THE ASPECTS OF ANALYSIS OF BIOMETRIC AUTHENTICATION SYSTEMS OF THE TEACHING OF COMPUTER SCIENCE

Viktoras Stupak[*]
Raimondas Vasiliauskas[**]

Mykolas Romeris University

S u m m a r y

At the faculty of Public Safety of Mykolas Romeris University, subjects of computer science are taught during the first, second and third year. For the program of preparation of bachelors for a specialty of the right and protection of frontier, these disciplines are taught during the first and third years. For the program of preparation of bachelors for a specialty of the right and activity of police – during the first year. For non– university training, under the program activity of police – during the first and second years. In programs of subjects during studying the means of safety for both information technologies, and other objects, the consideration of biometrics authentication systems is stipulated.

Features of consideration of biometrics authentication systems at studying computer science are analyzed. Classification of biometrics systems is provided. Two groups of the automated biometrics systems are analyzed. The systems using unique physiological features of human are included in the first group. The second group includes the systems using specific features of behavior. The structure of the systems, tasks they carry out and areas of their application are analyzed.

BIOMETRINIŲ ATPAŽINIMO SISTEMŲ EFEKTYVUMO NAGRINĖJIMO INFORMATIKOS STUDIJOSE ASPEKTAI

Viktoras Stupak[*]

[*] Mykolas Romeris university Kaunas Faculty assoc. prof. dr. of Police Activity Department
[**] Mykolas Romeris university Kaunas Faculty assoc. prof. dr. of Police Activity Department

Raimondas Vasiliauskas[**]

Mykolo Romerio universiteto Kauno policijos fakulteto Policijos veiklos katedra
V. Putvinskio g. 70, LT- 44211, Kaunas
Telefonas 8 (37) 30 36 45
Elektroninis paštas v.stupak@mruni.lt; r.vasiliauskas@mruni.lt

SANTRAUKA

Teisės ir valstybės sienos apsaugos bakalauro studijų programoje informatikos profilio dalykai dėstomi I ir III kursuose, teisės ir policijos veiklos bakalauro studijų programoje – I kurse, policijos veiklos neuniversitetinių studijų programoje – I ir II kursuose. Dalykų programose, nagrinėjant priemones, užtikrinančias informacinių technologijų ir kitų objektų saugą, numatyti biometrinių sistemų analizės klausimai. Nagrinėjant biometrines atpažinimo sistemas analizuojamas sistemų efektyvumas.

Aptariami biometrinių atpažinimo sistemų nagrinėjimo informatikos studijose ypatumai. Analizuojama biometrinės sistemos racionalaus varianto pasirinkimo procedūra. Nagrinėjami veiksniai, įtakojantys šį pasirinkimą: sistemos naudojimo tikslai, vartotojų srauto dydis, sistemos kaina ir kt. Siūlomas biometrinės sistemos efektyvumo vertinimo metodas.

Pagrindinės sąvokos: atpažinimas, autentifikavimas, biometrinės sistemos, efektyvumas, informatikos studijos.

ĮVADAS

Informacinės visuomenės plėtros darbų, informacinių technologijų ir sistemų vystymasis kelia vis aukštesnius reikalavimus informacinių sistemų ir informacijos saugai, asmenų tapatybės nustatymo procedūroms.

Elektroninės valdžios koncepcijoje numatyta, kad „…Gyventojų pasitikėjimas valstybės informacinėmis sistemomis bus pasiektas tik tokiu atveju, jeigu šios sistemos bus saugios. E. valdžios projektai galės funkcionuoti, kai bus užtikrinta informacinių technologijų ir telekomunikacijų sauga, gyventojų interesų teisinė apsauga valstybės informacinėse sistemose…“ [1]. Be to, planuojama, kad „…bus sukurta gyventojų tapatybės nustatymo informacinėse sistemose sistema…“ [1].

---

[*] Mykolo Romerio universiteto Kauno policijos fakulteto Policijos veiklos katedros docentas
[**] Mykolo Romerio universiteto Kauno policijos fakulteto Policijos veiklos katedros docentas

Mykolo Romerio universiteto Viešojo saugumo fakultete rengiant būsimus policijos ir valstybės sienos apsaugos pareigūnus informatikos profilio disciplinos numatytos I, II ir III kursuose. Dalykų programose, nagrinėjant priemones, užtikrinančias informacinių technologijų ir kitų objektų saugą, numatyti biometrinių sistemų analizės klausimai. Nagrinėjant biometrines atpažinimo sistemas analizuojamas šių sistemų efektyvumas.

