de autentificare, bazate pe nume de utilizator și o parolă generată de un token. Aplicația și dispozitivul au doar rolul de a prelua irisul sau amprenta, acestea fiind transmise prin bluetooth în vederea prelucrării pe un dispozitiv mobil sau de tip laptop. Analiza și extragerea caracteristicilor biometrice nu se poate face pe dispozitivul Arduino Mega 2560 din cauza frecvenței mici a procesorului (12 MHz) și a spațiului relativ foarte mic al memoriei. Prelucrarea imaginilor obținute de la dispozitiv se poate face utilizând informațiile din cadrul [Capitolelor 2 și 3](#).

5.3. Diseminarea rezultatelor

O parte din rezultatele prezentate în această teză de doctorat au fost publicate în următoarele articole:

- **Cătălin Lupu**, Vasile-Gheorghiță Găitan, Valeriu Lupu, *Security enhancement of internet banking applications by using multimodal biometrics*, SAMI 2015, Herl'any, Slovacia, p. 47-52, ISBN 978-1-4799-8220-2, DOI: 10.1109/SAMI.2015.7061904 7301177 (*indexat IEEE Xplore și Thomson Reuters – ISI*)
- **Cătălin LUPU**, Vasile-Gheorghiță GĂITAN, Valeriu LUPU, „*Fingerprints used for security enhancement of online banking authentication process*”, IEEE 7th International Conference on Electronics, Computers and Artificial Intelligence – ECAI 2015, vol. 7, no. 1, 2015, p. 217-220, ISSN 1843-2115, ISBN 978-1-4673-6647-2 (PDF), 978-1-4673-6645-8 (DVD), 978-1-4673-6646-5 (Print), DOI 10.1109/ECAI.2015.7301177 (*indexat IEEE Xplore și Thomson Reuters – ISI*)
- **Catalin Lupu**, Valeriu Lupu, *The beginnings of using fingerprints as biometric characteristics for personal identification purposes*, Analele Universității

- „Contantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 3 / 2014, ISSN 1842-4856, B+ cod 718, p. 53-56 (*indexat EbscoHost*)
- **Cătălin Lupu**, Valeriu Lupu, *Biometrics used for authentication in internet-banking applications*, Analele Universității „Contantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 3 / 2014, ISSN 1842-4856, B+ cod 718, p. 57-63 (*indexat EbscoHost*)
 - **Cătălin Lupu**, *Development of optimal filters obtained through convolution methods, used for fingerprint image enhancement and restoration*, **The USV Annals of Economics and Public Administration, Section 5: Statistics, economic informatics and mathematics**, vol. 14, no. 2 (20)/2014, pg. 156-167, ISSN 2285-3332, Online ISSN 2344-3847 (*indexat EbscoHost*);
 - **Cătălin Lupu**, Vasile-Gheorghiiță Găitan, Valeriu Lupu, *Improving the Security of Internet Banking Applications by Using Multimodal Biometrics*, Journal of Applied Computer Science & Mathematics, no. 19 (9) /2015, Suceava, p. 37-42, ISSN 2066-4273 (*indexat EbscoHost*);
 - **Cătălin Lupu**, Valeriu Lupu, Gheorghe Gîlcă, “*Securing online banking services using iris recognition*”, Analele Universității „Contantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, CNCSIS B+ cod 718, p. 69-75 (*indexat EbscoHost*);
 - **Cătălin Lupu**, Valeriu Lupu, Gheorghe Gîlcă, “*Overview on a personal recognition system that uses iris images as main biometric characteristic*”, Analele Universității „Contantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, CNCSIS B+ cod 718, p. 76-79 (*indexat EbscoHost*);
 - Gheorghe Gîlcă, Nicu-George Bîzdoacă, **Cătălin Lupu**, “*Classification algorithms of facial expressions by using the feedforward neural networks*”, Analele Universității „Contantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, CNCSIS B+ cod 718, p. 80-85 (*indexat EbscoHost*);
 - Gheorghe Gîlcă, Nicu-George Bîzdoacă, **Cătălin Lupu**, “*Artificial vision algorithms based on fractals for the image description*”, Analele Universității „Contantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, CNCSIS B+ cod 718, p. 86-90 (*indexat EbscoHost*).

