

ბიომეტრია: მითები და რეალობა

განვითარებული ქვეყნების მიერ დეკლარირებული დოქტრინა „ცოდნაზე დამყარებული ეკონომიკა“ კიდევ უფრო ზრდის ინფორმაციის როლს და, შესაბამისად, მისი დაცვის მნიშვნელობას როგორც ვირტუალური, ასევე ფიზიკური თვალსაზრისით. ამასთან დაკავშირებით კიდევ უფრო მწვავედ დგება უზარმაზარი რაოდენობის პროცესების ინფორმაციის მომხმარებლის – პიროვნების იდენტიფიცირების საკითხი, რაც საჭიროა: აღჭურვილობასთან დაშვებისათვის, იარაღთან დაშვებისათვის, სოციალური დახმარებების გაცემისა და განაწილებისათვის, პენსიის მისაღებად და ა.შ. ამდენად, არაა გასაკვირი ბიომეტრიული ტექნოლოგიების მიმართ ბოლო წლებში გამოჩენილი ინტერესი. ეს ტექნოლოგიები მეტად მიმზიდველი იქნა ნებისმიერი სახის დაშვების განხორციელებისათვის, რამდენადაც უზრუნველყოფენ იდენტიფიცირების მაღალ საიმედოობას, თანაც შეიძლება ინტეგრირებულნი იქნან დაშვების კონტროლის ნებისმიერ სისტემაში სხვადასხვა გასაღებებთან და პაროლებთან ერთად.

ბიომეტრია ტრადიციულად განისაზღვრება, როგორც მეცნიერების დარგი, რომელიც შეისწავლის ადამიანის ბიოლოგიური მახასიათებლების მათემატიკური და სტატისტიკური დამუშავების მეთოდებს. დღეისათვის, ტერმინმა „ბიომეტრია“ დატვირთვა შეიცვალა და აღიქმება როგორც ადამიანის იდენტიფიცირების ტექნოლოგია, რომელიც იყენებს ბიოლოგიურ მახასიათებლებს.

ბიომეტრიას, კერძოდ კი დაქტილოსკოპიას, ადამიანები უხსოვარი დროიდან იყენებდნენ. მაგრამ დამოუკიდებელ მეცნიერებად ჩამოყალიბდა მე-19 საუკუნეში, მე-20 საუკუნეში ბიომეტრიული სისტემები ძირითადად გამოიყენებოდა სამხედრო და მნიშვნელოვანი კომერციული ინფორმაციის დასაცავად. აშშ-ში 2001 წლის ტერორისტული აქტის შემდეგ კი სიტუაცია მნიშვნელოვნად შეიცვალა. დიდ პრობლემად იქცა პიროვნების იდენტიფიცირების საკითხი, ბიომეტრიის გამოყენება დაიწყო უსაფრთხოების სფეროში ახალი ტექნოლოგიების დანერგვისას. აქედან იწყება ბიომეტრიის აღმასვლა და ტერმინ „ბიომეტრიის“ შინაარსის ცვლილებაც ამასთან არის დაკავშირებული.

ადამიანის ბიომეტრიული იდენტიფიცირების მეთოდები

პიროვნების იდენტიფიცირების მეთოდები ბიომეტრიული პარამეტრების გამოყენების მიხედვით იყოფა ორ ჯგუფად: სტატიური (ადამიანის ფიზიკური მახასიათებლები) და დინამიური (ადამიანის ქცევითი მახასიათებლები).

სტატიური მეთოდები ეყრდნობა ადამიანის არაცვალებად ფიზიოლოგიურ მახასიათებლებს, როგორცაა: თითის ანაბეჭდი; სახის ფორმა და გეომეტრია; თავის ქალის ფორმა და გეომეტრია; თვალის გუგა; ხელისგულის, მტევნის ან თითის გეომეტრია; სახის თერმოგრაფია, ხელის თერმოგრაფია; ხელისგულზე ან თითზე ვენების გამოსახულების სურათი; დნმ; ორგანიზმის სუნი; ყურის ფორმა და სხვ.