Straipsnyje aptariami biometrinių atpažinimo sistemų efektyvumo nagrinėjimo informatikos studijose ypatumai. Analizuojama biometrinės sistemos racionalaus varianto pasirinkimo procedūra. Nagrinėjami veiksniai, įtakojantys šį pasirinkimą. Siūlomas biometrinės sistemos efektyvumo vertinimo metodas.

1. BIOMETRINIŲ ATPAŽINIMO SISTEMŲ EFEKTYVUMO NAGRINĖJIMO INFORMATIKOS STUDIJOSE YPATUMAI

Biometrinių atpažinimo sistemų nagrinėjimą informatikos studijose studentai pradeda nuo susipažinimo su informacinių sistemų bei informacijos sauga, nuo sistemos vartotojų ir aplamai asmenų atpažinimo (tapatybės nustatymo) klausimų nagrinėjimo [2]. Toliau atliekamas biometrinių sistemų klasifikavimas, analizuojama jų struktūra, panaudojimo sritys, sistemų techniniai ir kiti parametrai, sistemų naudojimo efektyvumas.

Užsiėmimuose pabrėžiama, kad biometrinių atpažinimo sistemų naudojimo efektyvumo klausimą tikslinga nagrinėti priimant sprendimus, leidžiančius užtikrinti nagrinėjamo objekto saugos lygį. Tokių sprendimų pavyzdžiai galėtų būti šie: kokią biometrinę sistemą naudoti konkrečiu atveju, kokį pasirinkti biometrinės sistemos gamintoją, atpažinimo procedūroje ar naudoti vieną arba iškart kelis biometrinius tapatybės nustatymo metodus, ir pan. Atliekant šiuos darbus tenka analizuoti ir tokius klausimus:

- kokiam tikslui bus naudojama biometrinė sistema – verifikacijai, identifikacijai ar paieškos (stebėjimo) sąrašo analizei;
- kokie yra nustatyti saugumo reikalavimai objektui, kuriame turėtų būti įdiegta biometrinė asmens tapatybės nustatymo sistema;
- koks vartotojų, kuriems turėtų būti nustatoma tapatybė, srauto dydis;
- ar geometriniai biometrinio skenerio dydžiai turės įtakos biometrinės sistemos panaudojimui konkrečiu atveju;
- koks asmens tapatybės nustatymo algoritmas ir programinis aprūpinimas – ar sistema dirbs automatiniu ar automatizuotu režimu, dalyvaujant operatoriui;
- kokia biometrinės sistemos kaina;

- koks biometrinės sistemos kainos atsipirkimo laikas;
- kokia biometrinės sistemos kainos įtaka sistemos panaudojimo galimybėms;
- kokie biometriniai požymiai gali būti pasirenkami asmens tapatybės nustatymo procese;
- ar galima įdiegiamą sistemą integruoti į jau veikiančias.

Pabrėžiama, kad biometrinių atpažinimo sistemų efektyvumo analizė gali būti suprantama kaip sistemos racionalaus varianto pasirinkimo procedūra.

2. BIOMETRINIŲ ATPAŽINIMO SISTEMŲ EFEKTYVUMO ANALIZĖ

Biometrinės atpažinimo sistemos efektyvumu siūloma vadinti jos gebėjimą nustatytomis sąlygomis tenkinti poreikius laipsnį. Tuomet sistemos efektyvumo rodiklis E gali būti apskaičiuojamas taip:

$$E = \sum_{j=1}^{n} K_j P_j \,, \tag{1}$$

$$\sum_{j=1}^{n} K_j = 1 \,, \tag{2}$$

čia K_j – j – jo kriterijaus svorio koeficientas, ($j = \overline{1,n}$); P_j – j – jo kriterijaus įvertinimas balais, ($j = \overline{1,n}$); n – nagrinėjamų kriterijų skaičius.

Formulėse (1) ir (2) nagrinėjami kriterijai, įtakojantys efektyvumo rodiklio E vertes. Šiuos kriterijus galima skirstyti į bendrus, būdingus kiekvienam biometriniam metodui, ir papildomus. Lentelėje 1 pateikiamas šiuo metu vartojamų biometrinių metodų [3–5] sulyginimas pagal bendrus kriterijus. Biometrinio metodo atitikimas konkrečiam kriterijui (reikalavimui) vaizduojamas panaudojant kokybinę skalę: A – aukštas atitikimo laipsnis, V – vidutinis, Ž – žemas. Toliau išsamiau apibūdinami bendrieji kriterijai, nurodyti 1 lentelėje.

