Iurie BULAI,
doctor în drept, conferenţiar universitar interimar
al Catedrei „Procedură penală şi criminalistică" a Academiei „Ştefan cel Mare" a MAI
Rodica BULAI,
magistru în tehnologii informaţionale, lector universitar
al Catedrei „Activitate specială de investigaţii şi securitate informaţională"
a Academiei „Ştefan cel Mare" a MAI

AVANTAJELE ŞI DEZAVANTAJELE UTILIZĂRII SISTEMELOR BIOMETRICE ÎN ASIGURAREA SECURITĂŢII FRONTIEREI ŞI A STATULUI

Rezumat

Prezentul articolul este axat pe analiza particularităţilor de implementare a tehnologiilor biometrice în societatea modernă. Autorii identifică problematica, precum şi oprtunităţile utilizării tehnologiilor biometrice atât la momentul actual, cât şi în viitorul apropiat

Cuvinte-cheie: *tehnologii biometrice, caracteristici statistice ale metodei, baze de date, iris, retină, amprente digitale, identificare facială -2D, identificare facială -3D, structura venelor mâinii, geometria mâinii.*

Summary

The present article focuses on the analysis of the particularities of implementation of biometric technologies in the modern society. The authors identify issues such as the use of biometric technologies both at present and in the near future

Keywords: *biometric techniques, statistical characteristics of the method, databases, iris, retina, fingerprints, face identification -2D, facial identification -3D, hand vein structure, hand geometry.*

Introducere. Siguranţa unui stat începe prin asigurarea siguranţei atât în interior, cât şi la frontieră prin identificarea, preîntâmpinarea circuitului, accesului unor elemente criminale cu caracter local, regional şi internaţional. Siguranţa frontierei poate fi asigurată prin diferite modalităţi, una dintre acestea fiind tehnologiile biometrice.

Sistemele tehnice de identificare denumite şi „biometrie" există la nivel regiune-stat (în interiorul statului R. Moldova), regiune-state (reuniune de state - Uniunea Europeană), internaţional (sistemul biometric de identificare). Sistemele date sunt utilizate de structurile de stat, precum şi de cele private. Scopul constă în siguranţă, sarcina în identificarea tehnică a persoanelor. Identificarea tehnică în sistemele biometrice este realizată prin mai multe elemente anatomice umane.

Totodată, în acest context ţinem să menţionăm că fiecare sistem posedă atât avantaje, cât şi lacune/dezavantaje – precum şi puncte slabe/vulnerabilităţi. Prin factorii vulnerabili la utilizarea sistemelor biometrice putem nominaliza: furtul de date, scurgerea de date, falsul de date .

Prioritatea utilizării unor sau altor sisteme va reieși din valorificarea avantajelor, și mai ales prin identificarea lacunelor/dezavantajelor și aplicarea soluțiilor de înlăturare sau minimalizare a acestora [2].

Fiecare persoană are amprente digitale, voce, caracteristici faciale. Acești identificatori sunt întotdeauna cu noi, nu pot fi pierduți. Tehnologia modernă facilitează citirea și analizarea acestora. Magiei biometrice au cedat nu numai utilizatorii obișnuiți, ci și unele organizații/instituții prestigioase. Băncile britanice au introdus datele biometrice de amprentă pentru a intra în conturile clienților. Deblocarea smartphone-urilor s-a petrecut mult timp cu ajutorul aceloraşi amprente. Master Card lucrează la implementarea metodei de auto-autentificare folosind Selfie.

Autentificarea biometrică este cu siguranță convenabilă! Dar întrebare cît este de sigură? Să începem cu elementele de bază. În 95% din cazuri, biometria este în mod inerent statistică matematică. Statistica matematică este o știință exactă, ai cărei algoritmi sunt folosiți pretutindeni: în sistemele radare și bayesiene.

Ca două caracteristici de bază ale oricărui sistem biometric, pot fi acceptate erori de primul și al doilea tip. În teoria radarului (radiolacaţiunii), acestea sunt denumite de obicei „alarmă falsă" sau „omisiunea țintei", iar în biometrie cele mai cunoscute concepte sunt FAR (False Acceptance Rate) și FRR (False Rejection Rate).

Primul număr caracterizează probabilitatea unei coincidențe false a caracteristicilor biometrice a două persoane. A doua este probabilitatea de a refuza accesul unei persoane care are acces. Cu cât sistemul este mai bun, cu atât este mai mică valoarea FRR pentru aceleași valori FAR. Uneori este utilizată EER caracteristică comparativă, care determină punctul în care se intersectează programele FRR și FAR. Dar este departe de a fi mereu reprezentativ. Este posibil să se ia în considerare următoarele: dacă producătorii în date bazelor de date biometrice deschise nu oferă caracteristicile sistemului FAR și FRR, atunci acest sistem este cel mai probabil incompetitiv sau mult mai slab decât concurenții. Au fost dezvoltate câteva caracteristici empirice care permit să evaluăm calitatea sistemului. „Rezistența la contrafacere" este o caracteristică empirică, generalizând cât de ușor este să induci în eroare identificatorul biometric. „Stabilitatea faţă de mediul înconjurător" este o caracteristică empirică de evaluare a stabilității sistemului în diferite condiții externe, cum ar fi schimbarea nivelului de iluminare sau a temperaturii încăperilor. „Simplitatea utilizării" arată cât de dificil este de a folosi un scaner biometric dacă este posibil să se identifice în timpul mișcării. O caracteristică importantă este „viteza de lucru" și „costul sistemului". Nu trebuie să uităm că caracteristicile biometrice ale unei persoane se pot schimba în timp, aceasta fiind un dezavantaj semnificativ. Abundența metodelor biometrice este uimitoare. Principalele metode care utilizează caracteristicile biometrice statice ale persoanei sunt identificarea desenul papilar la degete, irisul, geometria feței, retinei, structura venelor pe mână, geometria mâinii. Există, de asemenea, o serie de metode în care se utilizează caracteristicile dinamice: identificarea prin voce, dinamica scrierii de mână, ritmul inimii, mersul.