დინამიური მეთოდები ეყრდნობა პიროვნების ქმედებების ანალიზს, ანუ თავისებურებებს, რომელიც ახასიათებს ადამიანს რაიმე მოქმედების დროს. დინამიური მეთოდები დღეისათვის მნიშვნელოვნად ჩამორჩებიან სტატიურ მეთოდებს სიზუსტეში და ეფექტურობაში, მაგრამ მაინც ხდება მათი გამოყენება. ამ მეთოდებს განეკუთვნება: ხელმოწერის დინამიკა; კლავიატურაზე მუშაობის დინამიკა; ხმა; ტუჩების მოძრაობა; სიარულის მანერა; ხელნაწერი ტექსტის თავისებურებები.

კონკრეტული ბიომეტრიული ტექნოლოგიის შესაქმნელად ადამიანის ბიომეტრიული მახასიათებლის შერჩევა ძირითად ამოცანას წარმოადგენს. ადამიანის იდეალური ბიომეტრიული მახასიათებელი უნდა იყოს უნივერსალური, უნიკალური, სტაბილური და აღქმადი. ბიომეტრიული მახასიათებლის უნივერსალურობა ნიშნავს, რომ ეს ბიომეტრიული მახასიათებელი უნდა ქონდეს ყველა ადამიანს. უნიკალურობა ნიშნავს, რომ არ შეიძლება არსებობდეს ორი ადამიანი, რომლებსაც ეს მახასიათებელი ექნებათ ერთნაირი. სტაბილურობა გვჩვენებს, რომ არ უნდა იცვლებოდეს ბიომეტრიული მახასიათებელი დროის განმავლობაში. ამასთან ადამიანის ბიომეტრიული მახასიათებლის აღქმა ტექნიკური საშუალებებით უნდა იყოს შესაძლებელი და მოსახერხებელი.

ადამიანის რეალური ბიომეტრიული მახასიათებლები არ არის იდეალური. სხვადასხვა ბიო-

მეტრიული მახასიათებლისათვის უნივერსალობის, უნიკალობის, სტაბილურობის და აღქმადობის კრიტერიუმების მიხედვით სამბალიანი ექს-

პერტული შეფასებით მიღებულია ცხრ. 1-ში მოტანილი შედეგები [1].

ცხრილი 1

ადამიანის ბიოლოგიური მახასიათებელი	უნივერსალობა	უნიკალობა	სტაბილურობა	აღქმადობა
სახის გამოსახულება	მაღალი	დაბალი	საშუალო	მაღალი
სახის თერმოგრამა	მაღალი	მაღალი	დაბალი	საშუალო
თითის ანაბეჭდი	მაღალი	მაღალი	მაღალი	საშუალო
ხელის მტევანი	საშუალო	საშუალო	საშუალო	მაღალი
თვალის ფერადი გარსი	საშუალო	მაღალი	მაღალი	საშუალო
თვალის ბადურა	მაღალი	მაღალი	საშუალო	დაბალი
ხელმოწერა	დაბალი	დაბალი	დაბალი	მაღალი
ხმა	საშუალო	დაბალი	დაბალი	საშუალო
ტუჩები	მაღალი	მაღალი	საშუალო	დაბალი
ყური	საშუალო	საშუალო	საშუალო	საშუალო
წერის დინამიკა	საშუალო	მაღალი	დაბალი	მაღალი
სიარულის მანერა	მაღალი	საშუალო	დაბალი	დაბალი

როგორც ცხრილიდან ჩანს, ვერცერთი ბიომეტრიული მახასიათებელი აკმაყოფილებს მაქსიმალურად მოთხოვნებს ჩამოთვლილი თვისებების მიხედვით. მიუხედავად მატერიალური დანახარჯების და სიზუსტის საშუალო მაჩვენებლებისა, დღეისათვის, გაყიდვებით ლიდერის პოზიცია უჭირავს ბიომეტრიულ ტექნოლოგიებს თითის ანაბეჭდის საფუძველზე, რაც გარკვეულწილად განპირობებულია მეთოდური, ტექნიკური და ალგორითმული ტრადიციულობით და კარგი საექსპლუატაციო მახასიათებლებით.