Universalumas – kriterijus apibūdina tai, kad biometrinį požymį, kuris reikalingas naudojamam biometriniam metodui, turi turėti kiekvienas žmogus. Tikrovėje kiekvienas metodas turi tam tikrus apribojimus, nes daliai žmonių metodas negali būti taikomas iš principo (pvz. žmogus neturi piršto ar jo dalies, akies ir pan.).

Unikalumas (skirtingumas) – kriterijus apibūdina tai, kad tokio pačio biometrinio požymio, kuris naudojamas atpažinimui, negali turėti du skirtingi žmonės. Unikalumą galima apibrėžti, kaip minimalią atpažinimo antrojo laipsnio klaidos tikimybę (pripažinti „svetimą“ kaip „savą“). Praktikoje šios tikimybės mažinimas susietas su metodo jautrumo sumažėjimu ir su

atpažinimo pirmojo laipsnio klaidos tikimybės padidėjimu, kai sistema neatpažįsta jai žinomą subjektą.

1 lentelė. Biometrinių požymių sulyginimas pagal bendrus kriterijus

Biometrinis požymis (metodas)	*Bendri kriterijai*							
	Universalumas	*Unikalumas*	*Permanentiškumas*	*Pamatuojamumas*	*Atsparumas aplinkos faktoriams*	*Tikslumas*	*Atsparumas klastojimui*	*Socialinis priimtinumas*
Piršto atspaudai	V	A	A	V	Ž	A	V	V
Delno atspaudai	V	A	A	V	V	A	A	V
Delno geometrija	V	V	V	A	V	V	V	V
Delno kraujagyslės	V	V	V	V	V	V	A	A
Akies rainelė	A	A	A	V	V	A	A	Ž
Akies tinklainė	A	A	V	Ž	A	A	A	Ž
Veidas dvimatis	A	Ž	V	A	Ž	V	V	A
Veidas trimatis	A	V	V	V	V	V	A	A
Veido termograma	A	A	Ž	A	V	V	A	A
Ausies geometrija	V	V	A	V	V	A	V	A
Kvapas	A	A	A	Ž	Ž	Ž	Ž	V
Genetinio kodo	A	A	A	V	A	A	A	V

fragmentai								
Eisena	V	Ž	Ž	A	Ž	A	V	A
Darbas su klaviatūra	Ž	Ž	Ž	V	Ž	V	V	V
Parašas	Ž	Ž	Ž	A	A	V	Ž	Ž
Balsas	V	Ž	Ž	V	Ž	V	Ž	A

Permanentiškumas – kriterijus apibūdina tai, kad naudojamas biometrinis požymis turi nesikeisti laike (taip vadinamas biometrinio šablono senėjimas). Permanentiškumą galima įvertinti atpažinimo pirmojo laipsnio klaidos tikimybės dydžio priklausomybe nuo laiko. Šiuo tikslu naudojama informacija apie testus, atliekamus su tais pačiais atrinktais individais, esant fiksuotai atpažinimo antrojo laipsnio klaidos tikimybei.

Pamatuojamumas – kriterijus apibūdina tai, kad biometrinis požymis turi būti lengvai pamatuojamas. Pamatuojamumo kriterijų galima kiekybiškai įvertinti nepasisekusios registracijos dydžiu – tai yra procentiniu santykiu individų, kurie nebuvo užregistruoti (sistema negalėjo sukurti biometrinio šablono) per vidutinišką atpažinimo trukmę.

Sprendžiant prieigos kontrolės uždavinius, ypatingai sudėtingose transporto sistemose, atpažinimo trukmė tiesiogiai sąlygoja praėjimo per kontrolės punktą greitį, o tuo pačiu ir jo pralaidumą. Nepasisekusios registracijos dydis nusako procentą žmonių, kurie negalės pasinaudoti sistema. Į šį dydį įskaitomi ir tie atvejai, kai individas neturi reikalingo biometrinio požymio arba jis dėl įvairių priežasčių duotam asmeniui esamu skeneriu negalės būti pamatuotas. Pavyzdžiui, atpažinimui pagal akies tinklainę, reikalingas didelės skiriamosios gebos jos vaizdas, kuris gali būti gautas tik esant tiksliam akies pozicionavimui skenerio atžvilgiu. Tapatybės nustatymas panaudojant piršto atspaudą daugelio žmonių grupių yra apsunkintas. Tai žmonės dirbantys fizinį darbą, žmonės su silpnai išreikštu ar ištrintu papiliariniu raštu, pagyvenę žmonės su sausa oda ar žmonės su dermatologiniais defektais. Bet to dėl didelio nuolatinio kontakto pirštų atspaudų skenerių paviršiai užsiteršia. Asmens tapatybės nustatymo metodai pagal dvimatį ar trimatį veido vaizdą yra bekontaktiniai, įrenginiams registruojantiems veido vaizdą nekeliami specialūs reikalavimai, todėl ir biometriniai požymiai yra santykinai lengvai pamatuojami.

