Universitatea din București
Facultatea de Matematică și Informatică

Contribuții asupra Securității Protocoalelor Biometrice de Autentificare

Rezumatul Tezei de Doctorat

Coordonator Științific:

Prof. Univ. Dr. Adrian ATANASIU

Doctorand:

Ing. Marius Iulian Mihailescu

București, 2014

Cuprins

Prefaţă

Această teză doctorală are ca temă de cercetare securitatea datelor biometrice, cum ar fi semnăturile on- şi off-line sau procesul de recunoaştere a trăsăturilor faciale, precum şi oportunităţile şi provocările acestora în societatea contemporană. Tehnologiile biometrice reprezintă o contra-metodă pentru teroriști, care au sporit ameninţarea la adresa securităţii naţionale. Diverse dispozitive biometrice sunt acum disponibile pentru ambele tipuri de utilizatori, atât cei publici, cât şi cei particulari. Scopul acestor dispozitive este acela de a captura măsuri biometrice ale amprentelor digitale, ale palmei, retinei, apăsării tastelor, vocii şi expresiilor faciale. Un aspect este foarte important în privinţa măsurătorilor, şi anume acurateţea acestora, care variază şi are impact direct asupra diferitelor niveluri de securitate pe care le oferă. Pentru a combate problemele ridicate de identificarea furtului şi diferite probleme de securitate, societatea va trebui să facă un compromis între siguranţă şi variile libertăţi personale. Secolul XXI a adus cu sine o nouă societate, bazată pe tehnologie, care necesită o securitate crescândă şi metode de măsurare precise.

Un alt aspect al acestei lucrări este acela că am identificat impactul cel mai puternic al aplicaţiilor biometrice de securitate şi am prezentat diferite maniere prin care am minimalizat riscul de responsabilitate al profilulor biometrice care sunt stocate în baza de date. Identificarea şi verificarea au fost deja obţinute prin prezentarea unui document (paşaport, carte de identitate, insignă, permis de conducere) şi printr-un element cunoscut doar de către utilizator (parola). Situaţia compromiţătoare are loc la finalul procesului de autentificare (în mediul unei reţele) prin introducerea de date ilegale, fapt ce reprezintă o vulnerabilitate majoră. Modulul de autentificare (metode şi funcţii) poate fi ”păcălit”. În acest punct este necesară definirea unei proceduri de măsurare a riscului pentru sistemele biometrice aflate în funcţiune, cu o atenţie sporită asupra modulului de autentificare, care uneori nu are capacitatea de a verifica datele primite în cazul unei tranzacţii live.

Obiectivul primordial al tezei este acela de a satisface necesitatea unei persoane de a asigura securitatea identităţii. În fiecare secundă au loc atacuri virtuale asupra identităţii conectate sau asupra identităţii societăţilor comerciale care oferă diverse servicii online. Aceste atacuri sporesc nu doar din punct de vedere numeric, ci şi în ceea ce priveşte ingeniozitatea atacatorilor. De exemplu, atacurile de tip *phishing* (adică furtul de informaţii sensibile ale unei persoane: PIN, cod numeric personal etc.) sau cele de tip ”web-spoofing” (adică păcălirea victimei cu scopul de a oferi informaţii prin crearea unei interfaţe virtuale) şi multe altele. Luând în considerare faptul că în viitor va fi utilizată o tehnologie din ce în ce mai inteligentă pentru identificarea personală (ca de exemplu paşapoartele biometrice) din ce în ce mai multe acţiuni vor fi realizate online: cumpărături, votare etc., iar în acest fel managementul identităţii va căpăta o importanţă şi mai mare, iar prevenirea unor atacuri va juca un rol decisiv, întrucât informaţiile obţinute de atacatori vor fi mai importante.

În condiţiile descrise mai sus va apărea necesitatea ca sistemele de autentificare să aibă un grad mai mare de securitate, să fie cât mai transparente pentru utilizator şi uşor de implementat pentru dezvoltatori. Timpul consumat de către companiile furnizoare, care oferă servicii ce necesită autentificare pentru obţinerea de module cu această funcţie, trebuie să fie cât mai scurt posibil. Timpul de autentificare efectivă trebuie redus la minumum. Pentru o autentificare corespunzătoare, este necesară implementarea unei metode cu rata de intruziune apropiată de 0.

Aşa cum am menţionat anterior, teza doreşte să satisfacă necesităţile descrise mai sus prin includerea unei metode de autentificare biometrică bazată pe semnătura holografică combinată cu amprente şi carduri inteligente în toate serviciile online de autentificare sau în general în toate modulele de autentificare în care va fi utilizată o conexiune biometrică. Semnătura holografică reprezintă o caracteristică importantă a individului. Metoda descrisă mai

sus este protejată la nivel național de patentul ”Sistem și metode de analiză a achiziției și autentificare a semnăturii de mână”.

Sistemul construiește un kit de dezvoltare a soluțiilor (Solution Developer Kit), oferit dezvoltatorilor de aplicații, care facilizează obținerea subsistemelor de autentificare. Arhitectura respectă conceptele standardelor SoA și SaaA, preia procesele de autentificare de la calculatorul clientului și îl realizează pe un sistem dedicat, făcând din el un proces invizibil pentru utilizator. Practic, fiecare companie care necesită un sistem de protecție pentru seviciile oferite va fi capabilă să construiască un modul de autentificare utilizând un SDK ce va comunica prin intermediul internetului cu unicul serviciu de autentificare implementat pe unități dedicate de prelucrare. Adevărata autentificare va fi realizată pe serverele sistemului și nu va impune un prag de performanță pentru stațiile de lucru ale clienților.

În ultimul deceniu tehnologiile biometrice de identificare au fost adoptate și integrate de laptopuri, telefoane mobile, mașini, sisteme de control al accesului în diverse spații, carduri naționale de identitate etc. Sistemele biometrice devin din ce în ce mai comune în clădiri care necesită un nivel înalt de securitate (departamente guvernamentale, organizații). Un sistem biometric precis este capabil să refuze utilizatorii autorizați, să eșueze în procesul de identificare pentru utilizatori cunoscuți, să identifice incorect utilizatorii sau să trateze o persoană neautorizată ca un utilizator recunoscut. Pentru a rezolva astfel de probleme propunem în [2] o schemă de autentificare întemeiată pe criptografia bazată pe haos, în speranța că va îmbunătăți tehnicile de criptografie modernă și clasică și că va lansa noi provocări în acest domeniu, alături de criptografia cuantică.

Succesul tehnologiilor biometrice în identificarea personală este mai confortabil întrucât accesul, autentificarea și autorizarea sunt posibile datorită caracteristicilor unice, psihologice, biologice sau comportamentale ale indivizilor. Uneori percepem biometria ca pe ceva straniu, din altă lume sau aparținând tehnologiei SF, pe care ar trebui să o utilizăm alături de mașinile care se reîncarcă la soare și alte asemenea dispozitive, însă cine știe ce ne va rezerva viitorul?

Structura tezei este următoarea:

- **Capitolul 1 – Introducere.** Această parte reprezintă o privire de ansamblu asupra direcțiilor de cercetare, prezentând motivul pentru alegerea acestui subiect în lucrarea de doctorat. În ultima parte a capitolului există o scurtă analiză a unor probleme de securitate întâmpinate în procesul de creare și dezvoltare a sistemelor de autentificare biometrică.
- **Capitolul 2 - Schemele de protejarea șabloanelor biometrice de autentificare**. Aici vom discuta principalele vulnerabilități de securitate și câteva metode ce pot fi utilizate pentru a le preîntâmpina în cadrul procesului de înregistrare și autentificare.
- **Capitolul 3** – **Framework-urile biometrice.** Acest capitol va examina problemele inverse ale biometriei ce au loc în procesul de concepere și dezvoltare a unui sistem biometric. Vom realiza o cercetare asupra diferitelor metode utilizate pentru prevenirea variilor tipuri de atacuri, pentru a înțelege cum acționează atacurile asupra protocoalelor biometrice și RFID. În final ne vom opri asupra unor aspecte generale legate de modelele de urmărire, utilizate în sistemele biometrice, ce pot fi atacate cu scopul de a păcăli sistemul în vederea autentificării. Vom prezenta un background general asupra modului în care datele biometrice sunt organizate și expuse prin utilizarea unui pașaport biometric. Contribuția personală este desfășurată pe trei secțiuni, după cum urmează:
  - probleme directe și inverse (Secțiunea 3.1);
  - vulnerabilități, amenințări și etape de înregistrare pentru pașapoartele biometrice electronice (e-passports) (Secțiunea 3.2);
  - sisteme de modele de urmărire (tracking models systems) bazate pe componente biometrice optoelectronice (Secțiunea 3.3).

- **Capitolul 4** – **Recunoașterea facială**. Acest capitol va prezenta un cadru general în care vor fi detaliate principalele caracteristici ale procesului de recunoaștere facială și vulnerabilitățile de securitate. (Secțiunile 4.1 – 4.4). La final propun o soluție pentru asigurarea securității și integrității imaginilor faciale 2D și 3D (Secțiunea 4.4).
- **Capitolul 5** – **Prevenirea atacurilor algebrice împotriva protocoalelor biometrice și RFID**. Acest capitol reprezintă o contribuție personală care se concentrează pe identificarea posibilelor atacuri algebrice împotriva sistemelor de autentificare biometrice și RFID.
- **Capitolul 6** – **Semnăturile biometrice online și offline**. În acest capitol propunem câteva contribuții bazate pe cerințele de sinteză a semnăturilor (Secțiunea 6.1) necesare pentru a înțelege unde ar putea exista vulnerabilități de securitate (Secțiunile 6.2 – 6.5). Majoritatea contribuțiilor de cercetare din această secțiune sunt bazate pe proiectul ATHOS, propus și dezvoltat de SOFTWIN Inc. și proiectul european POSDRU 61434.
- **Capitolul 7** – **Concluzii și direcții viitoare de cercetare.** Aici vor fi schițate câteva direcții viitoare, cu scopul continuării cercetării curente.

1. Introducere

Biometria reprezintă o componentă majoră din viitorul şi din viaţa noastră. Totul va fi stocat pe dispozitive biometrice (carduri biometrice, paşapoarte biometrice, chipuri RFID etc.). Vulnerabilităţile sistemelor biometrice ridică multe probleme. Este foarte dificil să combaţi toate atacurile care ar putea avea loc, distrugând multe identităţi şi vieţi omeneşti. Metodele biometrice utilizate pentru autentificarea indivizilor pornesc de la caracteristici fizice sau acţiuni care sunt suficient de bine definite pentru a îndeplini cerinţele minime ale unei aplicaţii specifice. Succesul acestor tipuri de metode depinde de un număr de constrângeri:

- Zona fizică asupra căreia sistemul operează fără intervenţie umană;
- Gradul de unicitate al acelei trăsături şi orice altă confuzie cu alte identităţi din acel grup;
- Factori precum: cost, scalabilitate şi securitate.

Odată cu creşterea nivelului economiei globale şi al tehnologiei infromaţiei există din ce în ce mai multe zone care necesită o autentificare sigură a identităţii. Metodele tradiţionale de autentificare, bazate pe identitate, se concentrează pe ceea ce poate fi posedat la nivel fizic, cum ar fi cardurile de identitate şi ceea ce poate fi reţinut la nivel mental, cum ar fi parolele sau cheile. În această teză voi prezenta o parte din activitatea de cercetare, pe care am realizat-o în ultimii trei ani. În acest sens, am optat pentru trei direcţii de cercetare:

- Soluţiile generale de bază pentru a anticipa şi a combate diferite atacuri la adresa securităţii prin exploatarea diverselor vulnerabilităţi;
- Conceperea de noi algoritmi care sprijină procesul de generare a semnăturilor biometrice online şi offline şi a recunoaşterii faciale;
- Crearea unui nou cadru biometric care intenţionează să devină componentă a CrypTool şi, mult mai mult, să ajute şi să îmbunătăţească procesul de dezvoltare a aplicaţiilor şi sistemelor bazate pe autentificare biometrică. Acest cadru are următoarele obiective majore:
  - Simularea procesului de autentificare pentru diferite caracteristici biometrice;
  - Construirea unui sistem biometric în modul vizual prin plasarea diferitelor componente;
  - Utilizarea celor mai importante baze de date biometrice pentru experimente şi teste, cum ar fi: Biometric Ideal Test (BIT), SuSIG, ATVS etc.
  - Modulele criptografice: metode (criptografia modernă şi clasică, criptografia bazată pe haos etc.) pentru criptarea şi decriptarea datelor biometrice;
  - Funcţiile codurilor de autentificare;
  - Modulele de măsurare a performanţei: metricile FAR, FMR, FRR, FNMR, EER, CER, FTE, FER, FTC etc. O parte din aceste metrici sunt explicate în capitolul 2;
  - Grafice şi diagrame arătând diferite caracteristici biometrice;
  - Algoritmi de statistică.

În afară de sarcinile menţionate mai sus, voi investiga securitatea datelor biometrice din perspectiva criptografiei bazate pe haos, cum ar semnătura online şi offline şi procesul de recunoaştere facială, oportunităţile şi provocările pentru societatea noastră în prezent. Aşa cum am menţionat anterior, securitatea statelor este din ce în ce mai ameninţată de grupurile teroriste care încearcă, prin orice mijloace care le stă în putere, să atace şi să compromită siguranţa naţională. De aceea este nevoie acum, mai mult ca oricând, ca sistemele biometrice să fie protejate de cât mai multe atacuri posibile. Nu numai securitatea naţională poate avea de suferit din cauza acestor tipuri de atacuri. Ţinând cont de faptul că există acum dispozitive biometrice

atât pentru uz oficial, cât și pentru uz public, trebuie protejată identitatea persoanei, prin îmbunătățirea eficienței și siguranței sistemelor care întrebuințează șabloane biometrice, mai ales pentru a calma spiritele în ceea ce privește utilizarea unor astfel de sisteme. Este bine cunoscut faptul că, la ora actuală, există multe controverse și divergențe de opinii cu privire la utilizarea trăsăturilor biometrice cu scopul identificării personale. Cu toate acestea însă, necesitatea folosirii acestor tehnologii devine imperativă, în contextul politic și economic actual. Așadar, societatea trebuie să facă acest compromis la nivelul libertăților personale, prin diminuarea unor părți ale acestora, pentru a câștiga mai mult în planul siguranței.

Dificultatea nu mai constă în obiectele fizice probatoare (documente, pașapoarte, carduri etc.), această problemă fiind rezolvată prin adăugarea unei chei/ parole memorate, care, alături de documentul identificator, reprezintă o modalitate eficientă de identificare și, mai ales, autentificare a unui individ. Problema o reprezintă însă sistemele biometrice, care pot fi atacate la diferite niveluri. Despre punctele slabe și posibilele vulnerabilități, cât și despre posibile măsuri de corectare a acestora și îmbunătățire a calității sistemelor, vom discuta pe parcursul acestei teze.

Ținând cont de faptul că sistemele biometrice au ajuns să fie practic indispensabile în uzul cotidian, de la sedii strategice, organizații guvernamentale etc. până la dispozitive personale, cum ar laptopuri, mașini sau telefoane mobile, concluzia nu poate fi decât una singură: este nevoie de un efort continuu și constant pentru a spori acuratețea și precizia metodelor de autentificare pe baza trăsăturilor biometrice și a garanta securitatea datelor cu caracter personal utilizate în cadrul sistemelor biometrice.

2. Scheme pentru protecția șabloanelor biometrice în procesul de autentificare

În ultimul deceniu criptografia bazată pe haos s-a bucurat de o cercetare activă, datorită proprietăților sistemelor dinamice, cum ar fi gradul înalt de sensibilitate la condițiile inițiale, ergodicitatea și proprietățile mixte. Aceste proprietăți par să îndeplinească cerințele de bază ale principiilor securității Shannon, precum confuzia și difuzia. Astfel, recent au fost propuse câteva scheme de criptare pe bază de haos care sunt rapide, sigure și pot fi utilizate în faza de autentificare a proceselor biometrice de recunoaștere ([7, 8, 9]).

2.1. Caracteristicile schemelor de protecție a șabloanelor

Procesul de recunoaștere biometrică reprezintă o soluție viabilă în ceea ce privește problema autentificării utilizatorului pentru sistemele de management al identității (IMS). Ca o scurtă definiție, un IMS reprezintă un sistem de informație care poate fi folosit în mediul de întreprindere sau pentru managementul identității între rețele (cross-network identity management).

O schemă de protecție a șablonului reprezintă o structură în care datele biometrice sunt protejate cu un mecanism de securitate (algoritmi criptografici).

În articolul [45] se arată și este demonstrat faptul că schema de protecție a șablonului ar trebui să aibă patru proprietăți:

- **Diversitate:** șablonul care este securizat nu permite procese de tip cross-matching cu baza de date. În acest mod este asigurată discreția.
- **Revocabilitate:** este necesar să existe posibilitatea de a revoca șabloanele compromise și de a re-emite un nou șablon pe baza acelorași date biometrice.
- **Securitate:** obținerea șablonului biometric original trebuie să fie deosebit de dificil de realizat din punct de vedere computațional de la șablonul securizat. Astfel, adversarul nu va avea posibilitatea de a crea o machetă fizică a trăsăturii biometrice, pe baza șablonului sustras. De exemplu, putem vedea cum este aplicată securitatea pe pașapoartele biometrice [19].
- **Performanța:** Schema de protecție a șablonului ar trebui să respecte caracteristicile performanței – rata falsă de acceptare (FAR) și rata falsă de respingere (FRR) – ale unui sistem biometric.

Rata falsă de acceptare (FAR) reprezintă o unitate de măsură pentru sistemul de securitate biometric, care va accepta incorect o tentativă de acces de către un utilizator neautorizat.

Rata falsă de respingere (FRR) reprezintă o unitate de măsură pentru sistemul de securitate biometric, care va respinge în mod incorect o tentativă de acces din partea unui utilizator autorizat.

Cea mai mare provocare în conceperea unei scheme de protecție a șablonului biometric ce satisface toate criteriile menționate anterior este necesitatea de a manevra variabilitatea intra-utilizatori în identificatorii biometrici obșinuți.

În Figura 2.1 putem vedea că schemele de protecție a șabloanelor pot fi clasificate în două categorii: transformarea caracteristicilor și criptosistemul biometric. Contribuția din Secțiunea 6.3 aduce o nouă schemă de înrolare și pornește de la criptografia bazată pe haos, fiind situată în cea de-a doua categorie.