ბიომეტრიის განვითარების დღევანდელი დონე

დაქტილოსკოპიის ცოდნის პირველი ნიშნები ჩანს ჯერ კიდევ ჩვენს წელთაღრიცხვამდე. ჩრდილოეთ ამერიკაში ნაპოვნია ქვაზე ადამიანის ხელის გამოსახულება, რომელზეც ჩანს პაპილარული ხაზები. ასირიელები, ჩინელები დოკუმენტების დასამოწმებლად იყენებდნენ თიხის ბეჭდებს თითის ანაბეჭდით, ძველ ჩინეთში თითის ანაბეჭდებზე დაკვირვებით ხდებოდა ადამიანის ბედის განსაზღვრა, შემდგომ დაიწყო გამოყენება კრიმინალისტიკაში.

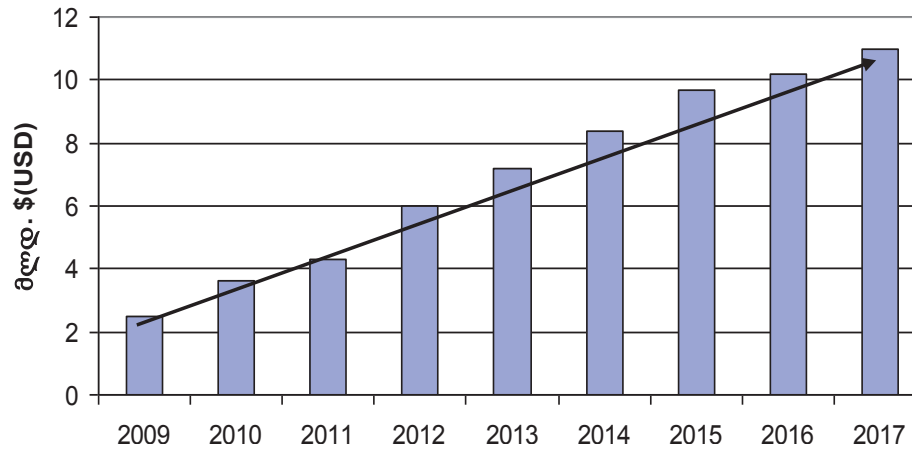
ევროპაში თითის ანაბეჭდით ადამიანის იდენტიფიცირებას ყურადღება მე-19 საუკუნეში მიაქცევს. დაქტილოსკოპიის თანამედროვე ისტორიის პირველ მკვლევარებად ითვლებიან უილამ გერშე-

ლი და ჰენრი ფოლდსი. გერშელი ინდოეთში მუშაობის პერიოდში თითის ანაბეჭდებს იყენებდა ადგილობრივი მოსახლეობისთვის დახმარებების აღრიცხვის დროს, შემდეგ კი ციხეში პატიმრების იდენტიფიცირებისთვის. ფოლდსმა დაქტილოსკოპიის შესწავლა დაიწყო გერშელისგან დამოუკიდებლად იმავე წლებში (1870 წ.), შექმნა თითის ანაბეჭდების კლასიფიცირების სისტემა და პირველმა მოახდინა იდენტიფიცირება მინის ბოთლზე ანაბეჭდით. ამ ორი მეცნიერის იდეებზე და გამოცდილებაზე დაყრდნობით გალტონმა შექმნა თითის ანაბეჭდის ინდივიდუალობისა და მუდმივობის თეორია, მან ასევე დაამტკიცა, რომ ერთი-დაიგივე ადამიანს ათივე თითზე აქვს განსხვავებული ანაბეჭდი, შექმნა პაპილარული ხაზების, კლასიფიცირების სისტემა, ე.წ. „გალტონის დეტალები“ [2].