Atsparumas aplinkos faktoriams – kriterijus apibūdina biometrinio metodo atsparumą supančios aplinkos pokyčiams. Įvairių biometrinių sistemų eksploatacinės savybės žymia dalimi priklauso nuo aplinkos sąlygų, kurioms keičiantis, prarandamas biometrinių požymių matavimų

rezultatų stabilumas. Pavyzdžiui pirštų atspaudų skeneriai užteršiami, dėl to pablogėja jų darbo kokybė, dvimačių veido atpažinimo metodų darbo rezultatai priklauso nuo išorinio apšvietimo sąlygų ir pan.

Tikslumas – kriterijus apibūdina biometrinio metodo paklaidas. Biometrinę tapatybės nustatymo sistemą galima nustatyti norimam „budrumo“ lygiui (atpažinimo antrojo laipsnio klaidos tikimybės reikšmei). Kaip buvo minėta, kuo šios tikimybės reikšmė yra mažesnė (sistema „budresnė“), tuo didesnė atpažinimo pirmojo laipsnio klaidos tikimybė. Priklausomai nuo konkrečių uždavinių sistema nustatoma atitinkamam kompromisui tarp šių tikimybių.

Atsparumas klastojimui – kriterijus apibūdina naudojamo biometrinio požymio atsparumo klastojimui (nesankcionuotai prieigai) laipsnį. Pavyzdžiui dvimatę veido atpažinimo sistemą gali būti bandoma „apgauti“ pateikiant jai „savo“, sistemai žinomo, žmogaus fotografiją ar kaukę. Svetimos akies rainelės vaizdą „pavogti“ yra sunkiau nei veido fotografiją, bet jei ši sąlyga yra atlikta, tai sistemą gali būti mėginama „apgauti“ fotografiniu vaizdu, gautu su didele skiriamąja geba ar užneštu ant kontaktinės linzės. Įvairūs klastojimo būdai, norint įvykdyti nesankcionuotą prieigą, gali pasitaikyti atpažinimo pagal piršto atspaudą sistemose ir priklauso nuo naudojamo skenerio tipo ir sistemos paskirties.

Šiuo metu labiausiai atsparios klastojimui yra sistemos, kurios atpažinimui naudoja trimačio veido vaizdo technologijas. Norint „apgauti“ tokią sistemą reikėtų padaryti veido kaukę, kuri ypatingai tiksliai atkartotų visų veido detalių geometriją. Jeigu sistema dirba realiame laike, tai ji gana lengvai gali fiksuoti ir veido mikrojudesius, kuriuos imituoti pagamintos kaukės pagalba yra sunkiai įgyvendinamas uždavinys.

Socialinis priimtinumas – kriterijus apibūdina visuomenės pritarimo rinkti ir panaudoti biometrinių požymių duomenis laipsnį. Dėl įvairių priežasčių atitinkamų biometrinių požymių duomenų rinkimas, saugojimas ir panaudojimas gali būti visuomenei nepriimtinas. Pavyzdžiui, pirštų atspaudai tradiciškai asocijuojasi su nusikaltimo tyrimu. Kai kuriems asmenims svarbu ir tai, kad tapatybės nustatymas pagal piršto atspaudą yra kontaktinis būdas, kurio esmė yra skeneris, liečiamas ir naudojamas kitų asmenų. Tapatybės nustatymas pagal akies rainelę gali būti susietas su iridodiagnostikos panaudojimu, o tuo pačiu ir galimybe gauti privačią informaciją apie asmens sveikatos būklę.

Tapatybės nustatymas pagal dvimatį veido vaizdą (fotografiją) yra labiausiai priimtinas visuomenei, nes tai bekontaktinis ir tradiciškas būdas. Trimatis skaitmeninis veido vaizdas (fotografija) šiuo požiūriu nesiskiria nuo įprasto, tačiau ženkliai padidina automatinio atpažinimo tikslumą.