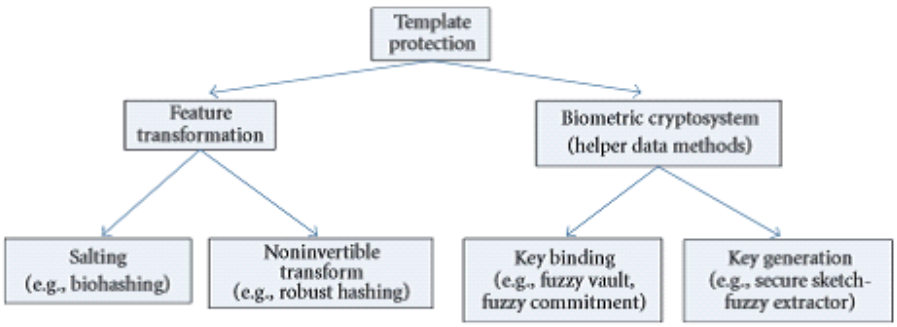

Figura 2.1 Diverse categorii de scheme de protecție a șabloanelor

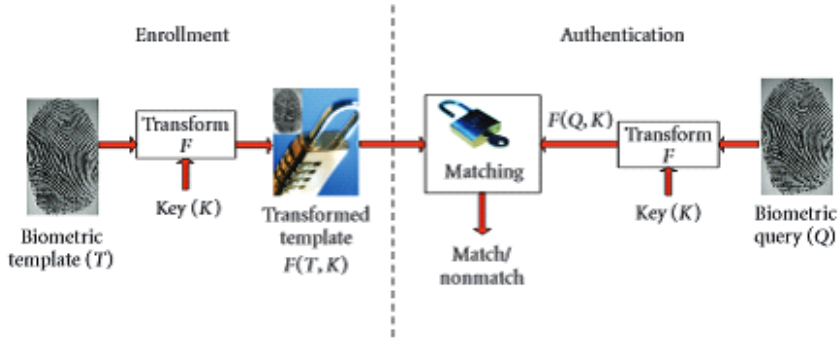

Figura 2.2 Mecanismul de autentificare când șablonul biometric este protejat utilizând o abordare de transformare a caracteristicii [14]

În prima categorie, *transformarea caracteristicilor*, transformarea funcției *F* este aplicată șablonului biometric *(T).* Șablonul este trecut prin procesul de transformare *(F(T, K))* și este stocat în baza de date (Vezi Figura 2.2). Parametrii funcției de transformare sunt derivați de la o cheie aleatorie *(K)* sau o parolă. Aceeași funcție de transformare este utilizată pentru caracteristicile interogării *(Q)* iar interogarea transformată ce a rezultat *(F(Q, K))* se contrapune în mod direct șablonului transformat *(F(T, K).*

În Figura 2.2 este prezentat un rezumat al diferitelor scheme de protecție a șabloanelor. În Figura 2.3 putem vedea cum un mecanism de autentificare arată când un șablon biometric este securizat, folosind o cheie generată pentru criptosistemul biometric.

În [154] este propus un criptosistem biometric care a fost initial dezvoltat pentru a asigura securizarea unei chei criptografice, folosind caracteristici biometrice sau generând direct o cheie criptografică din trăsăturile biometrice.

Există o informații publice într-un criptosistem (cunoscute sub numele de date de ajutor), care se referă la șabloanele stocate. Așadar, criptosistemele biometrice sunt cunoscute ca metode de ajutor pe bază de date. Datele de ajutor nu fac publice informații semnificative despre șablonul biometric original, necesar pe parcursul procesului de comparare pentru extragerea cheii criptografice din trăsăturile biometrice de interogare. Procesul de comparare este realizat în mod indirect prin verificarea validității cheii extrase (vezi Figura 2.3).

Criptosistemele biometrice pot fi clasificate în *sisteme biometrice prin intrdoucerea unei chei (key binding*) și *sisteme generatoare de chei*. Această clasificare este realizată în funcție de modul în care sunt obținute datele de ajutor.

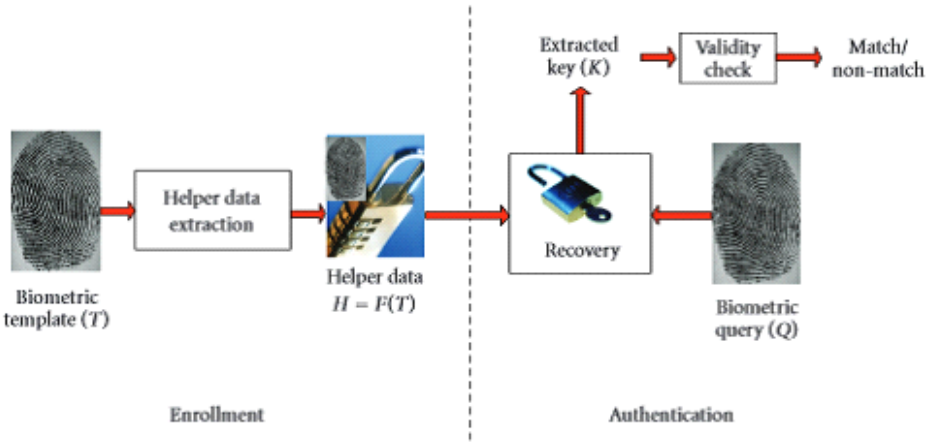

Figura 2.3: Mecanisme de autentificare când șabloanele biometrice sunt securizate utilizând un criptosistem biometric generator de chei. Autentificarea într-un criptosistem biometric bazat pe introducerea unei chei (key binding) este similară, cu excepția faptului că datele de ajutor sunt o funcție atât a șablonului, cât și a cheii *K*, așadar *H = F(T, K)* [14]

2.2. Vulnerabilitățile sistemului biometric

Pornind de la modelul de tip fish bone, Figura 2.4, putem vedea un sumar al diferitelor cauze ale vulnerabilităților sistemelor biometrice. Modelele de eșec pot fi clasificate în două categorii: *eșec intrinsec* și *eșec datorat atacului unui adversar*.

- **Eșecul intrinsec** poate avea loc din cauza limitărilor inerente la citirea, extragerea trăsăturilor sau a tehnologiilor de comparare, cât și din cauza discriminării limitate pentru trăsături biometrice specifice. În continuare vom clasifica atacturile din partea adversarilor în trei tipuri. Ne vom concentra pe factori care oferă posibilitatea adversarului de a compromite securitatea sistemului biometric. Acești factori sunt: administrarea, deschiderea (transparența) biometrică și infrastructura nesigură.

Această categorie reprezintă o lacună în securitate din cauza deciziei incorecte luată de sistemul biometric. Un sistem de verificare biometric poate avea două tipuri de erori: falsă acceptare sau falsă respingere. Un utilizator legitim poate fi respins în mod eronat de către sistem din cauza diferențelor majore stocate în șablonul utilizatorului.

Această lacună în securitate poate avea loc când nu există intenții serioase din partea unui adversar să stopeze sistemul. Acest tip de eșec mai este cunoscut și sub numele de *atacul de tip zero-effort* (*zero-effort-attack*).

- **Atacurile adversarilor** sunt îndreptate asupra sistemelor biometrice și au un caracter intenționat. Succesul acestora depinde de lacunele de securitate în designul sistemului. Atacurile adversarilor pot fi grupate în trei categorii: transparență biometrică, insfrastructură nesigură și atacuri la adresa administrării.
  - ***Transparența biometrică***. Această categorie de atacuri constă în procesul de obținere de către adversar a caracteristicilor biometrice ale unui utilizator autentic (de ex. amprenta, semnătura) și utilizarea acestora pentru a crea diferite artefacte fizice pentru trăsăturile biometrice.
  - ***Infrastructura nesigură***. Există diverse modalități pe care un adversar le poate folosi pentru a manipula componentele infrastructurii biometrice (software,

hardware sau comunicațiile din rețea) cu scopul de a crea breșe de securitate. Pentru mai multe detalii, vezi Combaterea atacurilor adverse, prezentată mai jos.

- ***Atacurile la adresa administrației***. Acest tip de atac este cunoscut, de asemenea, ca atac din interior și se referă la toate vulnerabilitățile care pot apărea din cauza administrației defectuoase a sistemului biometric. Acestea includ abuzul de metode de procesare a excepțiilor, coerciția (complotul) dintre administratorul sistemului și adversar și integritatea procesului de înrolare (de exemplu corectitudinea credențialelor pe parcursul procesului de înrolare).

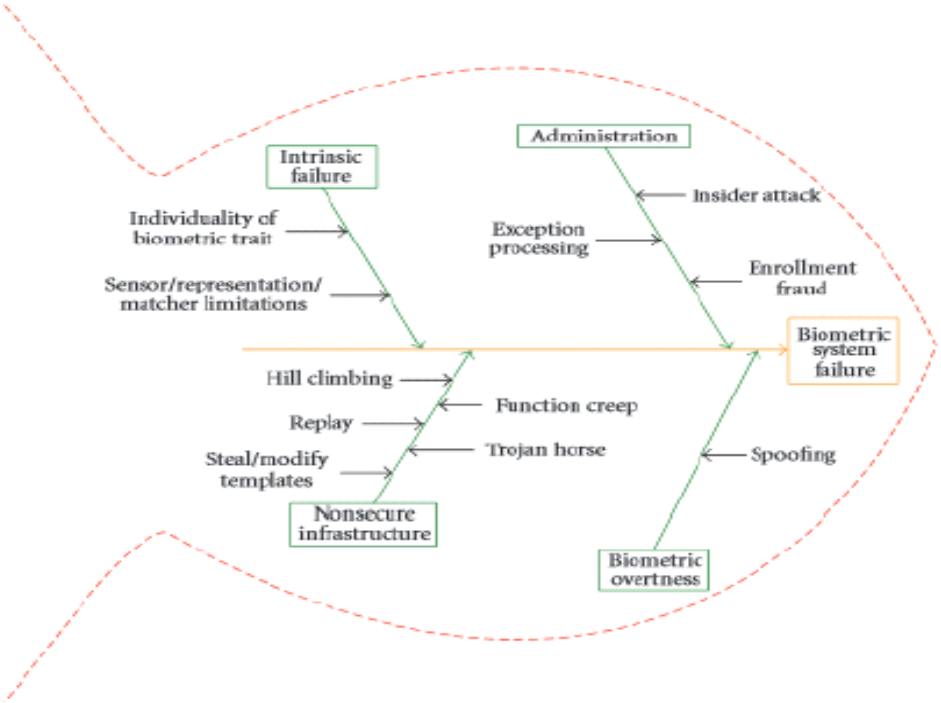

Figura 2.4 Categorizarea vulnerabilităților sistemului biometric utilizând modelul fish bone [15]

- **Urmările eșecului sistemului biometric**. Când un sistem de autentificare biometrică este compromis, avem de-a face cu două efecte: *refuzul serviciului* și *intruziunea*.

Refuzul serviciului are loc atunci când un utilizator legitim este împiedicat să obțină serviciul care i se cuvine. În acest caz, adversarul poate sabota infrastructura sistemului, împiedicând utilizatorii să acceseze componentele sistemului.

Intruziunea presupune că un impostor va câștiga acces ilegal în sistem, rezultând cu pierderea intimității, a datelor personale (de ex. accesul neautorizat la informație vitală) și accesul la pragul de control (de exemplu atunci când teroriștii încearcă sa treacă granița).

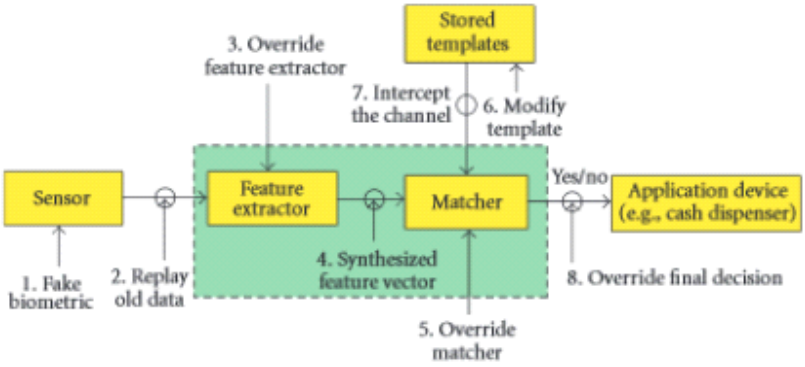

Figura 2.5: Puncte de atac în sistemul biometric [105, 115]

- **Apărarea de atacuri ale adversarilor**. Scopul acestor atacuri este de a exploata vulnerabilitățile sistemului și a diferitelor componente din structura acestuia. În [112] sunt identificate opt puncte de atac asupra diferitelor părți ale sistemului (Vezi Figura 2.5). Realizăm o clasificare a acestor atacuri în patru categorii: atacuri ce au loc la interfața cu utilizatorul – nivel de intrare, atacuri lansate la interfața dintre module diferite, atacuri asupra modulelor și atacuri asupra bazei de date a șabloanelor.
- (a) ***Atacuri asupra interfeței cu utilizatorul***. Acestea au loc prin prezentarea unei machete cu trăsătura biometrică [152, 153]. În acest caz, senzorul este incapabil să facă diferența dintre trăsăturile biometrice false și cele reale, iar adversarul ar putea cu ușurință intra în sistem, utilizând o identitate falsă. S-au făcut o serie de încercări pentru crearea și dezvoltarea unor soluții hardware și software concepute pe ideea de detectare a stării de existență în cazul mostrelor de trăsături biometrice [140].

  (b) ***Atacuri la interfața dintre module***. Un adversar are posibilitatea de a sabota comunicarea dintre diferite module. De exemplu, acesta poate plasa o sursă în apropierea canalului de comunicare. Dacă respectivul canal nu este securizat din punct de vedere fizic sau criptografic, un adversar va putea intercepta și modifica datele aflate în curs de transfer. În [26], autorii subliniază cele mai importante probleme de securitate și de intiminate care pot apărea la canalele nesigure de comunicare într-o aplicație pentru un pașaport electronic care utilizează autentificarea biometrică. O posibilitate de a asigura un astfel de canal este aceea de a aplica o codificare criptografică datelor care sunt trimise prin intermediul interfeței, când un utilizator legitim utilizează în mod corect formularul de autentificare din cadrul sistemului. O metodă de protecție pentru aceste atacuri este utilizarea marcajelor de timp [78] sau a unui mecanism bazat pe provocare/ răspuns [135].

  (c) ***Atacuri asupra modulelor software***. Programul de execuție (the executable program) situat într-unul dintre module poate fi modificat astfel încât să dea adversarului valoarea de ieșire dorită. Aceste tipuri de atacuri sunt cunoscute ca atacuri de tip Cal troian. În [123] sunt prezentate diverse tehnici pentru a asigura o execuare de cod (code execution).

  (d) ***Atacurile asupra bazei de date a șabloanelor***. Unul dintre cele mai periculoase atacuri la adresa sistemelor biometrice este cel împotriva șabloanelor biometrice stocate în baza de date a sistemului. Atacurile asupra șabloanelor au în vedere trei tipuri de vulnerabilități:

- Un șablon poate fi înlocuit de un fals pentru a obține acces neautorizat;
- O machete fizică poate fi obținută de la șablon [28] către sistem;
- Șablonul furat poate fi reutilizat pentru a obține acces ilegal.

În încheiere, acest capitol prezintă cele mai importante probleme de securitate pe care trebuie să ne concentrăm atenția, atunci când vorbim de procese de autentificare bazate pe biometrie. Când aplicațiile biometrice (software sau web) sunt dezvoltate de companii, este foarte important să se acorde importanță acestor tipuri de categorii listate mai sus. Procesul de inginerie software este foarte important în conceperea unor asemenea aplicații. Propunem câteva practici care pot fi utilizate în procesul de analiză, concepție și dezvoltare a sistemelor de autentificare biometrică [98, 106, 107, 108, 109, 110].

3. Framework-uri Biometrice

3.1. Introducere

Acest capitol se concentrează asupra problemei de tip invers folosită în biometrie [96], care reprezintă o direcție importantă pentru sinteza datelor biometrice. De-a lungul timpului a fost demonstrat că datele biometrice sintetice, atât non-automate, cât și cele semi-automate, sunt limitate.

Problema directă este definită ca procesul de analizare a informațiilor biometrice. *Problema inversă* reprezintă sinteza informațiilor biometrice. Procesul de analiză (problema directă) este reprezentată ca o mulțime de trăsături diferite folosite pentru recunoașterea și proiectarea sistemului biometric. Procesul de sinteză (problema inversă) este reprezentat de date biometrice sintetice proiectate de un set (mulțime) de reguli.

Câteva exemple sunt: amprente sintetice, semnături sintetice, iris sintetic, vorbire sintetică, melodii (muzică), emoții și expresii sintetice, roboți umanoizi.

Cea mai mare atenție va fi îndreptată către sinteza automată a datelor biometrice: recunoașterea facială și semnăturile. Analiza datelor biometrice reprezintă problema directă, iar sinteza datelor biometrice reprezintă problema inversă. Acest capitol aduce două contribuții personale pentru problema directă și inversă a sistemelor biometrice.

Prima contribuție [96] expune un studiu de bază care încearcă să clarifice confuzia asupra esenței a ceea ce înseamnă în sistemele biometrice problema inversă și problema directă. Am introdus un nou concept, numit *paradigma problemei directe și a problemei inverse*, divizată în două sub-paradigme (directă și inversă) și explicăm motivul pentru care ar trebui să ne concentrăm pe această paradigmă atunci când dezvoltăm sisteme biometrice; cea de-a doua contribuție [97] se concentrează asupra semnăturilor sintetice deoarece reprezintă unul dintre cele mai bune exemple pentru biometria inversă. De-a lungul istoriei, multe semnături olografice (handwriting) și atacuri false asupra semnăturii olografice (handwriting forgery attacks) au reprezentat una dintre cele mai mari probleme ale experților caligrafici și în special în cadrul juridic. Există câteva referințe și rapoarte în detectarea falsificării manuale, în care un atacator încearcă să simuleze o semnătură autentică.

Multe sisteme biometrice folosesc diferite metode și algoritmi, cum ar fi recunoașterea tiparului, căutarea bazelor de date, statistici, etc. cu scopul de a analiza datele biometrice colectate de la indivizi. Considerarea problemei inverse, sinteza, care reprezintă crearea unor date biometrice sintetice (artificiale) pentru a produce informații biologice importante cum ar fi existența unui sistem biometric, este folositoare.

Problema inversă se regăsește în mai multe domenii. Cineva încearcă să găsească un model care fenomenologic aproximează datele observate. În aceste situații, unele modele directe vor prezice o mulțime de date de care este interesat altcineva.

Alte aspecte abordate în acest capitol sunt:

- Introducerea modelelor folosite în procesul de sinteză al datelor biometrice, cu o atenție importantă asupra sinteza vizuală a informațiilor biometrice;
- Introducerea structurilor de date pentru a reprezenta informația biometrică sintetică;
- Prezentarea câtorva tehnici și unelte pentru generarea informației biometrice sintetică.

4. Recunoaștere facială

4.1. Componentele modelului facial

Când vorbim despre analiza sau sinteza expresiilor faciale, trebuie să reținem că fața umană este în primul rând caracterizată de complexitate, mobilitate și unicitate (cu anumite excepții). Topologia feței se numește *expresie facială* și modelarea aspectului facial se numește *sinteză facială*.

Construirea unei expresii faciale implică doi pași:

$$< Emotion, index(id) emotion, brain > \Rightarrow < Expression(face) > \quad (4.1)$$

Această secțiune descrie modelul expresiei faciale folosind schema definită:

$$< Emotion > \Rightarrow < Code > \Rightarrow < facialmuscles > \quad (4.2)$$

Problema directă și inversă a biometriei faciale este bazată pe modelul topologic, care conduce la concluzia că putem folosi transformări, reprezentări, măsuri de manipulare, toate din punct de vedere topologic.