În articol, vom lua în considerare doar acele caracteristici care sunt aplicabile în sistemele de control al accesului (ACS) sau în sarcinile aferente. Datorită superiorității sale, acestea fiind în primul rând caracteristicile statice. Din caracteristicile dinamice, recunoașterea vocală are o semnificație statistică (comparabilă cu cele mai proaste date statistice ale algoritmilor static FAR ~ 0,1%, FRR ~ 6%), dar acestea doar în condiții ideale. Pentru a conștientiza probabilitățile FAR și FRR, se poate estima cât de des vor apărea coincidențele false, dacă de instalat un sistem de identificare la punctul de control și trecere cu un număr de personal N. Probabilitatea unei coincidențe false a amprentei obținute de scaner pentru o bază de date cu amprente digitale N este FAR N. Și în fiecare zi prin punctul de control vor trece N persoane. Apoi, probabilitatea de eroare pentru o zi lucrătoare este FAR · (N · N). Desigur, în funcție de scopurile sistemului de identificare, probabilitatea de eroare pe unitate de timp poate varia foarte mult, dar dacă se ia o singură eroare într-o zi lucrătoare, atunci:

$$FAR \times N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}} \qquad (1)$$

Apoi, obținem acea funcționare stabilă a sistemului de identificare la FAR = 0.1% = 0.001 este posibil cu numărul de personal N≈30.

Scanere biometrice. Până în prezent, termenii „algoritm biometric" și „scaner biometric" nu sunt neapărat *interdependenți*. O companie poate produce aceste elemente singură sau în comun. Cea mai mare diferențiere a producătorilor de scanere și a producătorilor de software se realizează pe piața biometrică a desenului papilar al degetelor.

Cel mai mic pe piață este procentul scanerelor 3D de față. De fapt, nivelul de diferențiere reflectă în mare măsură dezvoltarea și saturația pieței. Mai multe alegeri – cu atât mai mult aspectul este elaborat și adus la perfecțiune. Diferitele scanere au un set diferit de proprietăți. Practic, acesta este un set de teste pentru a verifica dacă obiectul biometric este adevărat sau falsificat. Pentru scanerele cu deget, aceasta poate fi o verificare a temperaturii sau o verificare a reliefului, pentru scanerele de ochi aceasta poate fi o verificare de acomodare a irisului, pentru scanerele față – mișcarea elementelor feței. Scanerele au un efect foarte puternic asupra statisticilor FAR și FRR obținute. În unele cazuri, aceste cifre se pot schimba de zeci de ori, în special în condiții reale. De obicei, caracteristicile algoritmului sunt date pentru o bază „ideală" sau doar pentru una bună, unde cadrele de proastă calitate și neclare sunt aruncate. Numai câțiva algoritmi indică obiectiv baza și oferirea integrală a FAR/ FRR pentru aceasta..

Amprentele digitale. Dactiloscopia (recunoașterea amprentelor digitale) – este cea mai dezvoltată metodă biometrică de identificare a identității până în prezent. Catalizatorul pentru dezvoltarea metodei a fost utilizarea sa largă în criminlistica secolului al XX-lea. Fiecare persoană are un model unic de desene papilare, ceea ce face posibilă identificarea. De obicei, algoritmii utilizează puncte caracteristice pentru amprentele digitale: sfârșitul liniei de model, ramificația liniei, punctele unice. Suplimentar sunt utilizate informații cu privire la structura

morfologică a amprentei: poziția relativă a liniilor închise de amprentă digitală, „*arc*“, și liniilor în spirală. Caracteristicile desenului papilar sunt transformate într-un cod unic care păstrează imaginea informativă a amprentei., anume „*codurile amprentei*” sunt stocate în baza de date utilizată pentru căutare și comparare. Timpul pentru a transfera imaginea amprentei codului și identificarea sa nu depășește de obicei 1s, în funcție de dimensiunea bazei de date. Timpul desfășurat pentru prezentarea mâinii nu este luat în considerare.

Caracteristicile statistice ale metodei. Sursa de date pentru FAR și FRR sunt folosite statisticile VeriFinger SDK obținute cu scanerul de amprente DP U.are.U. În ultimii 5-10 ani, caracteristicile de recunoaștere a degetului nu au avansat semnificativ, astfel încât cifrele date ne indică o medie bună pentru algoritmi moderni. Algoritmul VeriFinger a câștigat câțiva ani concursul internațional „Competiția internațională de verificare a amprentelor digitale” (International Fingerprint Verification Competition), în care au concurat algoritmi de recunoaștere a degetului. Valoarea caracteristică a FAR pentru metoda de recunoaștere a amprentelor digitale este 0,001%. Din formula (1) vom primi că munca stabilă a sistemului de identificare la FAR = 0,001% este posibilă la numărul de personal N≈300.