Apskaičiuojant biometrinės atpažinimo sistemos efektyvumą pagal (1) ir (2), reikia pereiti prie atskirų kriterijų įvertinimo balais. Šiuo tikslu gali būti naudojama intervalinė, graduojama balais, skalė. Toliau tarp kokybinės ir kiekybinės skalių nustatomas atitinkamas tapatumas. Svorio koeficientų K_j, ($j=\overline{1,n}$), vertės surandamos panaudojant ekspertų apklausos rezultatus [6]. Reikia pažymėti, kad efektyvumas, apskaičiuotas pagal (1) ir (2), pasiekiamas tuo atveju, kai biometrinė sistema naudojama pagal paskirtį ir yra darbinga [7].

IŠVADOS

1. Elektroninės valdžios koncepcijoje numatyta, kad „…E. valdžios projektai galės funkcionuoti, kai bus užtikrinta informacinių technologijų ir telekomunikacijų sauga, gyventojų interesų teisinė apsauga valstybės informacinėse sistemose…“. Planuojama, kad „…bus sukurta gyventojų tapatybės nustatymo informacinėse sistemose sistema…“.
2. Fakultete, nagrinėjant informatikos profilio dalykus, studentai susipažista su biometrinėmis asmens tapatybės nustatymo sistemomis, jų panaudojimo efektyvumu.
3. Atliekant biometrinių sistemų efektyvumo kiekybinę analizę, siūloma įvertinti kaip bendrus, taip ir papildomus kriterijus (reikalavimus).
4. Parodyta, kad prieš įdiegiant biometrinę sistemą reikia atsižvelgti į šiuos pagrindinius veiksnius:

- biometrinės sistemos patikimumą;
- įvedamų biometrinių duomenų suderinamumą su ES reikalavimais;
- biometrinės sistemos standartizacijos lygį;
- įdiegiamos sistemos kainą ir jos atsipirkimo laiką;
- galimybę įdiegiamą sistemą integruoti į jau veikiančias.

LITERATŪRA

1. Elektroninės valdžios koncepcija, patvirtinta Lietuvos respublikos vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2115 „Dėl elektroninės valdžios koncepcijos patvirtinimo“// Valstybės žinios, 2003, Nr. 54.
2. Stupak V., Vasiliauskas R. Autentifikavimo procedūrų nagrinėjimo informatikos ir informacinių technologijų studijose aspektai// Teoriniai ir praktiniai statutinių pareigūnų

rengimo aspektai. Respublikinės mokslinės konferencijos straipsnių rinkinys. ISBN 9955–9777–0–1. –Kaunas: MRU KPF, 2005. – P. 101 – 110.

3. The Biometric Consortium <http://www. biometrics.org>.
4. International Biometric Group <http://www. biometricgroup.com>.
5. Bolle R., Connell J., Pankanti S., Ratha N., Senior A. Guide to Biometrics. New York: Springer – Verlag, 2004.
6. Добров Г.М., Ершов Ю.В., Левин Е.И., Смирнов Л.П. Экспертные оценки в научно-техническом прогнозировании. Киев: Наукова думка, 1974. – 263 с.
7. Stupak V. Pataisomųjų elektroninių įtaisų naudojimo efektyvumo vertinimas// Elektronika ir elektrotechnika. – Kaunas: Technologija, ISSN 1392 – 1215, 2001. – Nr.6(35) – P. 73 - 76.

THE ASPECTS OF ANALYSIS OF EFFICIENCY OF BIOMETRIC RECOGNITION SYSTEMS OF THE TEACHING OF COMPUTER SCIENCE

Viktoras Stupak[*]
Raimondas Vasiliauskas[**]
Mykolas Romeris University

S u m m a r y

For the program of preparation of bachelors for a specialty of the right and protection of frontier, subjects of computer science are taught during the first and third years. For the program of preparation of bachelors for a specialty of the right and activity of police – during the first year. For non – university training under the program activity of police – during the first and second years. In programs of subjects during studying the means of safety for both information technologies, and other objects, the consideration of biometrics systems is stipulated. At studying biometrics systems of recognition, analysis of efficiency of the given systems is stipulated.

Features of studying biometrics systems of recognition at studying computer science are considered. Procedure of a choice of a rational variant of biometrics system is analyzed. The factors influencing the given choice are considered: the purposes of the use of the system, the size of a stream of users, the cost of system, etc. The method of rating of efficiency of biometrics system is offered.

[*] Mykolas Romeris university Kaunas Faculty assoc. prof. dr. of Police Activity Department
[**] Mykolas Romeris university Kaunas Faculty assoc. prof. dr. of Police Activity Department