ბიომეტრიის თავბრუდამხვევი განვითარება დაიწყო 2001 წლის 11 სექტემბრის ტერაქტის შემდგომ, როცა ყველა მიხვდა, რომ ტერორიზმისაგან თავის დაღწევა მოითხოვდა პიროვნების გარანტირებულ იდენტიფიცირებას. იმ მომენტისათვის ბიომეტრიული აღჭურვილობის დამუშავებაში ჩაებნენ ისეთი ცნობილი კომპანიები, როგორიცაა: LG, Sanyo, Polaroid, NEC, Panasonic და სხვა. შეიძლება ითქვას, რომ ბიომეტრია დღეისათვის შეიჭრა ადამიანის მოღვაწეობის ყველა სფეროში, სადაც კი საჭიროა მისი იდენტიფიცირება.

ნახ.2-ზე მოცემულია Acuity Market Intelligence-ის მიერ 2011 წელს შედგენილი ბიომეტ-

რიული საშუალებების წარმოებისაგან მიღებული შემოსავლების პროგნოზი [3].

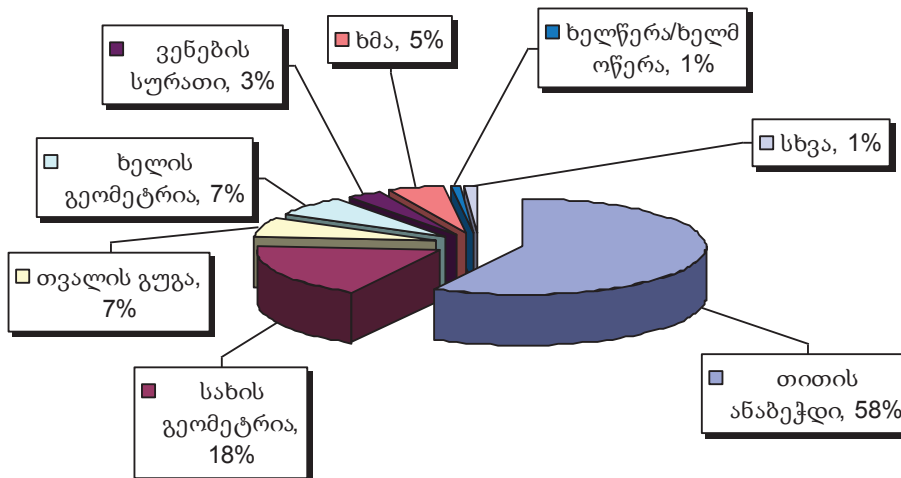


ნახ. 1. ბიომეტრიული ინდუსტრიის პროგნოზი

როგორც დიაგრამიდან ჩანს, ბიომეტრიული საშუალებების გაყიდვებისაგან მიღებული შემოსავლები ყოველწლიურად დინამიურად იზრდება და 2017 წელს მიაღწევს 11 მილიარ აშშ დოლარს.

დღეისათვის, ბიომეტრიულ სისტემებში გამოიყენება პრაქტიკულად ყველა ზემოთ ჩამოთვლი-

ლი ბიომეტრიული მახასიათებელი. ბიომეტრიული ბაზრის სეგმენტაციას გამოყენებული იდენტიფიკატორების მიხედვით კომპანია Acuity Market Intelligence-ის 2007 წლის მონაცემებით აქვს შემდეგი სახე:



ნახ.2. ბიომეტრიული ბაზრის გადანაწილება ბიომეტრიული მახასიათებლების მიხედვით

როგორც ვხედავთ, არსებული სტატიური და დინამიური ბიომეტრიული მეთოდებიდან დღეისათვის უფრო მეტად გამოიყენება თითის ანაბეჭდის ანალიზი, რაც განპირობებულია შემდეგი ფაქტორებით: თითის ანაბეჭდის იდენტიფიკატორი პიროვნების იდენტიფიცირებას, სხვა იდენტიფიკატორებთან შედარებით, ახდენს მეტი საი-