Avantajele și dezavantajele metodei. Avantajele metodei sunt: fiabilitate ridicată; indicatorii statistici ai metodei sunt mai buni decât indicatorii metodelor de identificare după față, voce și scris; costul scăzut al dispozitivului care scanează o imagine a amprentei digitale; o procedură destul de simplă pentru scanarea unei amprente digitale. **Dezavantaje**: modelul desenului papilar este foarte ușor, se lezează de zgârieturi mici, tăieturi.

Persoanele care folosesc scanerul la întreprinderile / instituțiile cu numărul de personal de câteva sute, afirmă prezenţa unui grad ridicat de eşec la scanare (refuzul scanării). Multe dintre scanere reacţionează inadecvat față de pielea uscată și nu oferă acces persoanelor vârstnice, de asemenea, are efect condiţiile în care activează persoanele. Cazul unei companii chimice unde încercarea de a introduce scanere de amprente digitale (s-au încercat sisteme diferite) nu s-a reuşit, deoarece impactul minim al substanţelor chimice pe degetele angajaţilor cauzează eşecul scanării (scanerele nu identifică degetele). Există, de asemenea, o lipsă de securitate împotriva imitației amprentei, parțial datorită răspândirii largi a metodei. Desigur, nu toate scanerele pot fi amăgite prin metode de la „distrugătorii de legende”,.Totuși., pentru unele persoane cu degete „nepotrivite” (în special temperatura corpului, umiditatea), probabilitatea de a i se refuza accesul poate ajunge la 100%. Numărul acestor persoane variază de la câteva procente pentru scanere scumpe până la zece la sută pentru cele necostisitoare. Desigur, trebuie remarcat faptul că un număr mare de deficiențe sunt cauzate de prevalența răspândită a sistemului, dar aceste neajunsuri au loc și se manifestă foarte des..

Irisul. Irisul ochiului este o caracteristică unică a unei persoane. Modelul irisului se formează în a opta lună de dezvoltare intrauterină, se stabilizează în final la vârsta de aproximativ doi ani și practic nu se schimbă în timpul vieții, cu excepția leziunilor grave sau a patologiilor acute. Metoda este una dintre cele mai

exacte dintre metodele biometrice. Sistemul de identificare a irisului este împărțit logic în două părți: un dispozitiv de captare a imaginii, prelucrarea primară și transmiterea acestuia la calculator și un calculator care compară imaginea cu imaginile din baza de date, transmiterea comenzii pentru admiterea la dispozitivul executiv. Timpul procesării imaginilor primare în sistemele moderne este de aproximativ 300-500 ms, viteza de comparație a imaginii rezultate cu baza are un nivel de 50 000-150 000 comparații pe secundă pe un PC convențional. O astfel de viteză de comparație nu impune restricții privind aplicarea metodei în organizații/instituţii mari atunci când este utilizată în sistemele de acces. Folosind calculatoare specializate și algoritmi de optimizare a căutării este posibilă chiar identificarea unei persoane printre locuitorii întregii țări.

Caracteristicile statistice ale metodei. Caracteristicile FAR și FRR pentru iris sunt cele mai bune în clasa sistemelor biometrice moderne (cu posibila excepție a metodei de recunoaștere după retina ochiului). Valoarea caracteristică a FAR este 0.00001%. Conform formulei (1) N≈3000 – numărul de personal din organizație, în care identificarea angajatului este destul de stabilă. Aici merită remarcată o trăsătură importantă care distinge sistemul de recunoaștere a irisului de alte sisteme. În cazul utilizării unei camere de rezoluție de la 1,3 MP, puteți capta doi ochi într-un singur cadru. Deoarece probabilitățile FAR și FRR sunt probabilități independente din punct de vedere statistic, când se recunoaște prin doi ochi, valoarea FAR va fi aproximativ egală cu pătratul valorii FAR pentru un ochi. De exemplu, pentru FAR 0,001% atunci când se utilizează doi ochi, probabilitatea de toleranță falsă va fi de 10-8%, FRR fiind doar de două ori mai mare decât valoarea FRR corespunzătoare pentru un ochi la FAR = 0,001%.

Avantajele și dezavantajele metodei. Avantajele metodei sunt: fiabilitatea statistică a algoritmului; capturarea imaginii irisului se poate face de la o distanță de câțiva centimetri până la câțiva metri, în timp ce contactul fizic al persoanei cu dispozitivul nu se produce; irisul este protejat de leziuni, deci nu se va schimba în timp. De asemenea, este posibil să se utilizeze un număr mare de metode care protejează împotriva falsificării.

Dezavantajele metodei. Prețul unui sistem bazat pe iris este mai mare decât prețul unui sistem bazat pe recunoașterea degetului sau recunoașterea feței. Disponibilitate redusă a soluțiilor gata făcute.