5.4. Direcții viitoare de cercetare privind tehnologiile biometrice

Printre principalele direcții viitoare de cercetare se pot aminti:

- securizarea accesului într-un automobil;
- crearea unei baze de date pentru identificarea persoanelor în cazul solicitării ambulanței la accidente rutiere sau pentru transportul unor persoane a căror identitate nu este cunoscută, împreună cu înregistrarea într-o bază de date centrală a istoricului medical al fiecărei persoane;
- securizarea dispozitivelor de identificare: pașaport biometric, carte de identitate, permis de conducere.

BIBLIOGRAFIE

- [1] ROSS, Arun A.; NANDAKUMAR, Karthik; JAIN, Anil K., „*Handbook of multibiometrics*”, Springer Science & Business Media, ISBN 978-0-387-22296-7, 2006
- [2] BERTILLON, Alphonse, „*Identification anthropométrique – Instructions signalétiques*”, Melun, Imprimerie administrative, 1893
- [3] BERTILLON, Alphonse, „*De l'identification par les signalements anthropométriques*”, în cadrul „Archives de l'anthropologie criminelle et des sciences pénales”, p. 272-299, 1887
- [4] SWETS, John A.; TANNER JR, Wilson P.; BIRDSALL, Theodore G., „*Decision processes in perception*”, în Psychological review, vol. 68, nr. 5, p. 301-340, DOI 10.1037/H0040547, 1961
- [5] POH, Norman; BENGIO, Samy, „*F-ratio Client-Dependent Normalisation on Biometric Authentication Tasks*”, Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), volum 1, pg. 721-724, Philadelphia, SUA, ISBN 0-7803-8874-7, DOI 10.1109/ICASSP.2005.1415215, 2005
- [6] <https://ampletrails.com/identix-k30-essl> (accesat la 23.05.2017)
- [7] <https://www.schiphol.nl/en/privium/> (accesat la 23.05.2017)
- [8] <http://www.haaretz.com/israel-news/1.657425> (accesat la 23.05.2017)
- [9] <https://www.atmmarketplace.com/articles/atm-security-in-asia-moves-to-veins/> (accesat la 23.05.2017)
- [10] <http://www.chron.com/business/article/Shoppers-can-now-pay-with-fingerprint-at-Kroger-2058416.php> (accesat la 23.05.2017)
- [11] <https://www.secureidnews.com/news-item/biometrics-at-the-disney-gates/> (accesat la 23.05.2017)
- [12] <http://www.dhs.gov/usvisit> (accesat la 23.05.2017)
- [13] FLOM, Leonard; SAFIR, Aran, „*Iris recognition system*”, patent nr. US 4,641,349, 1987
- [14] DAUGMAN, John, „*Biometric personal identification system based on iris analysis*”, patent nr. US 5,291,560, Iri Scan Inc., 1994
- [15] DAUGMAN, John, „*How iris recognition works*”, Proceedings of 2002 International Conference on Image Processing, Vol. 1, ISSN 1051-8215, p. I-33 – I-36, DOI 10.1109/ICIP.2002.1037952, 2002