მედობით; თითის ანაბეჭდის ანალიზი ბევრად სწრაფად ხდება; თითის ანაბეჭდით იდენტიფიცირების საშუალებები (პროგრამული და აპარატურული) ბევრად უფრო იაფია, რაც მნიშვნელოვნად უწყობს ხელს თითის ანაბეჭდის ანალიზის მეთოდების ფართო გავრცელებას; თითის ანაბეჭდით პიროვნების იდენტიფიცირების მეთოდები,

მათემატიკური მოდელები და ალგორითმები ბევრად კარგადაა დღეისათვის დამუშავებული, რაც განპირობებულია თითის ანაბეჭდის გამოყენების ტრადიციულობით.

ბიომეტრიული ტექნოლოგიების სრულყოფა ხდება დაჩქარებული ტემპებით, პირველ რიგში საიმედოობის ამაღლების და ღირებულების შემცირების კუთხით ისეთი ტრადიციული ტექნოლოგიებისათვის, როგორცაა: თითის ანაბეჭდის, სახის და თვალის ფერადი გარსის იდენტიფიკატორებისათვის.

ძველ ტექნოლოგიებთან ერთად წარმოიშვა ახალიც. მათგან ზოგიერთს, განსაკუთრებით კი სახის სამგანზომილებიანი გამოსახულებით სუბიექტის გამოცნობას, აქვთ მნიშვნელოვანი პოტენციალი და მომავალში შეუძლიათ სერიოზულად შეცვალონ ბიომეტრიული ბაზრის გადანაწილების სურათი.

და, რაც მთავარია, ბიომეტრიის სფეროში ძირითადი მოვლენა იქნება მოცემული ტექნოლოგიების მასიური დანერგვა და გამოყენება საპასპორტო-სავიზო დოკუმენტებში (დღეისათვის ეს პროცესი რიგ ქვეყნებში სერიოზულადაა დაძვრული). ეს მოვლენა მიგვიყვანს არა მხოლოდ ტექნოლოგიურ ცვლილებებთან და ბაზარზე არსებული სისტემების და მოწყობილობების განვითარებასთან, არამედ მთლიანად შეცვლის ადამიანების ყოფას. იმედი უნდა ვიქონიოთ, რომ ეს იქნება ვექტორი კარგისაკენ, რამდენადაც ბიომეტრია საშუალებას იძლევა ამაღლებული იქნას არა მხოლოდ ცალკეული ადამიანის უსაფრთხოება, არამედ საზოგადოების – მთლიანად.

ბიომეტრიის გამოყენების სფეროები

პასუხი კითხვაზე: სად გამოიყენება ბიომეტრია და როგორია მისი გამოყენების არეალის გაზრდის პერსპექტივა, შეიძლება იყოს ძალიან მოკლე: ყველგან და ყველგან, სადაც არის საჭირო ადამიანის იდენტიფიცირება, აუტენტიფიცირება და ა.შ. ბიომეტრიული იდენტიფიცირების გამოყენების სფერო შეიძლება „მოულოდნელიც“ იყოს, ანუ იქ სადაც ადრე საერთოდ არ ხდებოდა ადამიანის იდენტიფიცირება. მაგალითის სახით შეიძლება მოვიყვანოთ მოსწავლის იდენტიფიცირება სკოლის ბუფეტში და ა.შ. შეიძლება ითქვას, რომ ბიომეტრიული იდენტიფიცირება „აფართოებს“ ადამიანის იდენტიფიცირების სფეროების არეალს.