Detectarea/identificarea după față. Există multe metode pentru recunoașterea geometriei feței. Toate acestea se bazează pe faptul că trăsăturile feței și forma craniului fiecărei persoane sunt individuale. Această direcţie în biometrie pare a fi atractivă pentru mulți oameni, pentru că ne cunoaștem în primul rând după față. Această zonă este împărțită în două direcții: recunoaștere 2D și recunoaștere 3D. Fiecare dintre ele are avantaje și dezavantaje, dar depinde mult și de domeniul de aplicare și de cerințele înaintate unui algoritm concret. Pe scurt, vom scoate în evidență informații despre 2D și vom trece la una dintre cele mai interesante metode pentru ziua de azi – identificarea facială 3D.

Metoda 2D de recunoaștere /identificare a feței este una dintre metodele cele mai ineficiente din punct de vedere statistic al biometriei. A apărut de mult și

a fost folosită, în principal, în criminalistică, care a contribuit la dezvoltarea sa. Mai târziu, au apărut interpretările computerizate ale metodei, ca urmare a devenit mai sigură/fiabilă, dar în fiecare an din ce în ce mai mult pierde competiţia cu alte metode biometrice de identificare a personalităţii. În prezent, datorită indicatorilor statistici săraci, este utilizat în biometria încrucișată multimodală, sau în rețele sociale**.**

Caracteristicile statistice ale metodei. Pentru FAR și FRR, datele sunt folosite pentru algoritmi VeriLook. Din nou, pentru algoritmi moderni are caracteristici obișnuite. Uneori, se atestă algoritmi cu FRR 0,1% cu un FAR similar, însă bazele pe care sunt obținute sunt foarte îndoielnice (fundal tăiat, expresie facială asemănătoare, coafuri/frezuri asemănătoare, iluminare). *Valoarea caracteristică a FAR este de 0,1%***.** Din formula (1) obținem N≈30 - numărul personalului din organizație/instituţie, în care identificarea unui angajat este destul de stabilă. După cum puteți vedea, indicatorii statistici ai metodei sunt modești: aceasta surclasează avantajul metodei că este posibilă efectuarea unei fotografii ascunse a persoanelor în locuri aglomerate. Este amuzant să vedem cum de câteva ori pe an se finanțează următorul proiect pentru a detecta infractorii prin camere video instalate în locuri aglomerate. În ultimii zece ani, caracteristicile statistice ale algoritmului nu s-au îmbunătățit deși numărul acestor proiecte a crescut. Este demn de remarcat faptul că pentru a urmări oamenii în mulţime printr-o multitudine de camere, algoritmul este destul de potrivit.

Avantajele și dezavantajele metodei. Avantajele metodei. La recunoașterea 2D, spre deosebire de cele mai multe metode biometrice, nu sunt necesare echipamente/utilaje costisitoare. Cu echipamentul adecvat, există posibilitatea de recunoaștere la distanțe considerabile de la camera video.

Dezavantaje. Fiabilitate statistică scăzută. Există cerințe pentru iluminat (de exemplu, nu este posibil să se înregistreze persoanele care intră în încăperi de pe străzi într-o zi însorită). Pentru mulți algoritmi, inadmisibilitatea oricărei interferențe externe, cum ar fi ochelarii, barba, anumite elemente ale coafurii. Este obligatorie poziţia frontală a feţei cu mici deviaţii. Mulți algoritmi nu iau în considerare posibilele modificări ale expresiilor faciale, adică expresia trebuie să fie neutră.

Recunoașterea/identificarea feţei prin metoda 3D. Implementarea acestei metode este o sarcină destul de dificilă. În ciuda acestui fapt, în prezent, există multe metode pentru recunoașterea feţei 3D. Metodele nu pot fi comparate între ele, deoarece folosesc diferite scanere și baze. Nu toate oferă FAR și FRR, utilizând abordări absolut diferite. O tranziţie de la metoda 2D la 3D este metoda care pune în aplicare acumularea de informaţii despre o persoană. Această metodă are caracteristici mai bune decât metoda 2D, dar la fel ca aceasta folosește doar o singură cameră. Când subiectul este introdus în baza de date, subiectul își întoarce capul și algoritmul leagă imaginea împreună creând un șablon 3D. Când are loc recunoașterea sunt folosite mai multe cadre ale fluxului video. Această metodă se referă mai degrabă la cele experimentale și realizarea pentru sisteme ACS nu s-au testat. Metoda cea mai clasică este de proiectare a unui șablon. Ea constă în proiectarea unei grile pe un obiect (faţa). Apoi, aparatul foto face fotografii la o viteză de zeci de cadre pe secundă,

iar imaginile rezultate sunt procesate de un program special. Fasciculul care se încadrează pe suprafaţa curbată este îndoit - cu cît e mai mare curbura suprafeţei, cu atât e mai mare îndoirea fasciculului. Iniţial, a fost aplicată o sursă de lumină vizibilă, minimalizată cu „jaluzele". Ulterior, lumina vizibilă a fost înlocuită de o lumină infraroșie, care are o serie de avantaje. De obicei, în prima etapă de procesare, imaginile sunt aruncate, persoana nu este vizibilă deloc sau există obiecte străine care interferează cu identificarea. În baza imaginilor primite, este structurat modelul de faţă 3D, pe care se evidenţiează și îndepărtează interferenţe nedorite (păr, barbă, mustaţă și ochelari). Apoi modelul este analizat - sunt evidenţiate, elementele antropometrice, care în final sunt înscrise într-un cod unic introdus în baza de date. Timpul de captare și de procesare este de 1-2 secunde pentru cele mai bune modele. De asemenea, câștigă popularitate, metoda de recunoaștere 3D prin imaginea primită de la mai multe camere video.