- [16] WILDES, Richard P., "*Iris recognition: an emerging biometric technology*", Proceedings of the IEEE, 1997, vol. 85, nr. 9, p. 1348-1363., ISSN 0018-9219, DOI 10.1109/5.628669, 1997
- [17] MATSUSHITA, Mitsuji, "*Iris identification system and iris identification method*", patent US 5,901,238, Oki Electric Industry Co. Ltd, 1999.
- [18] HARUO, Ito, "*Iris Information Acquisition apparatus ad iris identification apparatus*", patent nr. 6.526.160 B1, Media Technology Corp., 2003
- [19] VATSA, Mayank; SINGH, Richa; NOORE, Afzel, "*Improving Iris Recognition Performance Using Segmentation, Quality Enhancement, Match Score Fusion, and Indexing*", IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, p. 1021-1035, ISSN 1083-4419, DOI 10.1109/TSMCB.2008.922059, 2008
- [20] HAMZA, Rida M., "*Distance iris recognition*", patent nr. US 7,593,550, Honeywell International Inc., 2009
- [21] TAMURA, Hideyuki, "*A comparison of line thinning algorithms from digital geometry viewpoint*", in Proc. of 4th Int. Joint Conf. on Pattern Recognition, Kyoto, Japan, pg. 715-719, 1978
- [22] RADU, Petru; SIRLANTZIS, K.; HOWELLS, W.G.J.; HOQUE, S.; DERAVID, F., "*Optimizing 2D Gabor filters for iris recognition*", Fourth International Conference on Emerging Security Technologies, p. 47-50, DOI 10.1109/EST.2013.15, 2013
- [23] YADAV, Daksha; DOYLE, James Jr.; VATSA, Mayank, "*Unraveling the effect of textured contact lenses on iris recognition*", IEEE Transactions on information forensics and security, vol. 9, no. 5, p. 851-862, ISSN 1556-6013, DOI 10.1109/TIFS.2014.2313025, 2014
- [24] OTHMAN, Nadia; DORIZZI, Bernadette, "*Impact of Quality-Based Fusion Techniques for Video-Based Iris Recognition at a Distance*", IEEE Transactions on Information Forensics and Security, Volumul 10, nr. 8, p. 1590-1602, ISSN 1556-6013, DOI 10.1109/TIFS.2015.2421314, 2015
- [25] ALI, Lasker Ershad; LUO, Junfeng; MA, Jinwen, "*Iris Recognition from Distant Images Based on Multiple Feature Descriptors and Classifiers*", ICSP2016, p. 1357-1362, ISBN 978-1-5090-1344-9, DOI 10.1109/ICSP.2016.7878048, 2016
- [26] GALDI, Chiara; DUGELAY, Jean-Luc, "*Fusing Iris Colour and Texture information for fast iris recognition on mobile devices*", 2016 23rd International Conference on Pattern Recognition (ICPR), p. 160-164, ISBN 978-1-5090-4847-2, DOI 10.1109/ICPR.2016.7899626, 2016
- [27] ANDERSEN-HOPPE, Esbern; RATHGEB, Christian; BUSCH, Christoph, "*Combining Multiple Iris Texture Features for Unconstrained Recognition in Visible Wavelengths*", 2017 5th International Workshop on Biometrics and Forensics (IWBF), ISBN 978-1-5090-5791-7, DOI 10.1109/IWBF.2017.7935090, 2017
- [28] CZAJKA, Adam; BOWYER, Kevin W.; KRUMDICK, Michael; VIDAL MATA, Rosaura G., "*Recognition of image-orientation-based iris spoofing*", IEEE Transactions on Information Forensics and Security, vol. 12, issue 9, p. 2184-2196, ISSN 1556-6013, DOI 10.1109/TIFS.2017.2701332, 2017
- [29] MALTONI, Davide; MAIO, Dario; JAIN, Anil K.; PRABHAKAR, Salil, "*Handbook*

- of Fingerprint Recognition*”, Springer, ISBN 978-1-84882-253-5, 2003
- [30] BOLDEA, Maria; BOLDEA, Costin Radu, „*Identificare biometrică*”, Revista *Informatică Economică*, nr. 1(25)/2003, pg. 78-82, ISSN 1453-1305, 2003
 - [31] GALTON, Francis, „*Finger Prints*”, Editura Macmillan and Co., Londra, 1892
 - [32] PĂȘESCU, Gheorghe; CONSTANTIN, Ion. R., „*Secretele amprentelor papilare*”, Editura Național, ISBN 973-97574-0-5, 1996
 - [33] NALINI, K. Ratha, „*Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images*”, ISSN 0031-3203 (95), p. 1657-1672, DOI 10.1016/0031-3203(95)00039-3, 1995
 - [34] FARINA, Alessandro; ZSOLT, M. Kovacs-Vajna; LEONE, Alberto, „*Fingerprint minutiae extraction from skeletonized binary images*”, Pattern recognition, vol. 32, nr. 5, p. 877-889, ISSN 0031-3203, DOI 10.1016/S0031-3203(98)00107-1, 1999
 - [35] ORT, James R., et. al, „*Fingerprint identification system*”, patent nr. US 5.926.555, Calspan Corporation, 1999
 - [36] SENIOR, A., „*System and method for transforming fingerprints to improve recognition*”, patent nr. US 6.466.686, International Business Machines Corporation, 2002
 - [37] DASS, Sarat C.; JAIN, Anil K., „*Fingerprint classification Using Oriented Field Flow Curves*”, ICVGIP Proceedings, p. 650-655, ISBN 81-7764-707-5, 2004
 - [38] LORENZO, Víctor López, ș.a., „*Fingerprint Minutiae Extraction Based On FPGA and MatLab*”, XXth Conference on Design of Circuits and Integrated Systems (DCIS 2005), Lisaboana Portugalia, ISBN 972-99387-2-5, 2005
 - [39] COVA, Jean-François; CHEVALIER, Frédéric, „*Method for identification of person by recognition of a digital fingerprint*”, Patent nr. US 7,596,248, SAGEM Sécurité, 2009
 - [40] PIZER, Stephen, ș.a., „*Adaptive histogram equalization and its variations*”, Computer Vision, Graphics, and Image Processing, Volum 39, nr. 3, pag. 355–368, ISSN 0734-189X, 1987
 - [41] GELLERT, Arpad; BRAD, Remus, „*Procesarea imaginilor – Aplicații (suport de curs)*”, Universitatea „Lucian Blaga” din Sibiu, (<http://webpace.ulbsibiu.ro/arpad.gellert/html/PI.pdf>, accesat la 23.05.2017)
 - [42] MARITA, Tiberiu, „*Procesarea imaginilor (Suport de curs)*”, Universitatea Tehnică din Cluj (<http://users.utcluj.ro/~tmarita/IPL/IPCurs/IPCurs.htm>, accesat la 23.05.2017)
 - [43] MASEK, Libor, „*Recognition of Human Iris Patterns for Biometric Identification*”, raport tehnic, Universitatea Australiei de Vest, 2003
 - [44] *IrisGuard EyeBank Solution Brochure* – <http://www.irisguard.com/eyebank/downloads/EyeBankPer%20Page.pdf>, pg. 7 (accesat la 23.05.2017)
 - [45] <http://bias.csr.unibo.it/fvc2002> (accesat la 23.05.2017)
 - [46] WU, Zhili, *Fingerprint recognition*, Teză de licență, Hong Kong Baptist University, Aprilie 2002
 - [47] YEO, Thomas, TAY, Wee Peng, TAI, Ying Yu, *Image Systems engineering Program*, proiect, Universitatea Stanford, 2008