ნათელია, რომ ბიომეტრიული სისტემების გამოყენების არეალი მეტად ფართოა, ამიტომ მოვიტანთ გამოყენების სფეროების მხოლოდ ჩამონათვალს: ფიზიკური დაშვების ბიომეტრიული მართვა (მაგალითად, დაშვება დაცულ ტერიტორიებზე); ლოგიკური დაშვების ბიომეტრიული

მართვა (მაგალითად, აუტენტიფიცირება მონაცემთა ბაზებში); სამართალდამცავი და იუსტიციის სფერო (კრიმინალისტიკა და პენიტენციური სისტემა); სამუშაო დროის აღრიცხვა (სჭირდება ყველა კომპანიას); სამედიცინო სფერო (განსაკუთრებით საჭიროა ჯანმრთელობის დაზღვევის სისტემებში); სასაზღვრო კონტროლი (სავიზო, საპასპორტო კონტროლი); ფინანსური და ტრანზაქციული ბიომეტრია (იდენტიფიცირების საიმედოობის ამაღლება განსაკუთრებით მნიშვნელოვანია საბანკო სექტორში); მობილური მოწყობილობები (მაგალითად, მობილური ბანკისათვის პიროვნების იდენტიფიცირება); ბიომეტრიული საკეტები (დღეისათვის უკვე ფართოდაა გავრცელებული, თუნდაც სასტუმროებში); სამომხმარებლო ბიომეტრია (მაგალითად, ხელჩანთებში, სეიფებში); სასწავლო დაწესებულებები; ბიომეტრიის გამოყენების სხვა სფეროები – მოხერხებულობა (მაგალითისათვის მოვიყვანთ სხვადასხვა თითის გამოყენებას სხვადასხვა პროგრამების გამოძახებისათვის).



ნახ.3. პედაგოგთა რეგისტრაციის სისტემის ტერმინალი

უფრო დაწვრილებით შევჩერდეთ ბიომეტრიის გამოყენების მნიშვნელობაზე სასწავლო დაწესებულებებში. განვითარებულ ქვეყნებში დაწყებულია ფართომასშტაბიანი პროექტები სკოლებში მოსწავლეთა ბიომეტრიული იდენტიფიცირებისათვის, სადაც შერწყმულია მოსწავლეთა აღრიცხვის და უსაფრთხოების ფუნქციები. ასევე ფართოდ გამოიყენება ბიომეტრიული იდენტიფიცირება სკოლის ბუფეტებში უსაფრთხოების მიზნით და შესაბამისად მოსწავლეებს აღარ აქვთ უშუალოდ ფულთან შეხების აუცილებლობა. მატერიალური დანახარჯების შემცირების მიზნით, ბიომეტრიული იდენტიფიცირებას იყენებენ საუნივერსიტეტო კამ-

პუსებში უცხო პიროვნების დაშვების აკრძალვის მიზნით. ამდენად უცხო პიროვნებას არ შეუძლია უფასოდ ისარგებლოს იმ სერვისებით, რაც გათვალისწინებულია სტუდენტებისათვის, მაგალითად, ბიბლიოთეკით. რამდენიმე წელია განვითარებად ქვეყნებში დაიწვეს ბიომეტრიული იდენტიფიცირების გამოყენება პედაგოგებისათვის. მაგალითად, ინდოეთში აღმოჩნდა, რომ თურმე ყველა პედაგოგი არ ასრულებს კეთილსინდისიერად მასზე დაკისრებულ მოვალეობას. ამ მხრივ ორიგინალურია პედაგოგთა რეგისტრაციის ბიომეტრიული სისტემა, რომელიც გამოიყენება საქართველოს ტექნიკურ უნივერსიტეტში (ნახ.3). უსაფრთხოების თვალსაზრისით ძალიან ეფექტური აღმოჩნდა ბიომეტრიული იდენტიფიცირების სისტემა საბავშვო ბაღებში, სადაც ბავშვის მოყვანა ბაღში, ან გაყვანა შესაძლებელია მშობლის ან მეურვის ბიომეტრიული იდენტიფიცირების შემდგომ.