Indicii statistici ai metodei 3D. Datele complete despre FRR și FAR pentru algoritmi din această clasă pe site-urile producătorilor nu sunt dezvăluite. Dar pentru cele mai bune modele ale companiei Bioscript (3D EnrolCam, 3D FastPass), care lucrează prin metoda de proiectare a șablonului la FAR = 0.0047% FRR este 0.103%. Se consideră că fiabilitatea statistică a metodei este comparabilă cu fiabilitatea metodei de identificare a amprentelor digitale.

Avantajele și dezavantajele metodei 3D. Avantajele metodei sunt: nu este nevoie să contactaţi scanerul; sensibilitate scăzută la factorii externi, atât asupra persoanei în sine (aspectul ochelarilor, bărbiilor, schimbarea coafurii), cât și în împrejurimile sale (iluminarea, întoarcerea capului); nivel ridicat de fiabilitate, comparabil cu identificarea amprentelor digitale.

Dezavantajele metodei. **3D.** Costurile sporite ale echipamentului. Sistemele disponibile în vânzare au depășit costul scanerelor pentru iris. Modificările mimicii feţei și interferenţele pe faţă înrăutăţesc fiabilitatea statistică a metodei. Metoda nu este încă bine dezvoltată, în comparaţie cu amprentele utilizate de mult timp, ceea ce face ca aplicarea sa să fie dificilă. Trebuie să remarcăm că această metodă este destul de răspândită și ei i se acordă preferinţă faţă de recunoașterea după irisul ochiului. Ponderea tehnologiilor de recunoaștere a feţei în volumul total al pieţei biometrice mondiale poate fi estimată la 13-18%. În domeniul recunoașterii 2D a feţei, subiectul principal al dezvoltării este software-ul, deoarece camerele obiţnuite sunt excelente la captarea imaginii feţei. Soluţia problemei recunoașterii feţei într-o oarecare măsură a ajuns într-un impas – pentru câţiva ani nu s-a oferit practic o îmbunătăţire a parametrilor statistici ai algoritmilor. În acest domeniu, are loc „lucrul sistematic asupra greșelilor". Recunoașterea 3D a feţei este acum o zonă mult mai atractivă pentru dezvoltatori. În domeniu muncesc o mulţime de echipe și în mod regulat apar noi descoperiri. O mulţime de lucrări se află într-o stare „pe cale să fie oferite".

În fine, considerăm că pentru asigurarea unui sistem eficient și viabil este necesar crerea unui sistem mixt care ar permite identificarea în baza diferitor parametri. Astfel ca spre exdemplu ne-ar putea servi sistemul de identificare biometric în baza amprentelor digitale și sitemul de identificare facială 2D (care este mai

ieftin), ulterior finnd înlocuit cu 3D când va fi la preţuri și viabilitate corespunzătoare disponibile pentru procurare. În cazul exemplului am menţionat că aceste sisteme se utilizează pentru acces în instituţii, dar totodată acestea ar putea fi utilizate și la trecerile de frontieră. În acest context considerăm viabilă comasarea unui sistem de tip „Imagetrac".

În anul 2004 în România s-a implementat sistemul integrat de identificare facială la nivel naţional numit „Imagetrac" care este compus dintr-un server de date central, instalat în Institutul de criminalistică a MAI, la care sunt conectate 42 de staţii de lucru, instalate în fiecare judeţ, sistemul oferind următoarele facilităţi: stocarea datelor de stare civilă pentru un număr de 500 mii de persoane, stocarea unui număr de maxim 6 fotografii digitale pentru fiecare persoană, căutarea și regăsirea în baza de date a unei persoane după datele de stare civilă, date antropometrice, semne particulare, cicatrice/tatuaje, căutarea și regăsirea în baza de date a unei persoane după fotografia frontală sau portretul robot [3, p.320]. Sistemul funcţionează în baza algoritmului de recunoaștere facială (Local Feature Analysis - LFA), se disting 80 de puncte nodale pentru faţă, care măsoară: distanţa între ochi, lăţimea nasului, adîncimea orbitelor, oasele feţei, linia maxilarului, bărbia. Algoritmul este independent de culoarea fotografiei sau a pielii; rasă (structura feţei este universală indiferent de rasă); sursa de preluare a imaginii (scaner, cameră foto sau video etc.); vârstă (faceprint-ul rămâne neschimbat odată cu trecerea timpului); machiaje, păr facial, ochelari, iluminare [1, p. 42-43]. În anul 2016 acest sistem a primit dezvoltare calitativă la nivel de ţară în România. Exemplul oferit de România ne oferă o viziunile de utilizare a sistemelor biometrice de ideentificare atât la nivel de ţară cât și la regimul de frontieră.

Sistemul respectiv în care să fie stocate datele persoanelor date în căutare pentru comiterea infracţiunilor pe teritoriul R. Moldova sau căutare internaţională și un sistem de identificare biometrică spre exemplu amprentă digitală și identificare facială 2D/3D care automat ar scana persoanele la trecerile de forontieră și ar semnala în caz de identificare personalul specializat și abilitat în acest domeniu (MAI, SIS etc.) în vederea întreprinderii unor măsuri corespunzătoare.