Prin urmare, putem defini fața ca aria dintre linia unde începe părul și bărbie, și dintre cele două urechi. Aceasta este zona fundamentală a expresiei faciale. Câteva scopuri si aplicații implică testarea sistemului, identificarea rapidă în baze de date și recunoașterea figurilor trucate (înșelătoare), interfețe om – mașină, pregatirea personalului de securitate, dar și pentru alte aplicații în medicină și psihologie. Pentru ca aplicațiile să funcționeze, este necesar un alt model de fiecare dată, depinzând de parametrii implicați și de sarcinile pe care trebuie să le îndeplinească (Figura 4.1). De exemplu, procesul de tip face matching nu necesită sensibilitate la expresiile faciale, deși trebuie să fie capabilă să identifice mișcarea mușchilor. Putem clasifica mișcările în *mișcări globale* (când este mișcat tot capul) și *mișcari locale* (diferite expresii faciale).

Capacitatea detectării mișcărilor musculare și schimbărilor în expresii este importantă în special într-o serie de aplicații, cum ar fi o nouă generație de detectoare de minciuni care nu implică contactul. Ca orice altă trăsătură biometrică, procesarea facială implică probleme inverse (inverse problems) unde fețele sunt sintetizate, și probleme directe (direct problems) unde este analizată structura topologică a feței. Asemanător cu analiza semnăturilor bazată pe paradigma de sinteză (synthesis paradigm), fețele sintetice sunt post-procesate pentru a obține o imagine care reproduce realitatea.

Psihologii dau diferite clasificări ale expresiilor faciale, cum ar fi teama, fericirea, surprinderea, tristețea etc, pe de o parte sau expresii care pot fi divizate în funcție de mulțumire sau nemulțumire, activitate sau pasivitate, sau capacitate de control. Relația dintre topologia facială și o expresie emoțională este definită de o extensie. Pentru a exemplifica, extensia unui zâmbet implică o serie de topologii faciale care necesită mișcarea gurii, a ochilor și a sprâncenelor.

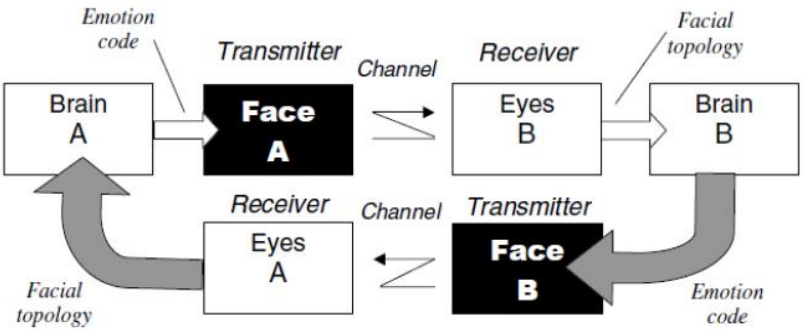

Figura 4.1 – Modelul comunicării față în față

Modelul facial poate fi considerat atât ca un întreg, dar şi ca o sumă de sub-părţi ale modelului, care include modele ale ochilor, ale gurii, ale nasului, ale sprâncenelor şi ale urechilor. Când construim un model facial, iniţial construim o faţă comună, neutră, căreia îi adăugam atribute specifice. În funcţie de sub-model, atributele pot fi: formă, mărime, textură, dinamism, calitatea de a fi deschis sau închis etc (Figura 4.2). Expresiile faciale reprezintă dinamica muşchilor şi a pielii, fapt pentru care modelarea facială implică o combinaţie între modelarea activităţii musculare şi deformarea pielii. Pe durata procesului, trebuie să luăm în considerare atributele amintite mai sus, de exemplu factorul de îmbătrânire, care schimbă trăsăturile pielii, în special elasticitatea. Pielea joacă cel mai important rol în recunoaştere şi generare.

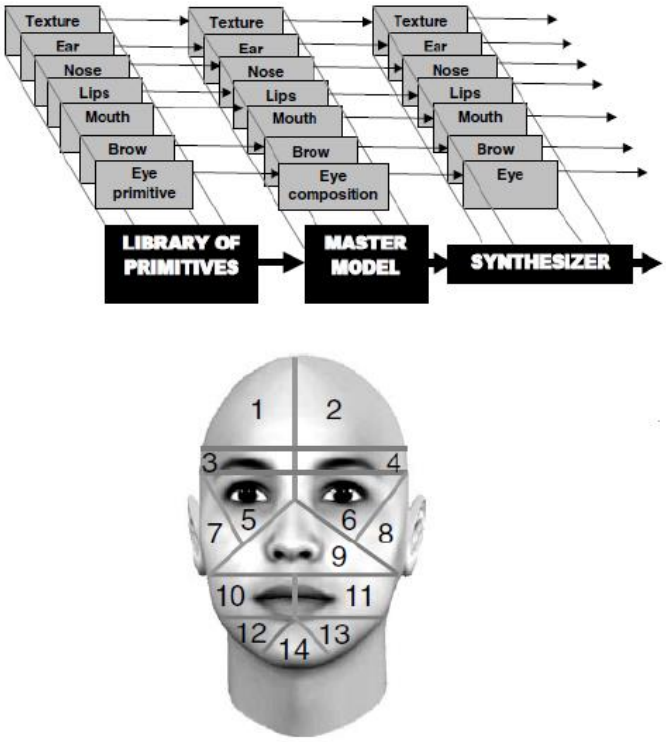

Figura 4.2 – Partiționarea feței pentru analiza facială

4.2. Modele ale comportamentului facial

Modelele faciale pot fi divizate în două categorii principale: *statice* (concentrate pe topologie) şi *dinamice* (modele care intenţionează să prezinte şi caracteristicile comportamentale). În al doilea caz, parametrii modelului depind de natura schimbărilor: *termen lung* (trăsături care se schimbă încet, de-a lungul vieţii) sau *termen scurt* (schimbări care au loc instantaneu, ca rezultat al emoţiilor). Schimbările pe termen scurt apar în special pe parcursul convorbirilor şi pot exprima mai multe lucruri, de la starea afectivă, activitatea cognitivă, trăsături de temperament şi personalitate, sinceritate, la psihopatologie. Deşi sunt foarte utile în interfeţele om-maşină, expresiile faciale pot reprezenta o problemă dificilă în încercările de identificare facială. Când comparăm o fotografie în care un om este serios cu o altă fotografie în care omul exprimă emoţii diferite, căutarea poate rezulta negaţii false.

În acord cu maniera sintetizării feţei este caricatura: o artă particulară a desenului care subliniază anumite trăsături ale feţei unei persoane cu scopul de a sugera idea ridicolului. În biometrie, caricaturile pot fi folosite pentru a testa capacitatea sistemului de a identifica aria feţei. Cea mai folosită tehnică de a caricaturiza o faţă este aceea prin care se schimbă distanţele dintre punctele de control (mărire sau micşorare) pentru a sublinia anumite trăsături specifice şi individuale, astfel încât, chipul persoanei, deşi modificat, să poată fi recunoscut. Înţelegerea acestor tehnici de către sistemele automate este un pas înainte în îmbunatăţirea tehnicilor de recunoaştere facială.

4.2.1. Diferite clasificări ale modelelor faciale

Cu ajutorul algoritmilor şi a reţelelor neuronale artificiale, putem descrie configuraţii topologice, clasificate, conform psihologilor, în cinci pană la opt emoţii de bază. Altă clasificare poate fi făcută în funcţie de mişcarea muşchilor.

Separat de aceasta, pot fi literalmente sute de topologii faciale diferite, date de complexitatea muşchilor. Cu toate acestea, toate trebuie să fie stocate şi descrise în sisteme automate. Când este vorba de analiza şi sinteza automată, aceste procese pot fi dificil de implementat, ţinând cont de rata ridicată a complexităţii şi abstracţiei.

Faţa este considerată o sursă de informaţii, atât modelul static, cât şi cel dinamic, care necesită noi paradigme în analiză şi sinteză. Tot o sursă de informaţii poate fi, de exemplu, vocea, care ne permite să deducem informaţii din tonalitate, despre genul, vârsta, sănătatea, personalitatea, emotivitatea sau sociabilitatea unei persoane.

De asemenea, există aşa numitele distribuţii ale surselor de informaţie, care sunt de fapt regiuni ale feţei ce transmit semnale despre starea emoţională şi psihică a subiectului şi despre veridictatea sa. Astfel de regiuni sunt reprezentate de zona din jurul gurii şi a buzelor, zona din jurul ochilor sau sprâncenelor. În fapt, ochii sunt adesea cei mai buni indicatori ai stării emoţionale.

4.3. Transformări şi manipulări ale topologiei faciale

Când este analizată starea emoţională a unei persoane, cel mai precis rezultat este obţinut prin combinarea tuturor indicatorilor pe durata procesului de testare: faţă, voce, mişcări ale mâinilor, vorbire şi relaţia dintre expresiile faciale şi postura corpului. Când analizăm expresia facială este foarte important să reţinem faptul că acestea pot fi neveridice. Este posibil să citim expresiile faciale chiar dacă oferă informaţii voluntar sau involuntar.

Ţinând cont că aspectul facial poate fi considerat ca o structură topologică, o primă tehnică pentru sinteza expresiei faciale implică transformări topologice. Printre caracteristicile feţei care pot fi măsurate sunt aria, perimetrul, rotunjimea, curbele, adâncimile, simetria şi, desigur, diferite distanţe dintre două puncte esenţiale ale feţei. Există o serie de puncte caracteristice care ajută la identificare.

Analiza şi sinteza chipului necesită efectuarea unor serii de masurători. Printre ele, se află poziţia şi orientarea în spaţiu a capului, mişcarea ochilor şi direcţia privirii, mişcarea gurii şi a buzelor şi acţiunile muşchilor feţei.

Morphing este o altă tehnică pentru sintetizarea expresiei faciale, a vârstei, a genului, a rasei sau a altor trăsături statice sau dinamice. Analiza şi sinteza facială folosesc două tipuri de transformări faciale: locale şi globale. Primele implică schimbări într-o zonă locală, dacă este dată o zonă topologică divizată în părţi (de exemplu, zona ochilor sau a gurii) în scopul de a fi modelate individual. Combinarea lor conduce la diferite transformări faciale (relativ la vârstă, stare emoţionlă etc). Celelalte, transformările globale, prezintă un grad mai mare de complexitate, care dă corelarea între părţi. În concluzie, este preferată prima opţiune pentru că are o optimizare şi o rată a eficacităţii mai mare.

Putem obţine două tipuri de informaţii de la regiunile feţei (ochi, gura, sprâncene, buze): informaţii vizuale şi semnale electropsihologice. Cu ajutorul algoritmilor de procesare, informaţia vizuală este procesată în scopul identificării şi recunoaşterii faciale, generării (is processed in order to perform identi_cation and facial recognition, generation). Semnalele electropsihologice reprezintă activitatea muşchilor faciali, cum ar fi clipirile şi mişcarea ochilor. Între cele două tipuri de informaţii există o conexiune dată de corespondenţa dintre topologia unei regiuni locale feţei şi activitatea electrică a muşchilor corespunzători (Figura 4.3). Sintetizatorii faciali folosesc nişte serii de tehnici bazate pe modele topologice şi fizice pentru a interpreta într-un prim pas informaţia facială, apoi să o sintetizeze. Un exemplu este sincronizarea dintre discurs/vorbire şi mişcarea buzelor în cazul feţei sintetizate.

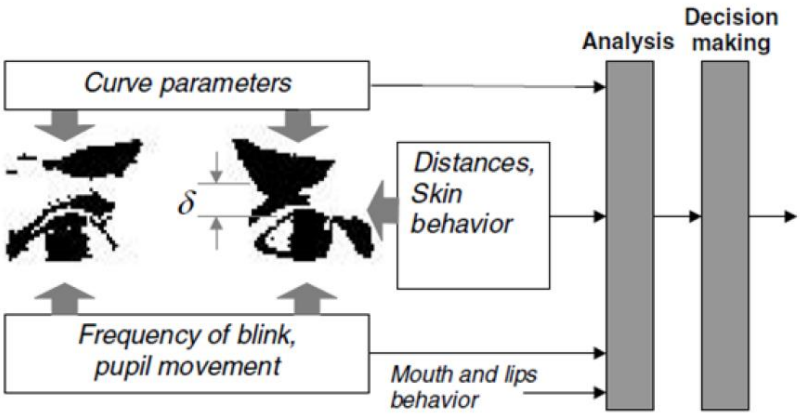

Figura 4.3 – Măsurarea comportamentului ochilor

Transmiterea facială necesită o tehnică bazată pe un sistem de codificare: iniţial, obiectul este identificat şi analizat pentru a crea un model al unui obiect tridimensional proiectat într-un spaţiu bidimensional. Imaginea astfel codată este transmisă şi după ce este primită, parametrii săi (incluzând trăsături ca forma, mărimea, poziţia) sunt decodaţi. Acest proces este urmat de sintetizarea imaginii. Codificatorul este bazat pe un model de analiză prin paradigma sintetizării, conţinând o copie a decodificatorului şi a feedback-ului iterativ, şi permiţând compararea intre cele două imagini: cea originală şi cea sintetizată.

4.4. Un nou framework pentru recunoașterea facială folosind criptografia vizuală

Criptografia vizuală [101] este o primitivă criptografică care descrie posibilitatea ca informaţia vizuală (poze, text etc) să fie criptată într-un mod în care decriptarea poate fi realizată cu sistemul visual uman, fără a fi nevoie de ajutorul computerelor.

Algoritmul folosit pentru criptare generează o imagine cifrată care este trimisă către destinatar printr-un canal de comunicare. Când această imagine este primită, sistemul sau utilizatorul setează cheia şi imaginea decriptată va fi obţinută. În Figura 4.4 putem vedea diagrama bloc a sistemului criptografic propus de Adi Shamir şi Moni Naor. Dimensiunea cheii este intre 50 şi 256 biţi cu posibilitatea extinderii până la 512 biţi.

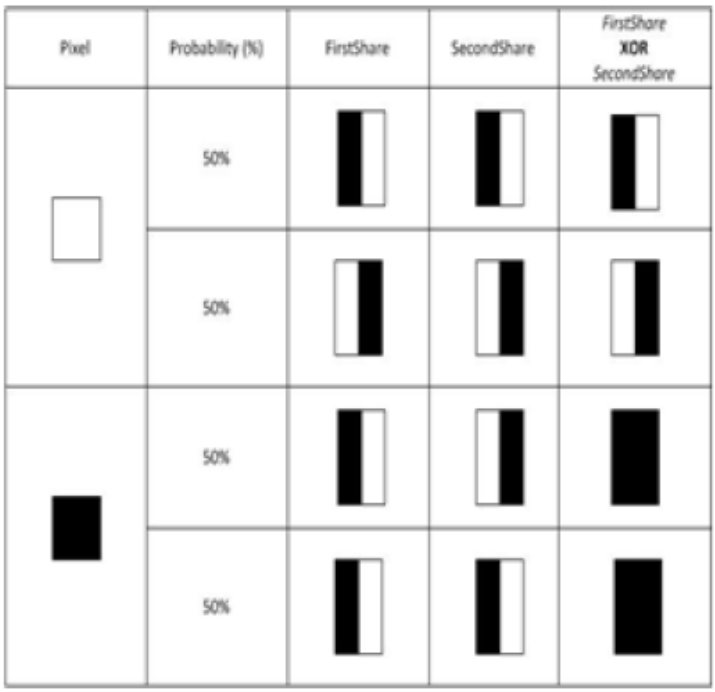

Figura 4.4 – Schema pentru codarea unui pixel binar în două partajări,

propusă de Naor și Shamir [101]

Am luat în considerare două caracteristici importante pentru a determina eficienţa sistemului criptografic propus [31]:

- Calitatea imaginii care este reconstruită

- Redimensionarea valorii factorului

Dacă există orice fel sau tip de pierdere a informaţiei în procesul fazei de reconstrucţie,

aceasta va conduce la reducerea calităţii imaginii recuperate. În cele mai multe cazuri, o imagine este reprezentată ca un spaţiu de culori RGB [76, 77], deoarece computerele, ca date de intrare şi date de ieşire, folosesc acest sistem de culori. Fiecare vector este format din trei componente care reprezintă intensitatea valorilor canalul în roşu, verde, albastru. Dacă este facută o schimbare în valoarea intensităţii, aceasta schimbă informaţia stocată în imagine. În acest caz, prin efectuarea unor schimbări în valorile intensităţilor, procesul de criptare a imaginii se poate efectua, iar procesul invers de decriptare va fi realizat cu succes. În cazul schimbărilor care au loc separat pe straturile roşu, verde, albastru vom avea un sistem criptografic vizual mai robust. Aceasta se datorează faptului că, dacă un intrus urmăreşte analiza completă a imaginii, trebuie să încerce să găsească valorile de bază ale intensităţilor, în vederea obţinerii imaginii originale. În acest caz, dacă criptarea a avut loc la un nivel de bază, spargerea sistemului va fi foarte dificilă.

Toate schimbările privind valorile intensităţilor sunt făcute folosind funcţii matematice. Toate conceptele criptografiei vizuale au fost introduse în 1994 de Naor şi Shamir. În [101], schema de codare propusă împarte imaginea binară în două distribuiri, *FirstShare* şi *SecondShare*.

Dacă un pixel este alb, atunci singura linie anterioară este aleasă pentru a genera *FirstShare* şi *SecondShare*. Acelaşi lucru se întâmplă dacă pixelul este negru. Fiecare pixel distribuit *p* este codat în doi pixeli albi şi doi pixeli negri. Fiecare partajare independentă nu oferă nicio posibilitatea să-şi dea seama dacă pixelul *p* este alb sau negru. În [101], autorii propun o tehnică de ascundere a unei imagini binare în două distribuiri semnificative folosind scheme de ascundere folosind domeniul spatial al imaginilor. Să reţinem că cele două partajări secrete sunt încorporate în două gray-level cover images, şi că, pentru a decoda mesajele ascunse, imaginile incorporate pot fi suprapuse. Ligu Fang [76] propune o schemă (2, *n*) bazată pe o combinație între doi parametrii, *contrast* și *expansiunea pixelilor*. Cei doi parametri sunt foarte importanți în criptografia vizuală.