როგორ მუშაობენ ბიომეტრიული ტექნოლოგიები

ბიომეტრია მოწოდებულია გადაჭრას ვერიფიცირების და იდენტიფიცირების საკითხები. თავდაპირველად ხდება კონკრეტული პირის ბიომეტრიული მახასიათებლის მათემატიკური მოდელის ანუ საწყისი შაბლონის ჩამოყალიბება. ზოგჯერ ამ პროცესს პიროვნების რეგისტრირებას უწოდებენ. ვერიფიცირების დროს ამოცანა მდგომარეობს იმაში, რომ დავრწმუნდეთ მოცემულ მომენტში მიღებული მათემატიკური მოდელი (ბიომეტრიული „რუკა“) შეესაბამება თუ არა ამ პირის რეგისტრირებულ შაბლონს. ვერიფიცირება (ანუ შედარება ერთი – ერთთან) გამოიყენება იმის შესამოწმებლად, არის თუ არა ეს სუბიექტი ის, რომლიდანაც თავს წარმოაჩენს. გადაწყვეტილება მიიღება ახლად ფორმირებული და რეგისტრირებული შაბლონების მსგავსების საფუძველზე. ბიომეტრიისათვის უპრიანია ვილაპარაკოთ შაბლონების მსგავსების დონეზე.

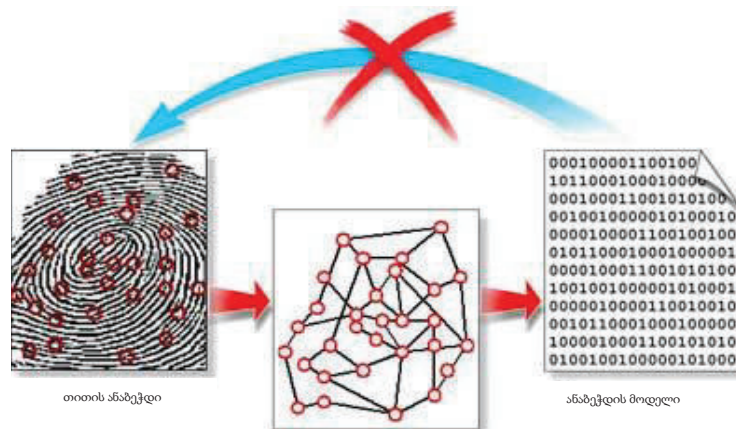
იდენტიფიცირება (ანუ შედარება ერთისა N-თან) წყვეტს ახლად მიღებული ბიომეტრიული შაბლონის ყველაზე უფრო მსგავსის მოძებნის ამოცანას რეგისტრირებული N შაბლონიდან. უმარტივეს შემთხვევაში ეს არის ახლად მიღებული შაბლონის თანმიმდევრული შედარება N შაბლონიდან ყველასთან. გადაწყვეტილება მიიღება იმ რეგისტრირებული შაბლონის სასარგებლოდ, რომელსაც ექნება ყველაზე მეტი მსგავსების დონე ახლად ფორმირებულ შაბლონთან, ანდა საერთოდ არ ექნება მიღებული დადებითი გადაწყვეტილება,

თუ თანმიმდევრულმა შედარებამ არ მოგვცა მსგავსების წინასწარ განსაზღვრული დონე [4].