Recunoașterea după structura venelor de pe mână. Aceasta este o nouă tehnologie în domeniul biometriei, aplicarea căreia a început acum 5-10 ani. Camera în infraroșu captează imagini din exterior sau din interiorul mâinii. Modelul venelor se formează datorită faptului că hemoglobina din sânge absoarbe radiaţiile IR. Ca urmare, gradul de reflecţie este redus, iar venele sunt văzute pe aparatul foto sub formă de linii negre. Un program special bazat pe datele obţinute creează o convoluţie digitală. Nu este necesar un contact fizic cu scanerul. Tehnologia este comparabilă după fiabilitate/siguranţă cu recunoașterea în baza irisului ochiului, fiind parţial superioară faţă de ultima, și în unele aspecte inferioară. Valorile FRR și FAR sunt pentru scanerul Palm Vein. Potrivit producătorului la FAR 0,0008% FRR este de 0,01%. Un grafic mai exact pentru mai multe valori nu este produs de nici o firmă**.**

Avantajele și dezavantajele metodei. Avantajele metodei. Nu este nevoie de contact fizic cu scanerul. Fiabilitate/siguranţă înaltă – indicatorii statistici ai me-

todei sunt comparabili cu indicaţiile identificării irisului. Caracteristicile camuflate: spre deosebire de toate cele menţionate mai sus, această caracteristică este foarte dificil de a obţine de la o persoană „pe stradă", de exemplu, fotografiind-o.

Dezavantajele metodei. Este inadmisibilă iluminarea scanerului cu raze solare și razele becurilor cu halogen. Unele boli legate de vârstă, cum ar fi artrita, afectează foarte mult FAR și FRR. Metoda este mai puțin studiată în comparaţie cu alte metode statice de biometrie. Recunoașterea venelor manuale este o tehnologie destul de nouă și, prin urmare**,** cota sa pe piaţa mondială este mică și este de aproximativ 3%. Cu toate acestea, această metodă devine din ce în ce mai interesantă datorită faptului că este o metodă precisă care nu necesită echipamente costisitoare, cum ar fi metodele de recunoaștere prin geometria feţei sau iris [4].

Retina ochiului. Până de curând, se considera cea mai sigură metodă de identificare biometrică și de autentificare a personalităţii. Este o metodă bazată pe scanarea retinei ochiului. Acesta conţine cele mai bune trăsături de identificare prin iris şi prin venele mâinii. Scanerul citește desenul capilarelor de pe suprafaţa retinei. Retina are o structură fixă, neschimbată în timp, cu excepţia cazulrilor de boală, de exemplu, a cataractei. Scanarea retinei se realizează utilizând lumină infraroșie cu intensitate scăzută, direcţionată prin pupilă către vasele de sânge din spatele ochiului. Scanerele retinale sunt utilizate pe scară largă în sistemele de control al accesului pentru obiecte securizate, deoarece au unul dintre cele mai mici procente de refuz al accesului pentru utilizatorii înregistraţi și nu există aproape nici un acces eronat. Din păcate, apar o serie de dificultăţi atunci când se folosește această metodă de biometrie. Scanerul aici este un sistem optic foarte complex și o persoană nu ar trebui să se deplaseze timp îndelungat în timp ce sistemul este indus, ceea ce cauzează senzaţii neplăcute. Potrivit lui EyeDentify pentru scanerul ICAM2001 la FAR = 0,001%, valoarea FRR este de 0,4%..

Avantajele și dezavantajele metodei.. Beneficii. Nivel ridicat de fiabilitate/siguranţă statistică. Datorită răspîndirii scăzute a sistemelor, există puţine probabilităţi de a dezvolta o modalitate de a le înșela.

Dezavantaje. Un sistem cu un timp de procesare ridicat este dificil de utilizat. Costul ridicat al sistemului. Lipsa unei piețe ample de aprovizionare și, ca o consecinţă, insuficienţa intensităţii de dezvoltare a metodei.

Geometria mâinilor. Această metodă provine din criminalistică și este utilizată de cel puţin 10 ani, dar în ultima perioadă de timp a înregistrat o scădere. Metoda se bazează pe obţinerea caracteristicilor geometrice ale mâinilor: lungimea degetelor, lăţimea palmelor etc. La fel ca retina ochiului pierde teren. Dat fiind faptul că are caracteristici mult mai slabe, nu vom realiza o descriere complexă. Uneori în sistemele de recunoaștere prin vene se aplică metode geometrice de recunoaștere. Adesea atunci când se recunoaște prin vene, se fotografiază doar palma (laba mâinii), în timp ce atunci când are loc recunoașterea prin geometrie, se efectuează și fotografierea degetelor.

Chiar și în clasa sistemelor statice de biometrie există o gamă largă de sisteme. Care ar trebui de ales? Totul depinde de cerinţele sistemului de securitate. Sistemele cele mai fiabile din punct de vedere statistic și rezistente la falsuri sunt

sistemele de toleranţă pentru iris şi venele mâinilor. La prima dintre ele există o piaţă mai largă de oferte. Dar aceasta nu este limita. Sistemele biometrice de identificare pot fi combinate pentru a obţine o precizie astronomică.