Notația (2, *n*) înseamnă că dintr-un număr arbitrar *n* de oameni, cel puțin 2 dintre aceștia sunt somați să decodeze secretul. În schema prezentată de Moni Naor și Adi Shamir, avem o imagine secretă codată cu *n* partajări care sunt imprimate folosind transparențe. Partajările sunt aleatoare și conțin informații care nu pot fi înțelese despre imaginea secretă. Dacă oricare două partajări sunt plasate, una în partea superioară a celeilalte, imaginea secretă va deveni clară pentru ochiul uman. Fiecare pixel din imaginea secretă este codat în sub-pixeli multipli în fiecare imagine partajată folosind o matrice pentru a stabili culoarea pixelilor. În cazul (2, *n*) un pixel alb din imaginea secretă este codat folosind o matrice:

- permutarea coloanelor

$$C_0 = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & \dots & 0 & \end{bmatrix}$$

În timp ce un pixel negru din imaginea secretă este codat folosind o matrice:

- permutarea coloanelor

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \end{bmatrix}$$

Pentru corectarea codurilor de eroare, în [148] a fost definit un prag visual pentru scheme secrete vizuale de partajare a secretelor, care reprezintă un amestec între operațiile *XOR* și *OR* cu inversare. Aceasta înseamnă că cu o investigare a unui prag a schemelor de partajare vizuală secretă bazate pe amestecul operațiilor *XOR* și *OR* putem obține o inversare bazată pe un cod binar liniar de corectare a erorilor. Schemele criptografice vizuale (k,n) reprezintă o metodă perfect sigură cu care putem cripta o imagine secretă prin împărțirea ei în diferite umbre de imagini. Prin folosirea lor, putem integra în biometrie procesul de recunoaștere a feței, așa cum vom vedea în cele ce urmează. Un sistem Visual Crypto (VC) bazat pe polarizarea luminii care are rezoluție bună, proprietățile de contrast și culoare sunt folosite cu succes în framework-ul propus.

Newton [48] și Gross [122] propun un algoritm de de-identificare a feței care se concentrează pe probabilitatea minimizată a procesului automat de recunoaștere a feței, ținând cont de păstrarea detaliilor feței, cum ar fi expresia, genul sau vârsta.

Metoda propusă ia în considerare cerințele schemei de protecție a șablaonelor:

- Metricii de diversitate și revocabilitate. Diferite tipuri de aplicații vor folosi diferite seturi de date publice pentru selecția imaginii. Gazdele selectate pentru a cripta o imagine a feţei pot fi diferite în diverse aplicaţii. Este absolut necesar să revocăm șabloanele stocate și să eliberăm altele noi pentru o nouă imagine a feței prin schimbarea gazdelor [10, 51, 121, 47]
- Măsurători de securiate şi performanţă. Este foarte greu să obţinem prin calcul imaginea originală a feţei. Procesul de obținere este completat de șabloanele individuale stocate în sensul criptografiei vizuale [10, 36, 37, 50, 51, 52, 67, 70, 78, 99, 100, 102, 103, 121,123, 128, 134, 139, 141].

În Figura 4.5, procesul este foarte bine ilustrat. În faza inițială, persoana va sta în faţa unui aparat şi îi va fi scanată imaginea. Imaginea iniţială va fi criptată cu o cheie. Sistemul de criptare folosit este simetric. După ce imaginea este criptată cu un algoritm simetric, se realizează criptarea RSA asupra pachetului. Prin urmare, avem doi paşi de criptare. În primul pas este folosit un algoritm clasic, precum AES, TripleDES sau DES cu lungimea cheii cuprinsă între 56-256 biţi. În al doilea pas este folosită o cheie publică a algoritmului RSA. Aceasta va conduce la o criptare mai puternică a imaginii [48].

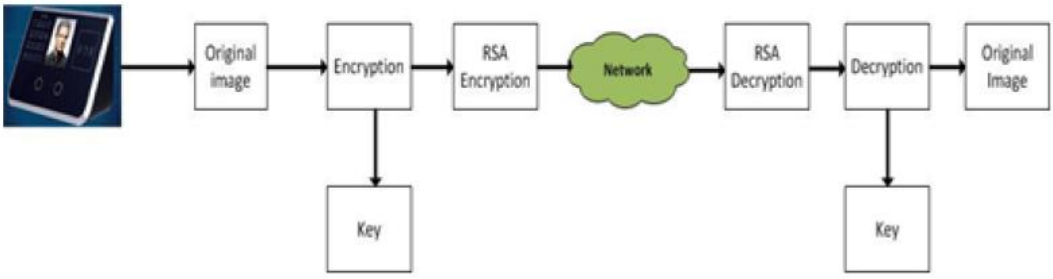

Figura 4.5 – Diagrama bloc a Framework-ului

Framework-ul generează altă imagine care va fi asemănătoare cu un strat al imaginii iniţiale capturată de la dispozitiv. Pachetul criptat astfel obţinut va fi stocat în altă imagine.

Schema vizuală criptografică (imaginea generată) va fi stocată în şablon, iar procesul de decriptare va fi făcut la nivelul bazei de date folosind algoritmul prezentat în Figura 4.5.

Schema principală folosită este o schemă criptografică vizuală de tip *k-out-of-n*. VSS-ul (*Verifiable Secret Sharing*) este o (*k, n*) VCS. În cazul nostru, imaginea binară originală va fi criptată în *n* imagini, ca:

$$T = S_{h_1} \oplus S_{h_2} \oplus \dots \oplus S_{h_k} \quad (4.3),$$

unde $\oplus$ reprezintă operaţia booleană, S_{h_i} ($h_i \in \{1,2,\dots,k\}$) reprezintă imaginea care va apărea ca un zgomot alb, $k \leq n$, iar n reprezintă numărul de imagini zgomotoase. Este foarte greu de decriptat o imagine T folosind o singură $S'_{h_i}s$.

Pornind de la definiţiile date mai sus, modelul schemei este definit:

- Imaginea umană (HI). Reprezintă imaginea capturată de la dispozitivul de citire. (vezi Figura 4.5, prima componentă de la stânga)
- Imaginea aleatoare (RI). Reprezintă o imagine generată automat de sistem. Această imagine, văzută ca un strat (layer), va fi suprapusă peste imaginea iniţială.
- Imaginea secretă (SI). Reprezintă imaginea în care originalul a fost ascuns.
- Gazda. Reprezintă imaginea care va fi folosită pentru a cripta imaginea secretă folosind un nivel de gri, cunoscut ca *Gray-level Extended Visual Cryptography Scheme* (Figura 4.6). În framework-ul nostru aceasta este reprezentată ca o corespondenţă între imaginile feţei care sunt în seturile de date publice.
- Şabloane. Imaginea va fi criptată în diferite şabloane mici care compun un şablon standard. Acestea vor apărea ca zgomot aleator (aici este vorba de (k,n) schemă criptografică vizuală) sau ca o poză normală (aici este vorba de cazul GEVCS, Figura 4.6).
- Ţinta (TA). Reprezintă imaginea reconstruită prin stivuirea sau superpoziţionarea şabloanelor mici.
- Expansiunea pixelilor (EP) este numărul de sub-pixeli folosiţi de şabloanele mici reprezentate de imaginile mici folosite pentru codarea fiecărui pixel din imaginea originală.
- Partajările (SH). Reprezintă criptarea fiecărui pixel care va fi criptat folosind o mulţime de *n* colecţii de *m* sub-pixeli negri şi albi, unde *m* este numărul de sub-pixeli negri şi albi.
- Contrastul relativ (RC). Reprezintă diferenţa în intensitate măsurată între doi pixeli diferiţi, unul negru şi altul alb în imaginea de destinaţie.
- Ponderea Hamming (HAM(V)). Reprezintă numărul de *l* biţi egali cu 1 din vectorul binar *V*.

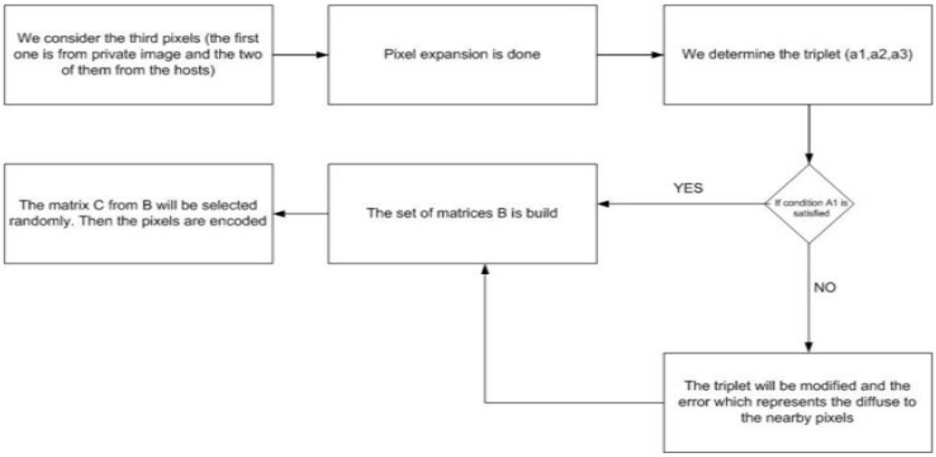

Figura 4.6 – Diagrama fluxului Grey-Level Visual Cryptography Scheme la nivel de pixel

Toate aspectele menţionate mai sus reprezintă nucleul aplicaţiei şi sunt integrate în framework. În Figura 4.7 este descrisă o privire de ansamblu a framework-ului şi cum funcţionează în viaţa reală.

Funcţia folosită în aplicaţie este o funcţie bijectivă. Informaţia originală a imaginii va fi regăsită pe parcursul procesului de decriptare fără a se confrunta cu vreo eroare [52-56]. Funcţia este:

$$g = \frac{1}{log(tan((exp(x) \cdot cos(exp(1)) \cdot sin(exp(A))))))}$$

unde *x* şi *l* reprezintă cheile, iar *A* reprezintă *cmmdc* dintre cele două chei folosinte în procesul de criptare.

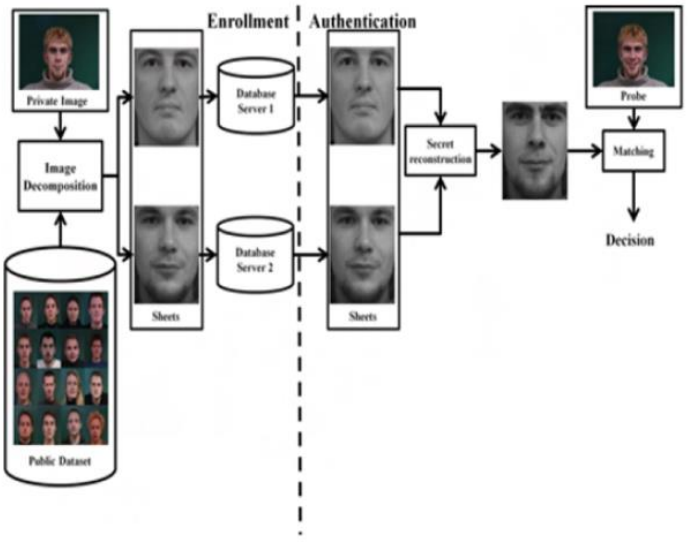

Figura 4.7 – Ilustrarea framework-ului propus

5. Prevenirea atacurilor algebrice asupra protocoalelor biometrice şi a protocoalelor RFID

Acest capitol îşi propune să demonstreze securitatea protocoalelor criptografice folosite în sistemele biometrice şi sistemele RFID [91]. Trebuie să ţinem cont de faptul că acestea sunt bazate pe expresii formale ale mesajului, considerând că mesajul de protocol va fi la un nivel înalt de abstractizare.

Într-un razboi informatic, asigurarea securităţii şi intimităţii datelor biometrice reprezintă o mare provocare şi necesită multă atenţie din perspectiva atacurilor.

Această contribuţie [22] prezintă diferite metode algebrice de verificare care, din punctul personal de vedere, reprezintă o combinaţie între cele două aspect menţionate mai sus. Aici vedem procesul de evaluare a securităţii protocoalelor prin luarea în considerare a algebrei termenului liber care este generat de mesajele care au fost schimbate între cele mai importante protocoale şi propuse de standardul propus de adversarul Dovlev Yao [134]. Autorii iau în considerare ca primitivele criptografice, cum ar funcţiile hash şi criptările, să fie perfecte. Când ne referim la aspectul computaţional, ne concentrăm pe cantitatea de informaţie compromisă datorită defectelor de securitate prin termeni în care sunt aplicaţi operatorii cu proprietăţi algebrice. Acest studiu nu îşi propune să arate care protocoale sunt sigure. Scopul principal este acela de a studia şi de a înţelege cum proprietăţi ale operatorilor algebrici şi ale funcţiilor pot fi folosite în protocoale de comunicare pentru a identifica motivul pentru care aceste protocoale nu funcţionează cum trebuie, şi de asemenea de a atinge scopurile de securitate. Teza prezintă trei categorii de vulnerabilităţi descoperite de studiul în domeniu şi analizarea protocoalelor publicate recent de RFID. Cercetarea caracteristicilor algebrice poate fi o unealtă folositoare în găsirea vulnerabilităţilor protocoalelor RFID.

Constrângerile de resurse impuse pe etichetele RFID au condus la o congestionare a propunerilor pentru protocoalele propuse folosind XOR, funcții de verificare redundanței ciclice, adunarea modular, și particularizarea funcțiilor hash. Încercarea de a demonstra că toate aceste protocoale sunt sigure folosind un model de securitate computaţională este inutilă şi nejustificată, pentru că un număr mare de protocoale care au fost propuse și răsturnate dovedite a fi greșite. Uneltele automate bazate pe metode formale abordate în prezent eşuează în verificarea securităţii celor mai multe protocoale, pentru că nu pot verifica anumite caracteristici de securitate, cum ar fi imposibilitatea de urmărire a etichetelor, sau nu consideră defectele datorate scurgerii parţiale ale cheilor.

Un cititor va lua în considerare cititorul RFID actual acelaşi ca potenţialul bazei de date sau comunicarea serverului cu cititorul, pentru că în toate protocoalele pe care le considerăm, comunicarea se realizează printr-un canal sigur. Un agent poate avea două identităţi, o etichetă sau un cititor, în timp ce un rol se referă la paşii protocolului, o etichetă sau un cititor este așteptat să ducă la bun sfârșit. O rulare reprezintă execuția unui rol de către un agent. Pentru intuiţie şi comoditate, vom face o referinţă despre diferite atacuri specifice care ţin locul protocoaleor ca atacuri calitative în timp. Există atacuri în care adversarul interacţionează cu o etichetă în absenţa unui cititor RFID sincer sau de încredere. Scopul unui astfel de atac este să trimită foarte atent provocări etichetei pentru a obţine diferite tipuri de informaţii vitale şi care, mai târziu, vor juca rolul unui cititor sau a unei etichete, urmărirea etichetei (tag) sau să atace orice tip de cerință a securității a unui protocol. Atacurile calitative în timp sunt des întâlnite în structuri mobile și structuri wireless, structuri naturale ale etichetelor RFID. Atacurile pot fi

realizate asupra etichetelor care se întâmplă să fie în vecinătatea unui adversar pentru o scurtă perioadă de timp sau etichete unde atacatorul este capabil să le izoleze de natura lor pentru o perioadă mai mare de timp.

În acest capitol lucrurile sunt simplificate pentru prezentarea protocoalelor de câte ori este posibil, prin sărirea unor anumiți număr de pași, termeni, comunicare redundantă. Descrierea oferă suficiente informații pentru reconstruirea atacurilor asupra protocoalelor originale. Când vorbim despre imposibilitate detectării unui protocol, înțelegem faptul că etichetele nu pot fi urmărite.

Pentru confortul cititorilor, este foarte important cum este realizată descrierea protocolului. De exemplu, folosim frecvent următoarele notații:

- k , pentru o cheie secretă distribuită;
- h, pentru funcțiile hash;
- $r_1, \dots, r_n$ pentru valorile de tip *nonce*;
- ID, care reprezintă ID-ul etichetei.

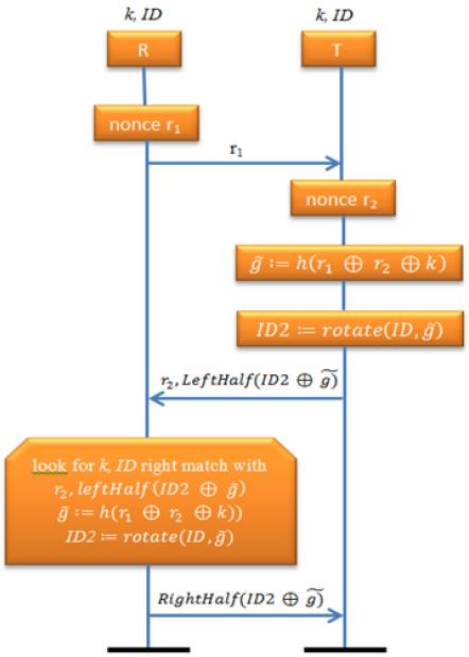

Figura 5.1 – Protocol de autentificare greșit

Vor exista cazuri speciale care vor necesita adunare și variabile, iar atunci vom folosi notația propusă de autorii protocolului.

Când un atac este compus din mai multe rulări, termenii folosiți în a doua rulare sunt primi.

În această lucrare prezentăm protocoalele în mod grafic, folosind diagramele de secvențe UML, ca în Figura 5.1. Fiecare mesaj prezentat în diagramă ilustrează numele rolurilor. Mai sus de numele rolurilor, sunt arătate rolurile termenilor secreți. Un chenar reprezintă acțiunile, cum ar fi generarea valorilor de tip *nonce*, calcul și atribuiri. Săgețile care conectează rolurile reprezintă mesajele care sunt trimise și se așteaptă să fie primate sunt specificate mai sus. Un agent va continua executarea procesului doar dacă primește mesajul în acord cu specificațiile. Alte condiții care trebuie îndeplinite sunt illustrate în chenarele romb. Să luăm, de exemplu, în Figura 5.1 , numele rolurilor sunt identificate de *R* și *T*, ambele sunt

cunoscute ca *k* şi *ID*, care sunt termenii secreţi. *R* va genera valoarea de tip *nonce* r_1 înainte de trimiterea primului mesaj. Când este primit mesajul, *T* va genera o valoare de tip *nonce* şi va calcula răspunsul. Cititorul va accepta răspunsul doar dacă condiţia de găsire a perechii (*k, ID*) este satisfăcută; perechea va genera acelaşi termen când îi este aplicat procesul de calcul arătat. Cititorul va continua cu calculul şi trimiterea ultimului mesaj în cazul în care este acceptat răspunsul.

5.1. Caracteristici de securitate şi proprietăţi. Modele ale adversarilor

Această secţiune începe cu studiul lui Gavin Lowe [135], în care autorul sugerează că, o cerinţă de autentificare adecvată va depinde de momentul folosirii protocolului şi va indentifica mai multe definiţii posibile ale autentificării. În ierarhia atentificarii lui Lowe, observăm că acesta ia în considerare cea mai recentă vivacitate pentru a fi cele mai adecvate cerinţe de autentificare pentru protocoalele RFID. Vivacitatea recentă prind faptul că eticheta necesită a avea generat un mesaj ca rezultat al cererii unui cititor. Luăm în considerare noţiunea de *nedetectabilitate* definită de Van Deursen în [136] în care autorii pun accentul pe faptul că o etichetă este nedectabilă dacă, pentru oricare două protocoale care rulează, o persoană nu poate spune dacă aceeaşi etichetă a executat ambele rulări sau dacă două etichete diferite au executat rulările. În final, termenii care nu sunt cunoscuţi de adversari se spune a fi secreţi.