- [48] JAIN, Lakhmi, ș.a., *"Intelligent biometric techniques în fingerprint and face recognition"*, The CRC Press, ISBN 978-0-849-32055-2, 1999
- [49] POPA, Mircea Virgil; DEMETER, Ștefan; OANCEA, Ramona; HANGAN, Alina, *"Prelucrarea numerică a imaginilor. Aplicații ale rețelelor neuronale în prelucrarea imaginilor"*, 2006
- [50] VERTAN, Constantin; CIUC, Mihai, *Tehnici fundamentale de prelucrarea și analiza imaginilor*, Ed. MatrixROM, București, ISBN 978-973-755- 207-5, 2007
- [51] MOLDOVEANU, Florica, *Curs – Sisteme de prelucrare grafică*, capitolul Detectia frontierelor în imagini (<http://andrei.clubcisco.ro/cursuri/4spg/9.detectia.frontierelor.in.imagini.PDF>, accesat la 23.05.2017)
- [52] YOUNG, Ian T.; VAN VLIET, Lucas J.; VAN GINKEL, Michael, *"Recursive Gabor filtering"*, IEEE Transactions on signal processing, vol.50, no.11, p. 2798-2805, ISSN 1053-587X, 2002
- [53] BRAD, Radu, *"Procesarea Imaginilor și Elemente de Computer Vision"*, Ed. Univ. "Lucian Blaga" din Sibiu, ISBN 973-651-739-X, 2003
- [54] CANNY, John, *"A computational Approach to Edge Detection"*, IEEE Transaction on pattern Analysis and Machine Intelligence, Vol.8, No.6, pp. 679 – 698, ISSN 0162-8828/86, DOI 10.1109/TPAMI.1986.4767851, 1986
- [55] MARR, David; HILDRETH, Ellen, *"Theory of Edge Detection"*, Proceedings of the Royal Society of London B: Biological Sciences, vol. 207, nr. 1167, p. 187-217, ISSN 0962-8452, DOI 10.1098/RSPB.1980.0020, 1980
- [56] POPESCU, Rozica-Maria, *„Lecții complementare de teoria grafurilor"*, Editura Sfântul Ierarh Nicolae, ISBN 978-606-577-028-7, 2010
- [57] BÎZOI, Cristian-Gabriel, *„Algoritmul ungar"*, (http://gabi.bizoi.home.ro/Algoritmul%20ungar_aplicatie.pdf, accesat la 23.05.2017)
- [58] NĂDĂBAN, Sorin; ȘANDRU, Andrea, *„Algoritmica grafurilor – sinteze de curs și aplicații"*, Editura MIRTON Timișoara, ISBN 978-973-52-0249-1, 2007
- [59] LUPU, Cătălin; GĂITAN, Vasile-Gheorghiță; LUPU, Valeriu, *„Security enhancement of internet banking applications by using multimodal biometrics"*, SAMI 2015, Herl'any, Slovacia, p. 47-52, ISBN 978-1-4799-8220-2, DOI: 10.1109/SAMI.2015.7061904 7301177, 2015
- [60] LUPU, Cătălin; Vasile-Gheorghiță GĂITAN, Valeriu LUPU, *„Fingerprints used for security enhancement of online banking authentication process"*, IEEE 7th International Conference on Electronics, Computers and Artificial Intelligence – ECAI 2015, vol. 7, no. 1, p. 217-220, ISSN 1843-2115, 2015
- [61] LUPU, Cătălin; Valeriu Lupu, *„The beginnings of using fingerprints as biometric characteristics for personal identification purposes"*, Analele Universității „Constantin Brâncuși" din Târgu Jiu / Annals of the „Constantin Brâncuși" University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 3 / 2014, ISSN 1842-4856, p. 53-56, 2014
- [62] LUPU, Cătălin; Valeriu Lupu, *„Biometrics used for authentication in internet-banking applications"*, Analele Universității „Constantin Brâncuși" din Târgu Jiu / Annals of the „Constantin Brâncuși" University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 3 / 2014, ISSN 1842-4856, B+ cod 718, p. 57-63, 2014