La prima vedere, utilizarea pe scară largă a identificării biometrice pare foarte tentantă. Nu este nevoie să vă amintiţi parolele, nu există riscul de a pierde o cartelă inteligentă sau alte mijloace de acces, de obicei, identificarea trece rapid şi simplu. Din păcate, toate aceste avantaje sunt compensate de dezavantajul fundamental al informaţiilor biometrice, fiind un bun identificator, este o „cheie" ce lasă de dorit. Problema reiese din faptul că orice sistem biometric nu compară între ele obiecte din lumea reală, ci rezultatele măsurătorilor. Prin urmare, o serie de oportunităţi excelente de a o induce în eroare. De exemplu, obţinând rezultate de măsurare ale altor persoane, le puteţi salva în prealabil şi utiliza ulterior pe un sistem gata de procesare şi, după ce aţi accesat echipamentul, intraţi în sistem ocolind senzorii biometrici. Accesul la software va înlocui datele stocate în sistem de către un alt utilizator cu proprii lor. Dar fără acces, este uşor să înşelaţi verificarea biometrică, prezentând senzorilor un model/mulaj, de exemplu, degetul altcuiva. Acum, noile paşapoarte marcate cu un simbol special sunt inscripţionate cu un cip electronic care conţine date personale şi biometrice standardizate. Din cele din urmă, cu toate acestea, utilizate pe scară largă până acum, dar şi atât de disponibil în fotografia documentului, în unele ţări sunt deja gata să scrie pe cip nu numai amprentele, ci şi datele scanării irisului. Dacă la punctul de acces/control se va depista că desenele lor nu se potrivesc cu ale tale, ar fi ca şi cum ai da paşaportul poliţistului de frontieră cu o fotografie străină. Pentru a falsifica un astfel de desen este mult mai greu decât fotografiile: chiar dacă s-ar învăţa cum de înlocuit cipul imprimat, datele înregistrate trebuie să fie certificate cu o semnătură digitală electronică pe care o au numai autorităţile care emit paşapoarte biometrice. Se pot citi liber datele existente, dar nu le veţi putea genera fără cheia secretă a semnăturii digitale. Acesta este un aspect „la moment" sigur. Totuşi, încercând să demonstreze vulnerabilitatea paşapoartelor biometrice, grupul hackerilor „The Hacker's Choice" a produs un document fals în 2006 în numele lui Elvis Aaron Presley. S-a dovedit că, în terminalul aeroportului din Amsterdam, datele din paşaport au fost citite fără probleme şi au fost afişate pe ecran. Cu toate acestea, acest lucru nu a deranjat autorităţile. Spre deosebire de scanerele de control al frontierei, terminalul folosit de hackeri era doar un dispozitiv de referinţă/scanare, citea date din paşaport, dar nu verifica semnătura lor digitală.

Deci, pentru a crea un fals complet al paşapoartelor biometrice infractorii vor trebui să fure cheia privată, cu care Ministerul de Interne al unei ţări semnează datele din cipurile paşapoartelor, iar acest lucru este un spionaj de nivel superior . Dar mai devreme sau mai târziu, şi acest lucru ar trebui să se întâmple, astfel încât în viitor cheile să fie schimbate periodic, iar cetăţenii respectabili vor trebui să-şi actualizeze paşapoartele.

Un alt aspect social privind tehnologiile biometrice constă în faptul că fiecare verificator al unui identificator poate genera o înregistrare în baza de date despre circumstanţele acestui eveniment. Când prezentaţi un paşaport la un ae-