5.2. Atacuri asupra autentificării bazate pe răspunsuri algebrice

Multe studii pun accentul pe moduri comune de a autentificare a etichetelor RFID, accentul fiind pus pe mecanismul de răspuns-provocare. Cititorul RFID trimite provocări (*challenge*) etichetei folosind o valoare aleatoare de tip *nonce* r_1 în care eticheta furnizează o replică cu un termen derivat din r_1; anumite informaţii reprezintă indentificarea etichetei, şi potenţial o valoare de tip *nonce* este generată de etichetă. Dacă există, valoarea r_2 reprezintă procvocarea etichetei pentru cititor în autentificarea reciprocă sau ca "termen de orbire" (*blinding term*) pentru a obţine nedetectabilitatea etichetei. Putem reprezenta răspunsul etichetei la provocarea cititorului ca perechea $r_2, g(r_1, r_2, s)$ cu menţiunea că r_2 poate fi constant sau poate lipsi. Cititorul verifică autenticitatea prin aplicarea inversei funcţiei g asupra termenului şi verificarea dacă răspunsul conţine r_1şi un *s* valid. Dacă g este funcţie de tip one-way, atunci cititorul verifică autenticitatea etichetei calculând funcţia $g(r_1, r_2, s)$ şi comparând-o cu valoarea primită. Cititorul va putea calcula această funcţie, valoarea r_1, pentru că valoarea este generată de el însuşi, valoarea r_2 este furnizată de etichetă, cititorul are o bază cu valorile lui *s* pentru fiecare etichetă. În continuare demonstrăm că următoarele două proprietăţi sunt necesare pentru mecanismul provocare – răspuns pentru garantarea vivacitatea recentă a etichetei.

Proprietate. Pentru r_2 şi *s* fixate, intervalul funcţiei $r_1 \rightarrow g(r_1; r_2; s)$ trebuie să fie mare. Mai precis, dându-se r_2 şi *s*, avantajul adversarului în ghicirea valorii corecte $g(r_1, r_2, s)$ pentru un r_1 necunoscut, arbitrar ales, trebuie să fie neglijabil.

ARR (Algebraic Replay Resistance). Fie *Os*(*x*) un oracol care pentru data de intrare *x*, alege aleator *y* şi returnează *y* şi *g*(*x*;*y*;*s*). Dacă nu se cunoaşte *s*, atunci accesul dat la un număr polinomial de cereri $Os(x_1), \dots, Os(x_l)$ la oracol nu este posibil.

Dacă este satisfacută această proprietate, atunci, aşa cum am stabilit, probabilitatea ca adversarul să găsească $g(r_1, r_2, s)$ este neglijabilă. Astfel, cu o probabilitate mare, un răspuns $r_2, g(r_1, r_2, s)$ la provocarea cititorului r_1 trebuie să fi fost generată după ce provocarea a fost trimisă. Această proprietate este evident necesară pentru vivacitatea recentă şi, în particular, exclude răspunsurile de atac clasice. Proprietatea ARR garantează că nu există un algoritm eficient de calcul al răspunsului $r_2, g(r_1, r_2, s)$ la provocarea $r_1$chiar şi după aflarea perechilor provocare-răspuns anterioare. Abilitatea unui atacator de a calcula un astfel de răspuns încalcă vivacitatea recentă şi această proprietate este necesară pentru el. Un astfel de atac generalizează atacuri pe bază de răspuns în loc pur și simplu să răspundă cu informația anterioară; atacatorul combină perechile provocare – răspuns obţinute anterior pentru a calcula răspunsul unei noi provocări. Prin urmare, ne referim la atacuri pe protocoale de autentificare provocare – răspuns exploatând lipsa proprietăţii ARR ca atacuri algebrice pe bază de răspuns.

Este evident că, pentru ca o funcţie să aibe proprietatea ARR, trebuie să menţină valoarea *s* secretă. Într-adevăr, funcţiile criptografice hash sunt folosite frecvent în tipul de mecanism provocare – răspuns considerat aici. În timp ce proprietatea de rezinstenţă la coliziune a funcţiilor criptografice hash nu este necesară pentru mecanismul provocare – răspuns, se ridică întrebarea dacă toate funcţiile de tip one-way satisfac proprietatea ARR, iar răspunsul este negativ. Este cu siguranţă fals pentru toate funcţiile de tip one-way homomorfice. Să considerăm, de exemplu, funcţia Rabin definită de $x \to x^2 mod\ N$, pentru un număr întreg compus *N* dat. Dacă $(r_1, r_2, s) \to g(r_1, r_2, s) = (r_1, r_2, s)^2\ mod\ N$ este o funcţie Rabin, atunci, dându-se o singură pereche provocare – răspuns $r_1, g(r_1, r_2, s)$ este uşor de calculat răspunsurile pentru orice provocare r_1', întrucât $g(r_1', r_2, s) = g(r_1, r_2, s) \cdot (r_1', r_2)^2$.

În plus, chiar funcţiile non-homomorfice de tip one-way, în general nu au proprietatea ARR dacă argumentele lor au proprietăţi algebrice. Cum am demonstrat în exemplele de mai sus, există mai multe protocoale care eşuează în obţinerea vivacitatea recentă datorită acestui motiv. În aceste protocoale construcţia provocare – răspuns poate fi reprezentată ca $g(r_1, r_2, s) = f(n \cdot r_2, s)$, unde *f* este funcţie criptografică hash (non-homomorfă) şi ° defineşte un operator cu următoarele proprietăţi algebrice. Fiind date *a*, *b*, *c* este uşor de găsit *d* astfel încât $a \cdot b = c \cdot d$. Această construcţie, în mod evident nu are proprietatea ARR, datorită proprietăţilor lui *f*. Atacul algebric de tip răspuns asupra unui astfel de protocol lucrează după cum urmează. Un adversar care observă o execuţie a protocolului, află r_1, r_2 şi $f(r_1 \circ r_2, s)$. Când este provocat cu r_1', adversarul găseşte r_2' astfel încât $r_1 \circ r_2 = r_1' \circ r_2'$ şi răspunde cu r_2' şi $f(r_1 \circ r_2, s)$. Atacul are success pentru că $f(r_1 \circ r_2, s) = f(r_1' \circ r_2', s)$.

Exemple de operatori ° pentru care aceste tipuri de atac se termină cu succes sunt *XOR*, adunarea modulară şi orice operator asociativ pentru care este uşor de calculat inversul la stânga.

5.3. Exemple de operatori °

În această secțiune am introdus cele mai recente exemple de atacuri atacurile algebrice de tip răspuns și de asemenea unde pot fi găsite. Un alt aspect important pe care îl prezentăm în secțiunea curentă sunt noile atacuri.

- În articolul [79], Lee și coautorii descriu detaliat protocolul propus, care este foarte vulnerabil la atacul algebric de tip răspuns în care adversarul trebuie să observe trei execuții ale protocolului sau să realizeze un atac de tip quality-time compus din trei

cereri. Executarea atacurilor algebrice de tip răspuns poate fi rezolvat cu un mic sistem de ecuații influențabil. Acest tip de atac a fost prima dată descris de Bringer în [27].

- Mecanismul provocare – răspuns propus de Chien H. Y. [30] folosește funcția XOR cu verificare ciclică a redundanței. Când avem o provocare r_1, eticheta va răspunde cu $r_2, CRC(EPC, r_1, r_2) \oplus k$, unde EPC reprezintă o constantă care identifică eticheta. În lucrarea lui Peris – Lopez [112] este prezentat atacul asupra protocolului. Observăm că CRC este homomorfism, i.e. $CRC(a) \oplus CRC(b) = CRC(a \oplus b)$.

Articolul prezintă un atac complet asupra protocolului propus de Chien și Huang [30], atac ilustrat în Figura 5.1. Cititorul *R* și eticheta *T* partajează *k* și *ID* – ul secrete. Cititorul începe cu trimiterea unui string aleator de biți r_1. Eticheta generează un șir aleator r_2 și hash-ul operației XOR între r_1, r_2 și *k*. Hash – ul și *ID*-ul sunt folosite ca date de intrare pentru o funcție în care *ID*-ul este rotit cu o valoare care depinde de hash-ul respectiv. Eticheta calculează XOR-ul dintre *ID*-ul rotit și hash-ul, înainte de a trimite jumătatea stângă a șirului de biți rezultat și valoarea r_2 către cititor. Cititorul îndeplinește aceleași operații pentru fiecare pereche formată din *ID* și *k* până găsește eticheta corespunzătoare. Apoi trimite jumătatea dreaptă a biților corespunzători către etichetă.

Pentru a juca rolul unei etichete este suficient să observăm că răspunsul etichetei la provocarea cititorilor depinde doar de $r_1 \oplus r_2$ și cheia secretă distribuită. Procesul de compunere al funcțiilor aplicate pe XOR și cheia secretă distribuită poate fi reprezentat de funcția *f* pe care am definit-o mai sus. Deci, adversarul poate avea un rezultat cu un atac de tip quality – time prin trimiterea unei provocări etichetei cu orice r_1 cu care are o combinație validă între r_1, r_2 și $Left(ID2) \oplus \bar{g}$. Aceste tipuri de informații sunt suficiente pentru ca adversarul să fie capabil să răspundă oricărei provocări viitoare r_1' primită de la un cititor.

5.4. Descrierea protocolul LD

Protocolul LD [42] a fost dezvoltat ca un protocol de autentificare reciprocă pentru etichete RFID care pot fi rescrise, garantând nelegarea etichetelor în rețeaua furnizată și nu numai. Fiecare rețea suplimentară conține o rețea de parteneri, fiecare fiind reprezentat de un cititor. Fiecare cititor R_i conține o cheie secretă k_i și cheia secretă a următorului cititor, k_{i+1}. În plus, fiecare cititor stochează identitatea *c* a fiecărei etichete care se poate autentifica. Fiecare etichetă *T* conține un pseudonim α, ce reprezintă o identitate temporară. Valoarea α este egală cu $c \oplus k_i$, unde k_i reprezintă cheia secretă a unuia sau mai multor cititori R_i care la momentul curent permite identificarea şi autentificarea etichetei.

Protocolul LD este un protocol bazat pe provocare – răspuns. Cititorul R_i trimite o provocare etichetei *T* cu valoarea de tip nonce *r*. Următorul pas constă în calcularea XOR-ului între cheia secretă curentă şi provocarea *r* şi va răspunde cu digest al acestei valori. Cititorul va considera eticheta autentică dacă va găsi o cheie secretă *c* pentru care $h(c \oplus r \oplus k_i)$ este egal cu răspunsul primit. În acest moment, cititorul va putea opri execuția protocolului oferind posibilitatea etichetei de a se autentifica din nou, într-o sesiune a unui proces de comunicare viitor. Avem un aspect alternativ: cititorul poate, de asemenea, să trimită etichetei o actualizare $a = k_i \oplus k_{i+1}$, însoțită de $b = h(a \oplus c \oplus k_i)$. Apoi eticheta va verifica dacă $b = h(a \oplus \alpha)$ şi va actualiza cheia secretă α, aplicându-i XOR cu *a*. Prin aceasta, posesorul etichetei *T* va fi transferat de la cititorul R_i la cititorul R_{i+1}. Protocolul este prezentat în Figura 5.2.

Un aspect negativ al protocolului LD este faptul că nu a fost dezvoltat pentru a fi nedetectabil, ci doar fără legătură directă. O etichetă nu va introduce nimic aleator în răspunsul său către o cerere care provine de la un cititor, ceea ce implică faptul că o etichetă este detectabilă între două actualizări de chei. Vom vedea în secţiunea următoare că protocolul LD nu va furniza nedetectabilitate, nici prin expunerea acestei proprietăţi. Expunerea din această secţiune este bazată pe analiza LD din [43].

Primul pas este acela de a demonstra că protocolul nu satisface nedetectabilitatea. Pentru aceasta, este suficient să prezentăm un caz în care adversarul recunoaşte o etichetă observată anterior după ce eticheta care a actualizat cheia secretă.

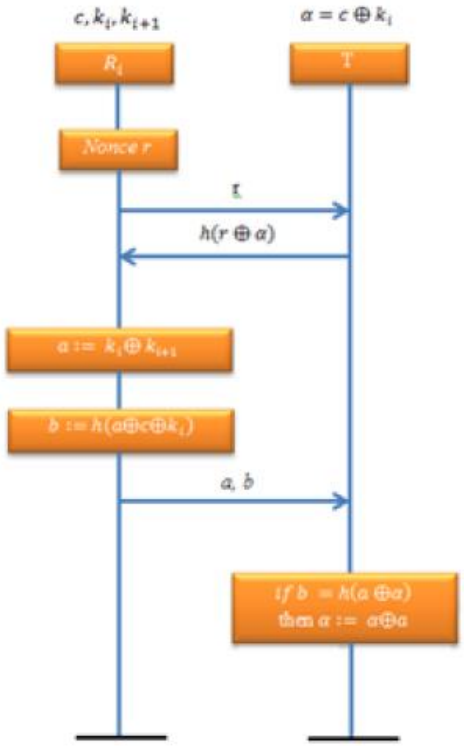

Figura 5.2 – Protocolul RFID pentru rețele suplimentare

Problema este dificilă în cazul interceptării unei sesiuni de autentificare validă. Între o etichetă şi un cititor, adversarul află $r, h(r \oplus \alpha), a, b$. La finalul execuţiei, eticheta va actualiza cheia sa secretă α prin înlocuirea cu $r' = r \oplus a$, căreia eticheta îi va răspunde cu $h(r' \oplus \alpha')$. Folosind o proprietate algebrică simplă a operaţiei XOR, răspunsul va fi egal cu cel anterior pe care l-am observat:

$$h(r' \oplus \alpha') = h(r \oplus \alpha \oplus \alpha \oplus \alpha) = h(r \oplus \alpha) \quad (5.1)$$

În figura 5.4 putem observa atacul.

Putem presupune că o persoană rău intenţionată nu este capabilă să se apropie destul de o etichetă în timp ce este actualizată, în concluzie, nedetectabilitatea poate fi ipotetic spartă. Astfel, putem presupune că un adversar poate şi este capabil să intercepteze mesajele cititorilor. În plus, putem presupune că persoanele rău intenţionate pot cere produse de intrare şi de ieşire în timp ce se află în afara ariei persoanei bine inţenţionate. Deci, următoarele extensii ale atacului de mai sus devin atunci reale şi plauzibile în contextul rețelei suplimentare. Atacatorul va genera o valoare de tip nonce r şi va cere toate produsele de intrare care au această valoare. Să ne oprim asupra ecuaţiei (5.1), unde interceptarea mesajului de la cititor la etichetă este suficient pentru a fi capabili să potrivească răspunsul produsului de intrare cu răspunsul produsului de ieşire şi astfel să legăm cele două produse. Ultimul mesaj de la cititor la etichetă

în protocol în [91] conţine valoarea actuală în care eticheta ar trebui să actualizeze cheia sa. Mesajul poate fi observat şi folosit de adversar pentru a sparge nedetectabilitatea.

După cum putem vedea în [91] trebuie să considerăm că adversarul poate alege aceeaşi valoare de tip nonce $r = r'$ pentru provocare înainte ca o etichetă să fie actualizată şi după ce eticheta este actualizată. Este demonstrat că în acest caz adversarul nu poate lega cele două răspunsuri $t = h(r \oplus c \oplus k)$ şi $t' = h(r \oplus c' \oplus k')$ fără a avea vreo cunoştinţă despre chei. Deci, setarea $r = r'$ nu este cea mai bună tactică şi soluţie pentru adversar. Să vedem de ce:

$$h(r \oplus c \oplus k) = h(r \oplus c' \oplus k') \Leftarrow r \oplus c \oplus k = r' \oplus c' \oplus k' \Leftarrow r' = r \oplus k \oplus k' \wedge c = c' \qquad (5.2)$$

Setarea $r' = r \oplus k \oplus k'$ este o alegere mai bună pentru adversar. Să ne amintim că k şi k' nu sunt chei ale unor cititori succesivi. Doar prin observarea procesului de actualizare a cheilor pentru o reţea de cititori $R, \dots R'$ care sunt trimise etichetelor, persoanle rău inteţionate pot calcula $k \oplus \dots \oplus k' = k \oplus k'$.

Greşeala din protocolul LD care afectează nedetectabilitatea se datorează chiar proprietăţii algebrice a XOR-ului, arătată în ecuaţia (5.2).

Această greşeală poate fi evitată dacă concatenarea dintre termenii care pot fi găsiţi în interiorul funcţiei hash este folosită, în loc de operatorul XOR, dacă cititorul trimite $h(a, (c \oplus k_i))$ în loc de $b = h(a \oplus c \oplus k_i)$, unde virgula reprezintă procesul. Concatenarea, care face calculul funcţiei hash mai expresiv pentru etichetă, reprezintă o alternativă mult mai bună.

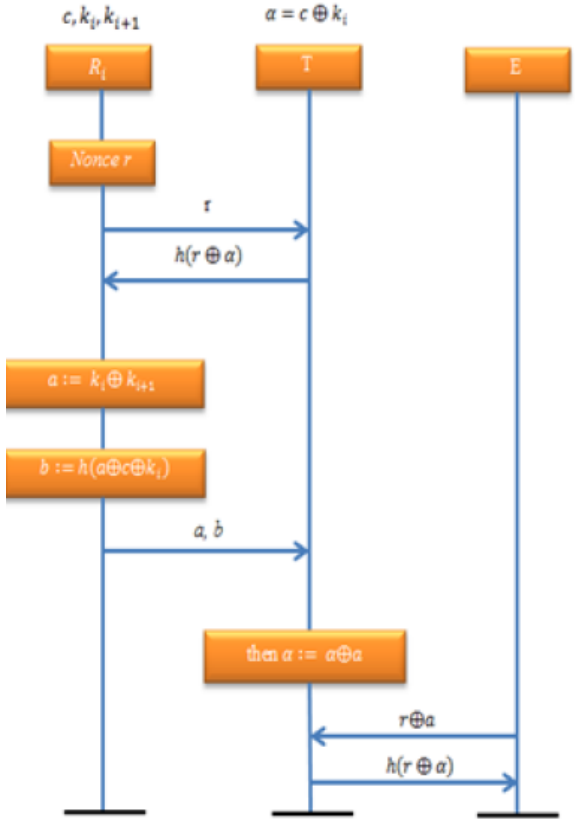

Figura 5.2 – Protocolul RFID pentru reţele suplimentare

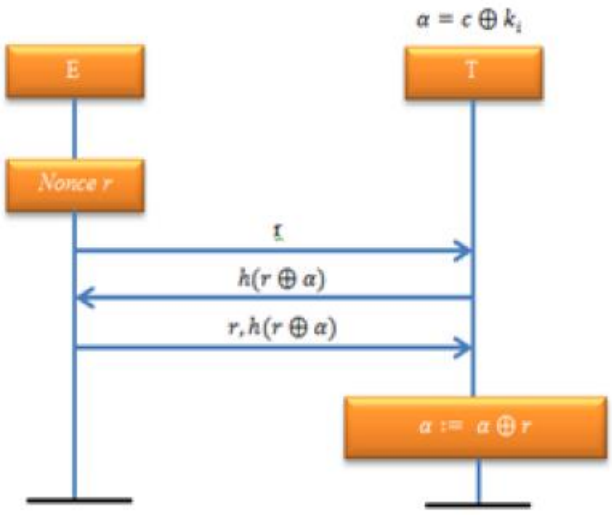

Figura 5.3 – Ilustrarea atacului asupra autentificării

6. Semnături biometrice on-line și off-line

Acest capitol am discutat și propus un algoritm care se bazează pe două metode de generare a semnăturii: *intra-class*, calea către o semnătură independentă de baza de date cu semnături exemplu, și *in-class* care are în vedere setul de semnături atunci când o semnătură sintetică este procesată.