- [63] **LUPU, Cătălin**, „*Development of optimal filters obtained through convolution methods, used for fingerprint image enhancement and restoration*”, The USV Annals of Economics and Public Administration, Section 5: Statistics, economic informatics and mathematics, vol. 14, no. 2 (20)/2014, pg. 156-167, ISSN 2285-3332, Online ISSN 2344-3847, 2014
- [64] **LUPU, Cătălin**; Vasile-Gheorghiță Găitan, Valeriu Lupu, „*Improving the Security of Internet Banking Applications by Using Multimodal Biometrics*”, Journal of Applied Computer Science & Mathematics, no. 19 (9) /2015, Suceava, p. 37-42, ISSN 2066-4273, 2015
- [65] **LUPU, Cătălin**; Valeriu Lupu, Gheorghe Gîlcă, “*Securing online banking services using iris recognition*”, Analele Universității „Constantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, p. 69-75, 2015
- [66] **LUPU, Cătălin**; Valeriu Lupu, Gheorghe Gîlcă, “*Overview on a personal recognition system that uses iris images as main biometric characteristic*”, Analele Universității „Constantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, p. 76-79, 2015
- [67] Gheorghe Gîlcă, Nicu-George Bîzdoacă, **LUPU, Cătălin**, “*Classification algorithms of facial expressions by using the feedforward neural networks*”, Analele Universității „Constantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, p. 80-85, 2015
- [68] Gheorghe Gîlcă, Nicu-George Bîzdoacă, **LUPU, Cătălin**, “*Artificial vision algorithms based on fractals for the image description*”, Analele Universității „Constantin Brâncuși” din Târgu Jiu / Annals of the „Constantin Brâncuși” University of Târgu Jiu, Seria Inginerie / Engineering Series, Nr. 4 / 2015, ISSN 1842-4856, p. 86-90, 2015
- [69] GRAGNANIELLO, Diego, ș.a. ”*An investigation of local descriptors for biometric spoofing detection*”, IEEE Transactions on Information Forensics and Security, vol. 10, nr. 4, pg. 849-863, ISSN 1556-6013, DOI 10.1109/TIFS.2015.2404294, 2015
- [70] NIGAM, Ishan; VATSA, Mayank; SINGH, Richa. “*Ocular biometrics: A survey of modalities and fusion approaches*”, Information Fusion, nr. 26, p. 1-35, ISSN 1566-2535, DOI 10.1016/j.inffus.2015.03.005, 2015
- [71] GRAGNANIELLO, Diego; SANSONE, Carlo; VERDOLIVA, Luisa, ”*Iris liveness detection for mobile devices based on local descriptors*”, Pattern Recognition Letters, vol. 57, pg. 81-87, ISSN 0167-8655, DOI 10.1016/J.PATREC.2014.10.018, 2015
- [72] BOWYER, Kevin W.; DOYLE, James S., ”*Cosmetic contact lenses and iris recognition spoofing*”, Computer, vol. 47, nr. 5, pg. 96-98, ISSN 0018-9162, DOI 10.1109/MC.2014.118, 2014
- [73] DOYLE, James S.; BOWYER, Kevin W, ”*Robust detection of textured contact lenses in iris recognition using BSIF*”, IEEE Access, vol. 3, p. 1672-1683, ISSN 2169-3536, DOI 10.1109/ACCESS.2015.2477470, 2015