roport, hotel sau ofiţer de poliţie care întocmește un process-verbal, fiţi pregătiţi pentru ca datele dvs. să rămână în evidenţa documentară electronică. Iar dacă autorităţile se vor interesa de personalitatea dvs., aceste informaţii vor fi extrase la suprafaţă. Dar aceasta a fost înainte, de introducerea documentelor biometrice. Ce s-a schimbat? Pentru moment aproape nimic - era de biometrie este doar la început. Anterior, o persoană lăsa o urmă informaţională numai în câteva locuri, de obicei în instituţii de stat. Această procedură a fost destul de laborioasă și a fost efectuată manual. Acum, oamenii, fără să le observe, generează o mulţime de înregistrări în bazele de date. Aceste baze sunt împrăștiate, deoarece acestea aparţin unor organizaţii diferite, și fiecare folosește un identificator diferit: pentru stat - detalii paşaport, banca - numărul de card de credit, în supermarket - carte cu discount la locul de muncă - trecere electronică, la operatorul de telefonie mobilă - numărul, furnizorul de servicii Internet și pe site-uri diferite - conectări multiple cu parole. În cazul unei anchete serioase, aproape toţi aceşti identificatori pot fi asociaţi cu o singură persoană, dar acest lucru necesită măsuri speciale de căutare operaţională. Identificarea biometrică ne va salva de o mulţime de cartele. Este suficient să plasaţi paşaportul biometric, sau să contactaţi cu degetul scanerul și să obţineţi tot ce vi se cuvine. Dar plata pentru comoditate va fi un singur identificator biometric atribuit persoanei pentru o varietate de baze de date. Dacă aveţi acces la ele, puteţi obţine rapid și ușor multe informaţii despre viaţa dvs. privată: cu cine comunicaţi, ceea ce cumpăraţi, unde vă odihniţi, dacă rămâneţi adesea la locul de muncă. Adăugaţi la aceasta datele de pe blogul dvs. și poftim în faţa escrocilor există un domeniu de activitate uriaș și cel mai important, având o astfel de bază de date cu milioane de înregistrări, un criminal poate selecta în mod optim o victimă. Nu cred că baza de date cu informaţii personale sunt atât de dificil de accesat. În lume există întotdeauna scurgeri mari de informaţii, cele cunoscute de opinia publică fiind probabil, doar o mică parte a numărului de acţiuni care au loc cu adevărat. Dacă anterior doar câteva agenţii/instituţii de stat ar putea să compună un dosar exhaustiv, acum aceasta este o activitate de rutină a serviciilor de securitate ale companiilor comerciale. Confidenţialitatea este rapid spălată din vieţile noastre. Dar chiar dacă informaţia nu merge dincolo de zidurile organelor abilitate ale statului, dacă este posibil să se bazeze pe faptul că guvernul va folosi informaţia despre cetăţenii săi numai în scopuri benefice, de exemplu, pentru a prinde teroriști și alţi criminali. Abilitatea de a stabili cu ușurinţă datele intime privind orice persoană creează un vector larg pentru abuz. Sursa de informare, pista de informaţii pot fi utilizate pentru a elimina concurenţi sau pentru a se răfuie cu adversarii politici. Deoarece de accesul la o astfel de bază de date au nevoie mai multe structuri guvernamentale, careva cu siguranţă poate fi veriga slabă. În sfârșit, guvernele nu numai că nu sunt perfecte, dar nici nu sunt veșnice. Democraţia poate fi înlocuită de un regim autoritar sau totalitar, așa cum s-a întâmplat adesea în cursul secolului trecut. Și atunci, bazele de date uriașe vor ajuta statul să caute și să urmărească oameni care nu sunt convenabili pentru el, desigur, de dragul unui scop măreţ, în aacest caz de un control total nu va scăpa nimeni - amprentele digitale și alte atribute biometrice ce le posedă omul de la naștere nu este

ușor să și le schimbe, chiar și cu suportul unui chirurg plastic calificat.

Respectiv este argumentat riscul unei astfel de evoluții a evenimentelor de acele facilități de uz casnic și o anumită creștere a eficacității structurilor de ocrotire a legii, care ne promite nouă epoca biometriei? Fără îndoială, este zadarnic să încerci să oprești progresul tehnologic. Tehnologiile biometrice și bazele largi de date cu caracter personal au intrat deja în viața noastră și au dus la eroziunea inevitabilă a vieții private. Pentru a păstra chiar rămășițele acesteia, sunt necesare legi pentru protejarea informațiilor personale împotriva violării. În multe țări există deja astfel de legi. Dar ei sunt, de asemenea, neputincioși să compenseze daunele rezultate din scurgeri de date și să servească doar pentru prevenirea și pedepsirea vinovaților. De multe ori putem auzi părerea: „Lăsați-i să se uite, un om cinstit nu are nimic de ascuns". Dar vorbitorii nu iau în considerare faptul că cei ce urmăresc nu se dovedesc neapărat că vor fi oameni cinstiți. Având ocazia de a observa viața privată a cetățenilor, aceștia pot, în propriile lor interese, să intervină în activități comerciale sau să persecuteze pentru convingeri. Desigur, în situații controversate, transparență și documentarea vieții private va ajuta statul și instituțiile sale a răspunde mai rapid la întrebarea: „Cine este vinovat?" dar în acest context apare întrebarea rezonabilă, va coincide această opinie cu privire la vinovăție cu a dvs?

Actualmente soluțiile biometrice oferă o doză suplimentară de asigurare a siguranței, totuși în lumina celor expuse în cadrul acestui articol fiind însoșită de o bază legală democtrică și supravegherea atâta din partea societății la nivel de țară cât și la nivel regional sau internațional în vederea preîntâmpinării utilizării abuzive de către un regim autoritar pe cale de a deveni – dictatorial.

În fine, considerăm prioritară asigurarea unui vechi dar viabil pentru toate timpurile deziderat: „**Cel ce este puternic să fie și drept, cel ce este drept să fie și puternic**".

BIBLIOGRAFIE

1. Bulai Iurie, Teza de doctor „Bazele științifice, pregătirea și efectuarea prezentării spre recunoaștere", Chișinău, 2016, p. 42-43.

2. Bulai Iu., Bulai R., Particularități de asigurare a securității frontierii prin sisteme biometrice de identificare.

3. Popa Gh., Utilizarea de către poliția română a sistemului „Imagetrak", sistem de recunoaștere și compunere facială. În: Revista de criminologie, criminalistică și de penologie. București, 2005, nr. 2, 320 p.

4. https://habrahabr.ru/post/126144.

5. 18 сентября 1990 «Как нам обустроить Россию», «Литературной газете» и «Комсомольской правде публицистическое эссе Александра Солженицына, написанное в июле 1990 года, содержащее размышления автора о путях возрождения страны и разумных основах построения жизни народа и государства после конца «коммунистического периода».