Una dintre cele mai importante trăsături biometrice în biometria inversă este semnătura. De asemenea, este unul dintre cele mai vechi moduri de identificare a unei persoane, cu mult înainte de folosirea amprentei sau a altor caracteristici biometrice moderne. Oamenii au încercat de secole să falsifice semnăturile sau scrisul de mână, în general. Pe de altă perte, au existat oamnei care au încercat să detecteze falsurile. Cel mai ușor mod de a recunoaște a fost falsificarea manuală, cât sunt de diferite față de original, în raport cu forma, dimensiunea. În prezent, semnăturile de mână fac posibilă analiza unor alte caracteristici ale semnăturilor, cum ar fi presiunea mâinii, viteza de scriere, dinamica, accelerația, durata scrierii etc.

Când avem de-a face cu procesul de semnare, este util să folosim atât transformările directe, cât și cele inverse. Primele sunt folosite pentru colectarea semnăturilor în vederea stocării într-o bază de date și analiza ulterioară, iar celelalte pentru colectarea semnăturilor sintetice. Apoi urmează un al doilea pas: validarea și analiza semnăturilor sintetice. În acest capitol vom prezenta câteva tendințe în problema directă și cea inversă cu privire la semnături. Apoi se pune problema sintezei automate a semnăturilor. Vom descrie câteva dintre cele mai folosite modele de sinteză împreună cu algoritmii necesari și direcții pentru cercetări viitoare.

7. Concluzii și direcții viitoare de cercetare

Prezenta lucrare de doctorat descrie diverse scheme și metode generalizate de autentificare biometrică pentru îmbunătățirea gradului de securitate cu multe posibile componente interconectate, de la semnătura holografică, utilizabilă în toate domeniile unde sunt necesare identificarea utilizatorilor, până la recunoașterea facială, care este utilizată în multe sisteme de autentificare. Întrucât semnătura a reprezentat de-a lungul secolelor un mijloc de autentificare, pe baza amprentei biokinetice a semnăturii umane există un punct de plecare alternativ și complementar pentru dezvoltarea tehnologiilor informatice de autentificare.

În ultimul deceniu au fost realizate progrese semnificative și strategice în ceea ce privește performanța sistemelor biometrice. Viitoarele aplicații vor necesita un nivel înalt de performanță în scenarii imaginate nu tocmai ideale. Zona perioculară din procesul de recunoaștere facială a fost propusă ca o potențială sursă de caracteristici biometrice și ca viitoare direcție de cercetare.

Principalele obiective ale acestei teze au fost următoarele:

- Să stabilească cerințele și configurația operațională pentru vulnerabilități în sistemele biometrice de autentificare bazate pe semnătură on- și off-line și pe recunoaștere facială. Am prezentat cerințele, serviciile, arhitectura aplicațiilor și configurația operațională pentru protecția datelor personale, utilizând ultimele tehnologii, care vor fi capabile să asigure un management al securității identității și a pseudo-identităților utilizând tehnologii biometrice pentru protejarea datelor cu caracter biometric (Figura 7.1)

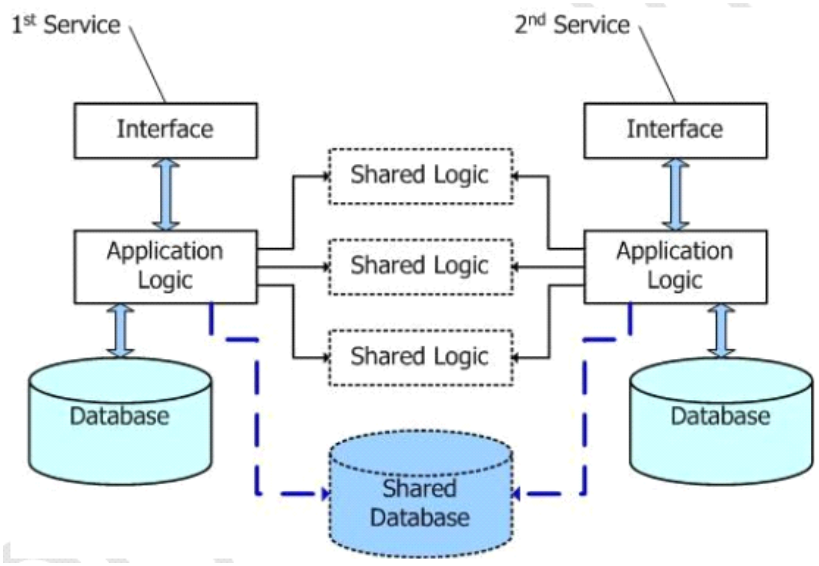

Figura 7.1: Schemele de serviciu

- Să propună o schemă interoperabilă de protecție a șabloanelor pentru semnăturile on-line și off-line. Această parte reprezintă o cercetare dedicată asupra aspectelor și mecanismelor ce asigură faptul că informațiile biometrice protejate nu pot fi inversate sau utilizate cu scopul de a extrage mostra biometrică originală. Pentru mai multe detalii, vezi Secțiunea 6.3 prezentată în teză. Aici este definită și implementată o soluție tehnologică ce oferă posibilitatea de a revoca o identitate biometrică protejată

(semnătură holografică, amprente, card inteligent etc.) și de a procesa mostra biometrică cu scopul de a genera diverse soluții de securitate pentru șabloanele biometrice.

- Protocoalele criptografice, evaluarea atacurilor la adresa identității. Scopul acestei cercetări, detaliat în Secțiunile 3.1, 6.1, prezentate în teză și Capitolul 5, este acela de a desemna protocoalele criptografice și metodele statistice pentru a proteja și coordona identitatea bazată pe semnătura holografică, amprente și/sau carduri inteligente. Au fost prezentate diverse scenarii de atac, evaluare și raporturi de analiză, iar securitatea este evaluată cu ajutorul variilor tipuri de atacuri.
- Evaluarea noilor tendințe în datele cu caracter personal, performanță și interoperabilitate. Secțiunile 3.3, 3.2, 3.4, 4, 6.2, 6.4, 6.5, prezentate în cadrul tezei, au pus accentul pe găsirea unor noi mecanisme de protecție, noi algoritmi și tehnologii pentru recunoașterea semnăturilor. Sunt prezentate și demonstrate mecanisme pentru interoperabilitate comparativă sau de tip benchmarking și o evaluare a capabilităților de performanță în cazul semnăturilor on-line și off-line și a procesului de recunoaștere facială. Demonstrația activităților este ilustrată și divizată în două părți:
    - Teste de performanță asupra interoperabilității biometrice;
    - Indicatorii utilizatorilor finali și a furnizorului de servicii au ocupat un loc important în teză, alături de evaluarea acestora. Aici demonstrăm cum o singură semnătură holografică sau amprentă (pe baza caracteristicilor primare ale unei persoane) pot genera câteva identități având diferite niveluri de încredere. Problema va fi modul acestora de utilizare și cum poate fi revocată o pseudo-identitate bazată pe semnătura holografică sau pe amprentă, și cum pot fi re-generate noi identități pe baza acelorași caracteristici biometrice ale unei persoane. Metodele de protejare a preferințelor biometrice vor fi evaluate pentru diferite cazuri generice sau din viața reală.

Noua schemă și studiile din cadrul tezei au ca scop protecția șabloanelor biometrice printr-o transformare criptografică a semnăturii sau a imaginii faciale într-o cheie non-invertibilă care va permite o comparație bit cu bit. Pentru a câștiga încrederea utilizatorului, cheia va fi, de asemenea, revocabilă, o nouă cheie independentă putând fi generată prin utilizarea aceleiași amprente.

În continuare, aș dori să menționez principalele contribuții personale și obiective care au fost atinse în lucrarea de față, însoțite de secțiunea unde au fost prezentate.

- **Cadrele biometrice (Capitolul 3).** În acest capitol ne-am concentrat asupra diferitelor aspecte ale problemelor inverse ale biometriei [96]. În [96] am definit și explicat noțiunile de probleme inverse și directe ale sistemelor biometrice. Am introdus o nouă paradigmă bazată pe probleme directe și inverse. În [97] ne concentrăm pe unul dintre exemplele proeminente ale biometriei inverse, denumit semnături sintetice. În Secțiunea 3.2 am prezentat o contribuție personală; [3] se concentrează pe toate aspectele tehnologice și de fezabilitate utilizate în dezvoltarea de aplicații, cum ar fi pașapoartele biometrice [25]. Lucrările [117] și [118] explică necesitatea implementării corecte a interfeței și acțiunile(care actiuni?). Am prezentat câteva experimente care pot fi de asemenea implementate în selecția directă a unui prag adecvat, relativ la asigurarea unei cantități mari de informație utilă.
- **Prevenirea atacurilor algebrice împotriva protocoalelor biometrice și RFID (Capitolul 4)**. Acest capitol este dedicat securității protocoalelor biometrice și RFID și modului în care putem preveni atacurile algebrice împotriva acestor protocoale. Ca o contribuție personală, ne-am concentrat asupra securității protocoalelor criptografice

utilizate în procesul de autentificare în sistemele biometrice și RFID [91], considerând că protocoalele bazate pe schimbul de mesaje va avea un grad înalt de abstractizare.

- **Recunoașterea facială (Capitolul 5).** Acest capitol se concentrează pe diferite caracteristici și aspecte tehnice ale problemelor directe și inverse legate de recunoașterea facială. În [97] considerăm caricaturile faciale, sintetizatoarele și transmisia ca un mod aparte de a descoperi ce anume scoate în evidență o anumită trăsătură a unei anumite persoane. Începând de la [97], am propus un nou cadru pentru recunoașterea facială biometrică [89], bazat pe tehnici vizuale de criptografie. Cadrul este conceput și dezvoltat în limbajul de programare C# și se concentrează pe rolul criptografiei vizuale pentru a proteja și cripta imaginea facială cu ajutorul RSA, prin crearea unei scheme criptografice vizuale secrete ce va proteja imaginea de indivizi rău intenționați, pe parcursul procesului de autentificare. Am explicat pașii ambelor faze, criptare și decriptare.
- **Semnăturile biometrice online și offline (Capitolul 6).** Acest capitol pornește de la premisa comparației dintre minim două specimene de semnătură, oferite de aceeași persoană. Contribuția [88] prezintă un cadru (instrument software) pentru recunoașterea biometrică optică a cifrelor scrise de mână utilizând Kernel Discriminant Analysis. Cadrul este conceput în limbajul de programare C#. În [95] am demonstrat cum este utilizată analiza discriminantă în procesul de recunoaștere a scrisului de mână. O schemă de înrolare pentru șabloanele biometrice fundamentate pe criptografia cu funcții hash bazată pe haos este propusă în [93]. Pentru alte funcții hash bazate pe haos, vezi Anexa A.1. Scopul acestei scheme este de a crea un proces de autentificare puternic și unic al șabloanelor biometrice. Secțiunea 6.4.1 din teză prezintă ATHOS (Serviciul Automat de Autentificare utilizând Semnătura Biometrică)-POS-CCE 208/20.07.2010 dezvoltat și propus de SOFTWIN, una dintre cele mai mari companii românești în doemniul Tehnologiei, Informației și Comunicării. Am participat timp de câteva luni în cadrul acestui proiect de cercetare, în calitate de membru și angajat în Procesare Paralelă și Criptografie. Pe parcursul implicării mele în acest proiect, am propus două contribuții, [90] și [92].

  În [90] am prezentat o privire de ansamblu asupra modului în care este realizată evaluarea sistemelor dinamice de autentificare a semnăturilor. Ne-am concentrat asupra unui aspect esențial pentru evaluarea performanțelor sistemelor biometrice de autentificare, anume optimizarea culegerii de date.

  În [92] am introdus o noțiune nouă și un dispozitiv fizic pentru evitarea accesului neautorizat în sistem. Dispozitivul fizic este reprezentat de un pix hardware [138], dezvoltat de compania SOFTWIN.

  Secțiunea 6.5 din teză descrie o soluție de sistem bazată pe verificare biometrică, cu ajutorul mouse-ului și al tastelor. Conceptul este prezentat ca o platoformă e-learning, iar simulările ideii propuse au fost realizate în cadrul proiectului de cercetare POSDRU 61434: Educație Modernă și Calitate pentru Viitor (Modern Education and Quality for Future), un proiect fondat de Uniunea Europeană. Începând din septembrie 2014, vor fi integrate soluții pentru verificarea prezenței studenților la cursuri și examene. Secțiunea include două contribuții personale, [94] și [98].

  În [94] am prezentat avantajele sistemului de verificare a utilizatorilor pe baze mouse-ului și a tastaturii. Metoda s-a dovedit a fi extrem de precisă și destul de eficientă pentru implementare și utilizare în viitor.

În [98] am prezentat viitorul mediu e-learning și riscurile de securitate ce necesită a fi eliminate pentru a garanta un mediu sigur și evitarea intruziunilor persoanelor rău intenționate.

Am atașat în cele ce urmează o listă a contribuțiilor personale publicate și a proiectelor de cercetare în cadrul cărora mi-am desfășurat activitatea de cercetare.

Nr.	Publicatie	Numar referinta
1.	Mihailescu Marius Iulian, Research on Biometric Synthetic Faces, Indian Journal of Research (PIJR), Vol. 2, Issues 9, September, 2013, pp. 38-40, ISSN: 2250-1991.	[96]
2.	Mihailescu Marius Iulian, Proposing a New Framework for Biometric Optical Recognition for Handwritten Digits Data Set, Journal of Knowledge Management, Economics and Information Technology, volume 3, issue 1, pp. ISSN:2069-5934, pp. 84-95 ,2013. www.scientificpapers.org.	[87]
3.	Mihailescu Marius Iulian, New Enrollment Scheme for Biometric Template using Hash Chaos-based Cryptography, Elsevier - Procedia Engineering, Volume 69, 2014, pages 1459-1468, ISSN: 1877-7058.	[92]
4.	Mihailescu Marius Iulian, Direct Problems and Inverse Problems in Biometrics Systems. Journal of Knowledge Management, Economics and Information Technology, vol. III, Issue no. 5, pp. 1-14 October 2013, ISSN: 2069-5934.	[95]
5.	Mihailescu Marius Iulian, Pau Valentin Corneliu, Proposing a Biometric Verification Method for Students Attendance using Mouse Movements, International Journal of Academic Research in Progressive Education and Development, Human Resource Management Academic Research Society, vol. 3, no. 11, november 2013, ISSN: 2222-6990.	[93]
6.	Mihailescu Marius Iulian, Marian Dorin Pirloaga, Optimisation strategies for data collections used in evaluating dynamic signature authentication systems. In proceedings of the 9th International Conference on Communications (COMM) - http://comm2012.ncit.pub.ro/, 21-23 June 2012 Bucharest, Romania, pp. 343-349, ISBN: 978-1-4673-2573-8, IEEE Catalog Number: CFP1241J-PRT.	[89]
7.	Mihailescu Marius Iulian, On Linear Discriminant Analysis for Biometric Handwritten Recognition Process Poster, Workshop Section. Advanced School Studies "Challenges of Cybernetics Security From paradigm to implementation", Project code: PN-II-SSA-2012-2-017, IDEI Programe, Romania, Bucharest-Busteni, 2012. http://cybersecurity.utm.ro/index.html.	[94]
8.	Pirloaga Marian, Mihailescu Marius Iulian, Comparative Study on Optoelectronic Tracking Models which can be used in Biometrics. In proceedings of the 9th International Conference on Communications (COMM) - http://comm2012.ncit.pub.ro/, 21-23 June 2012, Bucharest, Romania, pp. 107-111, ISBN: 978-1-4673-2573-8, IEEE Catalog Number: CFP1241J-PRT.	[117]
9.	Mihailescu Marius Iulian, Pirloaga Marian, A New Framework for Biometric Face Recognition Using Visual Cryptography. Proceedings of 23rd International DAAAM Symposium, Volume 23, No. 1, 2012, ISSN 2304-1382, ISBN 978-3-901509-91-9, pp.163-166.	[88]
10.	Pirloaga Marian, Mihailescu Marius Iulian, Contributions to the Modeling of a communication channel by RBF, Proceedings of 23rd International DAAAM Symposium, Volume 23, No. 1, 2012, ISSN 2304-1382, ISBN 978-3-901509-91-9, pp.381-384.	[116]
11.	Danut Turcu, Mihailescu Marius Iulian. Research on Vulnerabilities of Science and Information Technology Pylon of the Warfare Structure. International Conference of Strategies XXI "Military Science Universe", 14-15.04.2011, Bucharest, Romania. 6th Volume Informatics Systems, pp. 251-263, ISBN 978-973-663-886-2, 978-973-663-892-3.	[40]
12.	Mihailescu Marius Iulian, Research on Solutions for Preventing Algebraic Attacks Against Biometric and RFID Protocols. In Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, ICTAMI 2011, Alba Iulia, Romania, pp. 371-386, ISSN 1582-5329.	[90]

13.	Mihailescu Marius Iulian, Stefan Stelian Diaconescu, Mircea Sorin Rusu. Authentication Method Based on Holographic Signature Recognition System using Physical Modelling of a Pen. The 22^{nd} International DAAAM Symposium, 23-26 November 2011, Vienna, Austria. Annals of DAAAM for 2011 and Proceedings, ISBN 978-3-901509-73-5, ISSN 1726-9679, pp. 677-678.	[91]
14.	Mihailescu Marius Iulian, Gramada Argentina, Extending Knowledges and Developing Quality Media Rich Using SCORM Content Model Components and Content Packaging. The 7th International Scientific Conference eLSE eLearning and Software for Education, 28-29 April 2011, Bucharest, Romania. 2nd Volume Anywhere, anytime Education on Demand, pp. 319-326, ISSN 2066-026X.	[97]
15.	Pau Valentin Corneliu, Mihailescu Marius Iulian, Stanescu Octavian, Identification of Common Elements and Parameters for Creational Design Patterns in Order to Create a Framework Core. The 7th International Scientific Conference eLSE eLearning and Software for Education, 28-29 April 2011, Bucharest, Romania. 2nd Volume Anywhere, anytime Education on Demand, pp. 311-318, ISSN 2066-026X.	[105]
16.	Adrian Atanasiu, Marius Iulian Mihailescu, Biometric passports (ePassports), The 8th International Conference on Communications "COMM 2010", 2010, Bucharest, Romania. IEEE Catalog Number: CFP1041J-ART, pag. 443, ISBN: 978-1-4244-6363-3, IEEEXplore Print ISBN: 978-1-4244-6360-2, INSPEC Accession Number: 11417232, Digital Object Identifier: 10.1109-ICCOMM.2010.5509095.	[3]
17.	Pau Valentin Corneliu, Mihailescu Marius Iulian, Stanescu Octavian, Security Design Patterns. The 4th International Conference Education and Creativity for a Knowledge Society, 29-30 October 2010, Bucharest, Romania. ISSN 1841-7361, ISBN 978-606-8002-37-8.	[106]
18.	Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Antipatterns Implementing productive solutions to avoid developing problems for web and software applications, 1st International Workshop The Economy and the New Information Technologies, Suceava, Romania 2010. Journal of Applied Computer Science and Mathematics, No. 7, eISSN: 2066 3129, ISSN: 2066-4273.	[107]
19.	Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Best practices for using Lists as Design Web Patterns, 1st International Workshop The Economy and the New Information Technologies, Suceava, Romania, 2010. Journal of Applied Computer Science and Mathematics, No. 7, eISSN: 2066 3129, ISSN: 2066-4273	[108]
20.	Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Model View Presenter Design Pattern, 8th Edition of the International Conference on Advances in Electrotechnologies (ICAdET) 2010, Oradea, Romania, Journal of Computer Science and Control Systems, 3rd Volume, no. 1, pp. 173, P-ISSN: 1844-6043, E-ISSN: 2067-2101, CD-ISSN: 2067-2098.	[109]
21.	Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Model View Presenter Design Pattern, 8th Edition of the International Conference on Advances in Electrotechnologies (ICAdET) 2010, Oradea, Romania, Journal of Computer Science and Control Systems, 3rd Volume, no. 1, pp. 173, P-ISSN: 1844-6043, E-ISSN: 2067-2101, CD-ISSN: 2067-2098.	[109]
22.	Racuciu Ciprian Constantin Iulian, Mihailescu Marius Iulian, Garban Valentin, Praoveanu Iosif, Balan Constantin. Research on Estimation Length of Hidden Message. The 21st International DAAAM Symposium, 20-23 Octombrie 2010, Zadar, Croatia. Annals of DAAAM for 2010 and Proceedings, ISBN 978-3-901509-73-5, ISSN 1726-9679, pp. 967-969.	[119]

Tabelul 7.1 Listă de publicații personale

Viitoarele direcții de cercetare se bazează pe câteva obiective generale pe care intenționez să le duc la realizare în viitorul apropiat, după cum urmează:

- Să dezvolt o nouă tehnologie bazată pe soluții de sporire a gradului de intiminate pentru identitatea electronică ce are la bază autentificarea, utilizând semnături on-line, off-line și recunoaștere facială.
- Să aduc noi dovezi în ceea ce privește performanța și securitatea soluțiilor propuse anterior. Tehnologia propusă va fi utilizată în aplicațiile de comerț electronic ce implică identitatea, realizate în România, fapt care reprezintă un factor de progres pentru cetățenii utilizatori, cum ar fi: creșterea gradului de protecție a datelor cu caracter personal și sporirea încrederii utilizatorilor în managementul identității electronice prin utilizarea semnăturilor on-line/ off-line și a recunoașterii faciale.
- Integrarea criptografiei bazate pe haos în procesul de autentificare, utilizând scheme de înrolare pentru recunoașterea facială și semnăturile on-line/ off-line.
- Imputarea descrierii umane în biometrica semantică și generarea unor chei criptografice obținute din analiza semantică latentă. Ca o scurtă definiție, analiza semantică latentă reprezintă un model spațial vectorial concentrat pe descoperirea structurilor semantice latente bazate pe apariția trăsăturilor în cadrul documentelor.

• **2011 - 2013**	**POSDRU 61434: Învățământ modern și calitate pentru viitor** **Sistem informatic pentru învățământul la distanță.** ***Responsabilități personale*:** - Analiza, proiectarea si implementarea cerințelor pentru aplicația software (secretariat) și web (elearning). - Propunerea și implementare de algoritmi biometrici pentru verificarea facială. - Realizarea de scenarii (use cases) pentru student și secretariat. - Testarea funcționalităților aplicației de secretariat și a platformei web elearning. ***Tehnologii*:** C#, Java, JSP, PHP, Oracle 10g. **http://www.utm.ro/posdru_61434.php**
• **2010 - 2013**	**POS-CCE 208/20.07.2010: ATHOS (Automated Authentication Service using Biometric Signature. Serviciu automat de autentificare folosind semnătura olografică biometrică).** *Responsabilități personale:* - Implementarea unui sistem de management și distribuire al sarcinilor (task-urilor) (load balancer) folosind resursele arhitecturii (calculatoare clusterizate) cu scopul de optimiza folosirea resurselor și de a minimiza timpul de răspuns pentru operații și evitarea

	suprasolicitării resurselor. Elaborarea de documentație tehnică pentru implementarea load balancer-ului. *Tehnologii folosite la implementare:* C++, C#. - Proiectarea și testarea unei arhitecturi de tip SoA (Service-oriented Architecture) cu scopul de a permite utilizatorilor să combine diferite funcționalități pentru a forma aplicații de tip ad-hoc. - Analiza și implementarea de mecanisme criptografice (RSA) folosind C++. *Tehnologii*: C++, C#, AJAX, ASP, PHP, MFC. http://www.softwinresearch.ro/index.php/ro/proiecte/athos

Tabelul 7.2. Lista de proiecte în care am participat

În Tabelul 7.2 am prezentat două proiecte în cadrul cărora mi-am desfășurat activitatea de cercetare pe baza căreia am conceput prezenta teză de doctorat. În primul proiect (1) am examinat un set de aspecte de securitate ale unui sistem biometric de autentificare bazat pe semnătură holografică, un sistem implementat și testat în cadrul unei grile, într-un mediu arhitectural de cluster și cloud. În al doilea proiect (2) am exploatat câteva posibilități de integrare a diferitelor metode de autentificare (față, semnătură, mișcarea mouse-ului și apăsarea tastelor).

În Tabelul 7.3 sunt listate patru școli de vară la care am participat, îmbogățindu-mi astfel cunoștințele în varii domenii ale criptografiei. Mai mult, aceste școli mi-au pus la dispoziție posibilitatea de fi în pas cu ultimele cercetări în acest domeniu. În cadrul ECRYPT II, cea de-a treia școală, am aflat lucruri interesante și fascinante, elemente fundamentale ce privesc securitatea procesului de autentificare, acesta fiind și punctul de plecare al tezei mele doctorale.

• **29 Iulie – 02 August 2013**	**Crypt@B-IT, Summer School on Cryptography, Bonn, Germania - http://cosec.bit.uni-bonn.de/students/events/cryptabit2013/**
• **17 – 25 August 2012**	Școala de Studii Avansate "Provocări ale Securităţii Cibernetice – De la paradigmă la implementare", Cod proiect: PN-II-SSA-2012-2-017, Programul IDEI – România, București-Bușteni.
• **29 Mai – 3 Iunie 2011**	ECRYPT II, Design and Security of Cryptographic Algorithms and Devices, Albena - Bulgaria
• **2007 – 2008 (1 an)**	Bursă ERASMUS, Facultatea de Inginerie, Specializarea Calculatoare, Universitatea Southern, Institutul Maersk Mc-Kinney Moller (www.sdu.dk), Danemarca.

Tabelul 7.3. Lista școlilor și a stagiilor

În scopul pregătirii etapelor următoare ale acestei cercetări, am definit în continuare câteva obiective strategice:

- Aplicarea tehnicilor criptografice în cazul semnăturilor on-line/ off-line și a recunoașterii faciale, ca identitate non-invertibilă și pseudo-identitate pentru verificarea înregistrării;
- Crearea unei posibilități de a regenera șirurile de biți unice și independente, bazate pe aceleași șabloane on-line/ off-line și pe imaginea facială;
- Managementul schemelor reprezentate de pseudo-identitățile multiple și revocabile bazate pe unicitatea șirurilor de biți.
- Semnături biometrice on-line și off-line cu un grad de siguranță foarte ridicat, bazat pe verificări 1:1, prin utilizarea șirurilor de biți unice.

Bibliografie

[1] Abishek Nagar, Karthik Nandakumar, and Anil. K. Jain, Biometric Template Transformation: A Security Analysis,

http://www.cse.msu.edu/biometrics/Publications/SecureBiometrics/NagarTempTransSecAnalysis_SPIE10.pdf

[2] Adrian Atanasiu, Securitatea Informatiei - Protocoale de Securitate, vol. 2, ISBN: 978-973-1803-29-6/978-973-1803-18-0, 2009, Editura InfoData.

[3] Adrian Atanasiu, Marius Iulian Mihailescu, Biometric passports (ePassports), The 8th International Conference on Communications COMM 2010, 2010, Bucharest, Romania. IEEE Catalog Number: CFP1041J-ART, pag. 443, ISBN: 978-1-4244-6363-3, IEEEXplore Print ISBN: 978-1-4244-6360-2, INSPEC Accession Number: 11417232, Digital Object Identifier: 10.1109-ICCOMM.2010.5509095.

[4] Alex Poole, Linden J. Ball, Eye Tracking in Human-Computer Interaction and Usability Research: Current Status and Future Prospects, http://www.alexpoole.info/blog/wp-content/uploads/2010/02/PooleBall-EyeTracking.pdf

[5] Alwyn Goh, D.C.L. Ngo., Computation of cryptographic keys from face biometrics. In International Federation for Information Processing, volume 2828 of LNCS, 2003.

[6] Alwyn Goh, D.C.L. Ngo., Computation of cryptographic keys from face biometrics. In International Federation for Information Processing, volume 2828 of LNCS, 2003.

[7] Ana Cristina Dascalescu, Radu Boriga, Adrian Viorel Diaconu , Study of a New Chaotic Dynamical System and Its Usage in a Novel Pseudorandom Bit Generator, Mathematical Problems in Engineering, vol. 2013, article ID 769108, 10 pages, 2013.

[8] Ana Cristina Dascalescu, Radu Boriga, A Novel Fast Chaos-Based Method for Generating Random Permutations with High Shift Factor Suitable for Image Scrambling, Nonlinear Dynamics, vol. 74(1-2), pp. 307-318, 2013.

[9] Ana Cristina Dascalescu, Radu Boriga, Ciprian Racuciu, A New Pseudorandom Bit Generator using Compounded Chaotic Tent Maps, Proceedings of the 9th International Conference on Communications (COMM 2012), June 21-23, 2012, Bucharest, Romania, pp. 339-342, 2012.

[10] Anil K. Jain, P. Flynn, and A. Ross, Handbook of Biometrics, Springer, 2007.

[11] Anil K. Jain, Ross A, and Prabhakar S., An introduction to biometric recognition, IEEE Transactions on Circuit and Systems for Video Technology, 14(1):4?20, 2004

[12] Anil K. Jain, Pankanti S, and Bolle R, Eds., Biometrics: Personal Identification in Networked Society, Kluwer, Dordrecht, 1999.

[13] Anil K. Jain and Uludag U. Hiding biometric data. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(11):1494?1498, 2003.

[14] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Biometric Template Security, EURASIP Journal on Advances in Signal Processing, volume 2008, Article ID 579416, DOI: 10.1155/2008/579416

[15] Anil K. Jain, A. Ross, and S. Pankanti, Biometrics: a tool for information security,IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125143, 2006

[16] Arie van Deursen and Joost Visser, Source Model Analysis using the JJTraveler Visitor Combinator Framework. Software Practice and Experience, 34(14):1345-1379, 2004.

[17] A. Senthil Arumugam, N. Krishnan, Biometric Authentication System using Non-Linear Chaos, International Journal of Engineering and Technology, vol. 2(4),2010, pp. 267-275, ISSN: 0975-4024.

[18] A. Eriksson and P. Wretling, How exible is the human voice? A case study of mimicry, in Proceedings of the European Conference on Speech Technology (Eurospeech 97), pp. 10431046, Rhodes, Greece, September 1997.

[19] A. Juels, D. Molnar, and D. Wagner, Security and privacy issues in E-passports, in Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, (SecureComm 05), pp. 7488, Athens, Greece, September 2005.

[20] A. Adler, Vulnerabilities in biometric encryption systems, in Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA 05), vol. 3546 of Lecture Notes in Computer Science, pp. 11001109, Hilton Rye Town, NY, USA, July 2005

[21] A. Ross, J. Shah, and A. K. Jain, From template to image: reconstructing fingerprints from minutiae points, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 544560, 2007.

[22] Basel Alomair, L. Lazos, and R. Poovendran, Passive attacks on a class of authentication protocols for RFID. In ICISC, pages 102115, 2007.

[23] Berrin Yanikoglu, Alisher Kholmatov, Online Signature Verification using Fourier Descriptors, EURASIP Journal on Advances in Signal Processing, vol. 2009, article 260516, DOI: 10.1155/2009/260516.

[24] Bi-cubic Interpolation, http://en.wikipedia.org/wiki/Bicubic_interpolation

[25] Biometric Passports Law Upheld By The Romanian Authorities, http://www.edri.org/edri-gram/number7.5/biometric-passports-romania

[26] Bolle R, Connell J, Pankanti S, Ratha N, and Senior A. Guide to Biometrics. Springer, Heidelberg, 2004

[27] Bringer J., Chabanne H., Icart T., Cryptanalysis of EC-RAC, a RFID identification protocol. In: CANS. 149161, 2008.

[28] Chen S., Mulgrew B. and Grant P. M., A clustering technique for digital communications channel equalization using radial basis function networks. In IEEE Transactions on Neural Networks, 4, (4) (1993), 570-579.

[29] Chen Z., Huang Y.: Chaotic one way hash function. Communications Technology (7), 9698, 2001.

[30] Chien H.Y., Huang C.W., A lightweight RFID protocol using substring. In: Embedded and Ubiquitous Computing (EUC). (2007) 422431.

[31] Chin-Chen Chang, J. C. Chuang, and P.Y. Lin, Sharing A Secret Two-Tone Image In Two Gray-Level Images, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS05), 2005.

[32] Chirillo J and Blaul S. Implementing Biometric Security, John Wiley and Sons, New York, 2003.

[33] Christian Rathgeb, Andreas Uhl, A survey on biometric cryptosystems and cancelable, http://jis.eurasipjournals.com/content/2011/1/3

[34] Christos K. Dimitriadis, Biometric risk and controls, Information Systems control Journal, Vol. 4, 2004.

[35] Clark J and Yuille A. Data Fusion for Sensory Information Processing Systems. Kluwer, Dordrecht, 1990.

[36] Colin Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, Biometric encryption using image processing, in Proceedings of SPIE, 3314, pp. 178188, 1998.

[37] Colin Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, Biometric encryption, ICSA Guide to Cryptography, 1999.

[38] Constantin Vertan, Mihai Ciuc, Marta Zam_r, Prelucrarea si analiza imaginilor, Printech Publishing House Bucharest, 1999, ISBN 973-9475-71.

[39] Dascalescu Ana Cristina, Boriga Radu, Tehnici de Criptare Clasice si Tehnici de Criptare bazate pe Sisteme Dinamice Haotice, Silvana Publisher House, ISBN: 978-606-8249-34-6, 2013.

[40] Danut Turcu, Mihailescu Marius Iulian. Research on Vulnerabilities of Science and Information Technology Pylon of the Warfare Structure. International Conference of Strategies XXI „Military Science Universe, 14-15.04.2011, Bucharest, Romania. 6th Volume Informatics Systems, pp. 251-263, ISBN 978-973-663-886-2, 978-973-663-892-3.

[41] Dilip Gopichand Khairnar, Shabbir N. Merchant, U.B. Desai, Radar Signal Detection in Non-Gaussian Noise using RBF Neural Network, International Journal of Computers, Vol. 3, No. 1, pp. 32-39, January 2008.

[42] Deursen T.V., Radomirovic S., Attacks on RFID protocols (version 1.0). Cryptology ePrint Archive, Report 2008/310 (July 2008) http://eprint.iacr.org/2008/

[43] Deursen T.V., Radomirovic S., Security of an RFID Protocol for Supply Chains, http://satoss.uni.lu/papers/DR08a.pdf.

[44] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003.

[45] Dwijen Rudrapal, Smita Das, S. Debbarma, N. Kar, N. Debbarma, Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H. People, International Journal of Computer Applications, vol. 39, No. 12, February 2012, ISSN: 0975-8887.

[46] Edgar Osuna, R. Freund, and F. Girosi. Training support vector machines: An application to face detection. Proceedings of the IEEE Conf. Computer Vision and Pattern Recognition, pages 130136, June 1997.

[47] Elaine Newton, Latanya Sweeney, and Bradley Malin, Preserving privacy by de-identifying face images, IEEE Transactions on Knowledge and Data Engineering, pp. 232-243, 2005.

[48] Emanuele Maiorana, P. Campisi and A. Neri, Biometric Signature Authentication Using Radon Transform-Based Watermarking Techniques. In Biometric Symposium, 2007.

[49] Fred Bookstein, Principal warps: Thin-plate splines and the decomposition of deformations, IEEE Transactions on Pattern Analysis and Machine Intelligence 11(6), pp. 67585, 1989.

[50] George I. Davida, Y. Frankel, and B. J. Matt, On enabling secure applications through on-line biometric identification, in IEEE Symposium on Security and Privacy, pp. 148157, 1998.

[51] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and D. Stinson, Extended capabilities for visual cryptography, Theoretical Computer Science 250(1-2), pp. 143161, 2001.

[52] Gildas Avoine, Adversary model for radio frequency identification. Technical Report LASEC-REPORT-2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, September 2005.

[53] H. Gamboa and A. Fred. A behavioural biometric system based on human-computer interaction. In Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, volume 5404, pages 381392, Aug. 2004.

[54] Gonzalez RC, Woods RE, and Eddins SL. Digital Image Processing Using MATLAB. Pearson, Prentice Hall, 2004.

[55] Huang Guang-Bin., Chen Y. Q. and Babri H. A., Classi_cation ability of single hidden layer feed forward neural networks, IEEE Transactions on Neural Networks, 11, (3) (2000), 799-801.

[56] Huang Guang-Bin, Saratchandran P. and Sundararajan N., An efficient sequential learning algorithm for Growing and Pruning RBF (GAP-RBF) networks, IEEE Transactions on Systems, Man and Cybernetics-Part B: Cybernetics, 34, (6), (2004), 2284-2292.

[57] Henon map, http://en.wikipedia.org/wiki/H%C3%A9non_map

[58] Hill R. Retina identi_cation. In Jain AK, Bolle RM, and Pankanti S, Eds., Biometrics: Personal Identification in Networked Society, pp. 123?142, Kluwer, Dordrecht, 1999.

[59] Inhyok Cha, S.A. Kassam, Channel Equalization using Adaptive Complex Radial Basis Function Networks, IEEE J. Selected Areas in Communications, 13, 122-131, January 1995, Special Issue on Intelligent Signal Processing.

[60] Il Jung Kim, E. Y. Choi, and D. H. Lee, Secure mobile RFID system against privacy and security problems. In SecPerU, 2007.

[61] JeaCheol Ha, Sang-Jae Moon, Juan Manuel Gonzales Nieto, and Colin Boyd, Low-cost and strong-security RFID authentication protocol. In EUC Workshops, pages 795807, 2007.

[62] Jean-Sebastien Coron, Yevgeniy Dodis, Cecile Malinaud, and Prashant Puniya, Merkle-Damgard Revisisted: How to Construct a Hash Function. http://www.cs.nyu.edu/~puniya/papers/merkle.pdf

[63] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and KKwangjo Kim, Mutual authentication protocol for low-cost RFID. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[64] John Daugman, Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons, Proc. IEEE, vol. 94, no. 11, pp. 19271935, Nov. 2006.

[65] Jose L. Alba Castro, Elisardo Gonzalez Agulla, E. Argones Rua,and L. Anido Rifon. Realistic measurement of student attendance in LMS using biometrics. In To appear on the Proceedings of the International Symposium on Engineering Education Educational Technologies: EEET 2009, 2009.

[66] Kah-Kay Sung, Learning and Example Selection for Object and Pattern Detection. PhD thesis, Massachusetts Institute of Technology, 1996.

[67] Karthik Nandakumar, Anil K. Jain and Sharath C. Pankanti. Fingerprint-Based Fuzzy Vault: Implementation and Performance. IEEE Transactions on Information Forensics and Security, 2(4):744-757, 2007.

[68] Kechriotis G., Zervas E. and Manolakos E. S., Using recurrent neural networks for adaptive communication channel equalization.IEEE Transactions on Neural Networks, 5, (2) (1994), 267-278.

[69] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, XM2VTSDB: The extended M2VTS database. In Second International Conference on Audio and Video-based Biometric Person Authentication, 964, pp. 965966, 1999.

[70] K. Lam and D. Gollmann, Freshness assurance of authentication protocols, in Proceedings of the European Symposium on Research in Computer Security (ESORICS 92), pp. 261272, Toulouse, France, 1992.

[71] Kumar P. C., Saratchandran P. and Sundararajan N., Minimal radial basis function neural networks for nonlinear channel equalisation. IEEE Proceedings, Vision, Image and Signal Processing, 147 (5) (2000), 428-435.

[72] Kyosuke Osaka, Tsuyoshi Takagi, Kenichi Yamazaki, and Osamu Takahashi, An e_cient and secure RFID security method with ownership transfer. In CIS, pages 778787, 2006.

[73] Kwok, H., Tang, W.: A Chaos Based Cryptographic Hash function for Message Authentication. International Journal of Bifurcation and Chaos 15(12), 40434050, 2005.

[74] Lakhmi C. Jain, Halici U, Hayashi I, Lee SB, and Tsutsui S, Eds., In Fingerprint and Face Recognition, CRC Press, Boca Raton, FL, 1999.

[75] Liguo Fang and Bin Yu, Research On Pixel Expansion of (2,n) Visual Threshold Scheme, 1st International Symposium on Pervasive Computing and Applications, pp. 856-860, IEEE.

[76] Liu J., Xie J., Wang P., One way hash function construction based on chaotic mappings. Journal of Tsinghua University (Sci. and Tech.) 40(7), 55-58, 2000.

[77] Luis Torres, Is there any hope for face recognition?. In Proc. of the 5th International Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS, Lisboa, Portugal, 21-23 April 2004.

[78] Lee Y.K., Batina Lejla, Verbauwhede Ingrid: EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In: Proceedings of the 2008 IEEE International Conference on RFID. (2008) 97104

[79] Lin Hong, Anil K. Jain, and Sharath Pankanti, Can Multibiometrics Improve Performance?, Proc. AutoID '99, pp.59-64, October 2005.

[80] List of chaotic maps, http://en.wikipedia.org/wiki/List_of_chaotic_maps

[81] Liu J., Xie J., Wang P.: One way hash function construction based on chaotic mappings. Journal of Tsinghua University (Sci. and Tech.) 40(7), 5558, 2000.

[82] LiWen-xin, David Zhang, Xu Zhuo-qun, Palmprint Recognition Based on Fourier Transform, Journal of Software, vol. 13, no. 5, pp. 879-886, ISSN: 1000-9825, 2002.

[83] Ljupco Kocarev, Chaos-based Cryptography: A Brief Overview, IEEE, ISSN: 1531-636X, 2001. http://www.elettrotecnica.unina.it/files/demagistris/didattica/TdC/Chaos_Cryptography.pdf

[84] Logisitc map, http://en.wikipedia.org/wiki/Logistic_map

[85] Low-pass Filter, http://en.wikipedia.org/wiki/Low-pass_filter

[86] Manu Kumar, Reducing the Cost of Eye Tracking Systems, http://hci.stanford.edu/cstr/reports/2006-08.pdf

[87] Mihailescu Marius Iulian, Proposing a New Framework for Biometric Optical Recognition for Handwritten Digits Data Set, Journal of Knowledge Management, Economics and Information Technology, volume 3, issue 1, ISSN:2069-5934, www.scientificpapers.org, 2013.

[88] Mihailescu Marius Iulian, Pirloaga Marian, A New Framework for Biometric Face Recognition Using Visual Cryptography. Proceedings of 23rd International DAAAM Symposium, Volume 23, No. 1, ISSN 2304-1382, ISBN 978-3-901509-91-9, pp.163-166.

[89] Mihailescu Marius Iulian, Marian Dorin Pirloaga, Optimisation strategies for data collections used in evaluating dynamic signature authentication systems. In proceedings of the 9th International Conference on Communications (COMM) - http://comm2012.ncit.pub.ro/,21-23 Iunie 2012 Bucureti, Romania, pp. 343-349, ISBN: 978-1-4673-2573-8, IEEE Catalog Number: CFP1241J-PRT.

[90] Mihailescu Marius Iulian, Research on Solutions for Preventing Algebraic Attacks Against Biometric and RFID Protocols. In proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, ICTAMI 2011, Alba Iulia, Romania, pp. 371-386, ISSN 1582-5329.

[91] Mihailescu Marius Iulian, Stefan Stelian Diaconescu, Mircea Sorin Rusu. Authentication Method Based on Holographic Signature Recognition System using Physical Modelling of a Pen. The 22nd International DAAAM Symposium, 23-26 November 2011, Vienna, Austria. Annals of DAAAM for 2011 and Proceedings, ISBN 978-3-901509-73-5, ISSN 1726-9679, pp. 677-678.

[92] Mihailescu Marius Iulian, New Enrollment Scheme for Biometric Template using Hash Chaos-based Cryptography, Elsevier - Procedia Engineering, Volume 69, 2014, pages 1459-1468, ISSN: 1877-7058.

[93] Mihailescu Marius Iulian, Pau Valentin Corneliu, Proposing a Biometric Verification Method for Students Attendance using Mouse Movements, International Journal of Academic Research in Progressive Education and Development, Human Resource Management Academic Research Society.

[94] Mihailescu Marius Iulian, On Linear Discriminant Analysis for Biometric Handwritten Recognition Process Poster, Workshop Section. Advanced School Studies "Challenges of Cybernetics Security From paradigm to implementation", Project code: PN-II-SSA-2012-2-017, IDEI Programe, Romania, Bucharest-Busteni, 2012. http://cybersecurity.utm.ro/index.html.

[95] Mihailescu Marius Iulian, Direct Problems and Inverse Problems in Biometrics Systems. Journal of Knowledge Management, Economics and Information Technology, vol. III, Issue no. 5, October, ISSN: 2069-5934.

[96] Mihailescu Marius Iulian, Research on Biometric Synthetic Faces, Indian Journal of Research (PIJR), Vol. 2, Issues 9, September, 2013, pp. 38-40, ISSN: 2250-1991, Impact Factor 0.3208, ISI Journal

[97] Mihailescu Marius Iulian, Gramada Argentina, Extending Knowledges and Developing Quality Media Rich Using SCORM Content Model Components and Content Packaging. The 7th International Scientific Conference eLSE eLearning and Software for Education, 28-29 April 2011, Bucharest, Romania. 2nd Volume Anywhere, anytime Education on Demand, pp. 319-326, ISSN 2066-026X.

[98] Mikell B. Stegmann, Active appearance models: Theory, extensions and cases, Masters Thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU, August 2000.

[99] Mikell B. Stegmann, B. K. Ersboll, and R. Larsen, FAME a exible appearance modelling environment, IEEE Trans. on Medical Imaging 22(10), pp. 13191331, 2003.

[100] Moni Naor and Adi Shamir, Visual Cryptography, Advances in Cryptology EUROCRYPT, pp 1-12, 1994.

[101] Mizuho Nakajima and Yasushi Yamaguchi, Enhancing registration tolerance of extended visual cryptography for natural images, Journal of Electronic Imaging 13, pp. 654662, 2004.

[102] Mizuho Nakajima and Yasushi Yamaguchi, Extended visual cryptography for natural images, Journal of WSCG 10(2), pp. 303310, 2002.

[103] Nashed MZ and Scherzer O, Eds., Inverse Problems, Image Analysis, and Medical Imaging. American Mathematical Society, Providence, Rhode Island, 2002.

[104] N. K. Ratha, J. H. Connell, and R. M. Bolle, An analysis of minutiae matching strength. In Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA 01), pp. 223228, Halmstad, Sweden, June 2001.

[105] Pau Valentin Corneliu, Mihailescu Marius Iulian, Stanescu Octavian, Identi_cation of Common Elements and Parameters for Creational Design Patterns in Order to Create a Framework Core. The 7th International Scientific Conference eLSE eLearning and Software for Education, 28-29 April 2011, Bucharest, Romania. 2nd Volume Anywhere, anytime Education on Demand, pp. 311-318, ISSN 2066-026X.

[106] Pau Valentin Corneliu, Mihailescu Marius Iulian, Stanescu Octavian, Security Design Patterns. The 4th International Conference Education and Creativity for a Knowledge Society, 29-30 October 2010, Bucharest, Romania. ISSN 1841-7361, ISBN 978-606-8002-37-8.

[107] Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Antipatterns Implementing productive solutions to avoid developing problems for web and software applications, 1st International Workshop The Economy and the New Information Technologies, Suceava, Romania 2010. Journal of Applied Computer Science and Mathematics, No. 7, eISSN: 2066 3129, ISSN: 2066-4273.

[108] Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Best practices for using Lists as Design Web Patterns, 1st International Workshop The Economy and the New Information Technologies, Suceava, Romania, 2010. Journal of Applied Computer Science and Mathematics (B+), No. 7, eISSN: 2066 3129, ISSN: 2066-4273.

[109] Pau Valentin Corneliu, Stanescu Octavian, Mihailescu Marius Iulian, Model View Presenter Design Pattern, 8th Edition of the International Conference on Advances in Electrotechnologies (ICAdET) 2010, Oradea, Romania, Journal of Computer Science and Control Systems, 3rd Volume, no. 1, pp. 173, P-ISSN: 1844-6043, E-ISSN: 2067-2101, CD-ISSN: 2067-2098.

[110] Parisi R., Claudio E. D. D., Orlandi G. and Rao B. D.: Fast adaptive digital equalization by recurrent neural networks, IEEE Transactions on Signal Processing, 45, (11) (1997), 2731-2739.

[111] Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J., Ribagorda, A.: Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. (2007).

[112] Praveen Gauravaram, William Millan, Ed Dawson, and Kapali Viswanathan, Constructing Secure Hash Functions by Enhancing Merkle-Damgard Construction, ACISP, LNCS 4058, pp. 407-42, Springer-Verlag, Berlin Heidelberg, 2006.

[113] P. P. Gandhi and V. Ramamurti, Neural networks for signal detection in non-Gaussian noise, IEEE Transactions on Signal Processing, Vol.45, No.11 (1997).

[114] P. Syverson, A taxonomy of replay attacks, in Proceedings of the Computer Security Foundations Workshop (CSFW 97), pp. 187191, Franconia, NH, USA, June 1994.

[115] P. Indyk and Rajeev Motwani, Approximate nearest neighbors: Towards removing the curse of dimensionality, in Proc. 30th Annu. CMSymp. Theory of Computing, 1998, pp. 604613.

[116] Pirloaga Marian, Mihailescu Marius Iulian, Contributions to the Modeling of a communication channel by RBF, Proceedings of 23rd International DAAAM Symposium, Volume 23, No. 1, ISSN 2304-1382, ISBN 978-3-901509-91-9, pp.381-384, 201.

[117] Pirloaga Marian, Mihailescu Marius Iulian, Comparative Study on Optoelectronic Tracking Models which can be used in Biometrics. In proceedings of the 9th International Conference on Communications (COMM) - http://comm2012.ncit.pub.ro/, 21-23 Iunie 2012, Bucureti, Romnia, pp. 107-111, ISBN: 978-1-4673-2573-8, IEEE Catalog

Number: CFP1241J-PRT.

[118] Polonnikov R and Korotkov K, Eds., Biometric Informatics and Eniology, OLGA Publishing House, St. Petersburg, 1995.

[119] Racuciu Ciprian Constantin Iulian, Mihailescu Marius Iulian, Garban Valentin, Praoveanu Iosif, Balan Constantin. Research on Estimation Length of Hidden Message. The 21st International DAAAM Symposium, 20-23 Octombrie

2010, Zadar, Croatia. Annals of DAAAM for 2010 and Proceedings, ISBN 978-3-901509-73-5, ISSN 1726-9679, pp. 967-969

[120] Ratha Nalini K., J.H. Connell, and R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, vol. 40, no. 3, 2001.

[121] Ralph Gross, Latanya Sweeney, F. De La Torre, and S. Baker, Model-based face deidentification, IEEE Workshop on Privacy Research in Vision, 2006.

[122] Robert W. Floyd and Louis Steinberg, An adaptive algorithm for spatial greyscale, SPIE Milestone Series 154, pp. 281283, 1999.

[123] Root of Unity, http://en.wikipedia.org/wiki/Root_of_unity.

[124] Ruud M. Bolle, Jonathan H. Connell, S. Pankati, Nalini K. Ratha, A.W. Senior, The relation between the ROC curve and the CMC 4th IEEE Workshop on Automatic Identification Advanced Technologies, pp. 15 20, Bu_alo, New York, 17 18 Oct 2005.

[125] R. M. Bolle, J. H. Connell, and N. K. Ratha, Biometric perils and patches, Pattern Recognition, vol. 35, no. 12, pp. 27272738, 2002.

[126] R. Seacord, Secure Coding in C and C++, Addison-Wesley, Reading, Mass, USA, 2005.

[127] Salil Prabhakar, S. Pankanti, and A. Jain, Biometric recognition: Security and privacy concerns, IEEE Security and Privacy 1, pp. 3342, March-April 2003.

[128] S. Chiasson, P. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In USENIX Security Symposium, 2006.

[129] S. Sanderson and J. Erbetta, Authentication for secure environments based on iris scanning technology, in IEEE Colloquium on Visual Biometrics, vol. 8, pp.1-7, 2005.

[130] S. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, Time-series Detection of Perspiration as a Liveness Test in Fingerpint Devices. IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, vol. 35, no. 3, pp. 335-343, 2005.

[131] Sheng Chen, G. J. Gibson, C. F. N. Cowan , P. M. Grant, Adaptive equalization of finite non-linear channels using multilayer perceptions, Signal Processing, v.20 n.2, p.107-119, Jun. 1990.

[132] Sheng Chen, G. J. Gibson, C. F. N. Cowan , P. M. Grant, Reconstruction of binary signals using an adaptive radial-basis-function equalizer, Signal Processing, v.22 n.1, p.77-93, Jan. 1991.

[133] Stergios Papadimitriou, S. Mavroudi, L. Vladutu and A. Bezerianos, Generalized Radial Basis Function Networks Trained with Instance Based Learning for Data Mining of Symbolic Data. Applied Intelligence, 16, pp. 223-234, 2002

[134] Seong G. Kong, Jinguo Heo, Besma R. Abidi, Joonki Paik, and Mongi A. Abidi, Recent Advances in Visual and Infrared Face Recognition - A Review, Computer Vision and Image Understanding, Vol. 97, No. 1, pp.103-135, January 2005;

[135] Steven Shevell, The science of color, Elsevier Science Ltd., 2003.

[136] Sugimoto Y, Yoshitomi Y, and Tomita S. A method for detecting transitions of emotional states using a thermal facial image based on a synthesis of facial expressions. Robotics and Autonomous Systems,31:147?160, 2000.

[137] System and Methods of Acquisition and Authentification of the Handwritten Signature. Pattent Number WO 2006/085783, http://www.wipo.int/patentscope/search/en/WO2006085783.

[138] Tim Cootes, G. Edwards, C. Taylor, et al., Active appearance models, IEEE Transactions on Pattern Analysis and Machine Intelligence 23(6), pp. 681685, 2001.

[139] Timo Bartkewitz, Building Hash Functions from Block Ciphers, Their Security and Implementation Properties. http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bartkewitz.pdf.

[140] T. J. Stonham, Practical face recognition and verification with wizard. In H. D. Ellis, editor, Aspects of face processing. Kluwer Academic Publishers, 1986.

[141] Tae-Hong Min and Rae-Hong Park, Eyelid and eyelash detection method in the normalized iris image using the parabolic hough model otsus thresholding method. Pattern Recognition Letters, 30(12):1138-1143, 2009.

[142] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, Impact of artificial gummy fingers on fingerprint systems, in Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677 of Proceedings of SPIE, pp. 275289, San Jose, California, USA, January 2002.

[143] T. Matsumoto, M. Hirabayashi, and K. Sato, A vulnerability evaluation of iris matching (part 3), in Proceedings of the Symposium on Cryptography and Information Security (SCIS 04), pp. 701706, Iwate, Japan, January 2004.

[144] Uludag U, Pankanti S, Prabhakar S, Jain AK, Biometric Cryptosystems: Issues and Challenges. Proc. IEEE, 92:948-960, 2004

[145] Vizitiu Iulian-Constantin, D.Munteanu, A genetic procedure for RBF neural network center selection, Proc. Of the 9th WSEAS International Conference NN08, 2008, pp. 37-40

[146] W. R. Harrison, Suspect Documents, Their Scientific Examination, Nelson-Hall, Chicago, Ill, USA, 1981.

[147] Xiao-Qing Tan, Two Kinds of Ideal Contrast Visual Cryptography Schemes, International Conference on Signal Processing Systems, pp. 450-453, 2009.

[148] Xiaobo Zhou and Xiaodong Wang, Channel estimation for OFDM systems using adaptive radial basis function networks, IEEE Transactions on Vehicular Technology, vol. 52, no. 1, pp. 4899, Jan. 2003. DTV receiver performance test report - test report of multipath testing performed at ATTC, download available at http://www.attc.org/.

[149] Yagiz Sutcu, Shantanu Rane, Jonathan Yedidia, Stark Draper, Anthony Vetro, Feature Transformation of Biometric Templates for Secure Biometric Systems Based on Error Correcting Codes, http://www.merl.com/reports/docs/TR2008-029.pdf.

[150] Yi X., Hash function based on the chaotic tent map. Transactions on Circuits and Systems 52(6), 354357, 2005.

[151] Y. Li and X. Ding. Protecting RFID communications in supply chains. In ASIACCS, pages 234241, 2007

[152] Zhang D. Automated Biometrics: Technologies and Systems. Kluwer, Dordrecht, 2000.

[153] Zoi-Heleni Michalopoulou, Loren W. Nolta and Dimitri Alexandrou, Performance evaluation of multilayer perceptrons in signal detection and classification, IEEE Transactions on Neural Networks, Vol.6, No.2 (1995).