თითის ანაბეჭდის გამოცნობის შემთხვევაში რეგისტრირებული და მიმდინარე შაბლონები მიიღება დაქტილოსკოპიური სკანერის საშუალებით, რომელიც გვამღვს თითის პაპილარული ხაზების გამოსახულებას. შემდგომ ხდება ამ გამოსახულების დამუშავება და დამუშავების პროცესში ხდება მისი ისეთი მახასიათებელი თავისებურებების, როგორიცაა ხაზების განშტოება, ხაზების დაბოლოება ანდა ხაზების გადაკვეთის გამოყოფა. ყოველი მახასიათებელი თავისებურებისათვის ხდება მისი ტიპის, კოორდინატის, ფარდობითი განლაგების და ისეთი სხვა პარამეტრების დამახსოვრება, როგორიცაა, მაგალითად, ხაზების დაბოლოების წერტილისათვის – ხაზის მიმართულება. მახასიათებელი თავისებურებების მონაცემთა ერთობლიობა წარმოქმნის ბიომეტრიული მახასიათებლის შაბლონს. მათემატიკური მოდელის სახით მიიღება მრავალპარამეტრიანი ვექტორი. ნახ. 4-დან ჩანს, რომ განხილული პროცესი უკუქცევადი არაა, ანუ თითის ანაბეჭდის მათემატიკური მოდელიდან თითის ანაბეჭდის გამოსახულების აღდგენა ვერ მოხდება.

ბიომეტრიის საიმედოობა

ბიომეტრიული სისტემების მთავარი დანიშნულებაა პიროვნების იდენტიფიცირება, ანუ იდენტიფიკატორის შესაბამისობის დადგენა მის წარმოდგენთან, თუნდაც აუტენფიცირებისას. თუ ამ კუთხით მივუდგებით სისტემაში აუტენტიფიცირების ტრადიციულ (თუნდაც პაროლით, ან პლასტიკური ბარათით) მეთოდებთან შედარებით, შეფასების გარეშეც ცხადია, რომ ბიომეტრიული აუტენტიფიცირება გაცილებით საიმედოა, რამდენადაც შესაძლებელია პაროლის (ბარათის) დაკარგვა, დავიწყება და ა.შ. არაფერს ვამბობთ მრავალი პაროლით სარგებლობისას წამოჭრილ შეცდომებზე და ა.შ. ამდენად, განხილვის საგანს წარმოადგენს უშუალოდ ბიომეტრიული სისტემის საიმედოობა. ამდენად, ბიომეტრიული სისტემის საიმედოობაში იგულისხმება ზოგადად ტექნიკური სისტემის საიმედოობა, რომელმაც სწორად უნდა შეასრულოს მასზე დაკისრებული მოვალეობა. აუტენტიფიცირების ბიომეტრიული სისტემისათვის ეს გულისხმობს: სისტემამ არ უნდა დაუშვას „უცხო“ და დაუშვას „ნაცნობი“ მომხმარებელი. შესაბამისად უარი არ უნდა უთხრას დაშვებაზე „ნაცნობ“ მომხმარებელს.



ნახ.4. ბიომეტრიული სისტემის მოქმედების პრინციპი

მიუხედავად იმისა, რომ მეცნიერების მიერ დიდი ხანია დამტკიცებულია ადამიანის ბიომეტრიული მახასიათებლების მუდმივობა, პრაქტიკული გამოყენებისას გერჩება შთაბეჭდილება, რომ რიგ შემთხვევებში ასეთი შეფასება გადაჭარბებულია. რადგან „რეალურ ცხოვრებაში“ ბიომეტრიული სისტემა ხშირად „ვერ ცნობს“ დარეგისტრირებულ მომხმარებელს. ამ შემთხვევაში საკმარისია, რომ ხელმეორედ დავარეგისტრიროთ მომხმარებელი, ანუ განვაახლოთ ბიომეტრიული მახასიათებლის შაბლონი, რომ ხარვეზი მყისვე გამოსწორდეს. ეს უფრო ეხება დაქტილოსკოპიაზე აგებულ ბიომეტრიულ სისტემას. ამდენად, რჩება შთაბეჭდილება, რომ ადამიანის ბიომეტრიული მახასიათებელი თითქოს იცვლება. ამ „ჩახლართულ“ სიტუაციაში გარკვევის მიზნით, ჯერ ვნახოთ თუ რა შეცდომებს უშვებს ბიომეტრიული სისტემა.

ბიომეტრიული სისტემის შეცდომებიდან გამოყოფენ სამი ტიპის შეცდომას [5]:

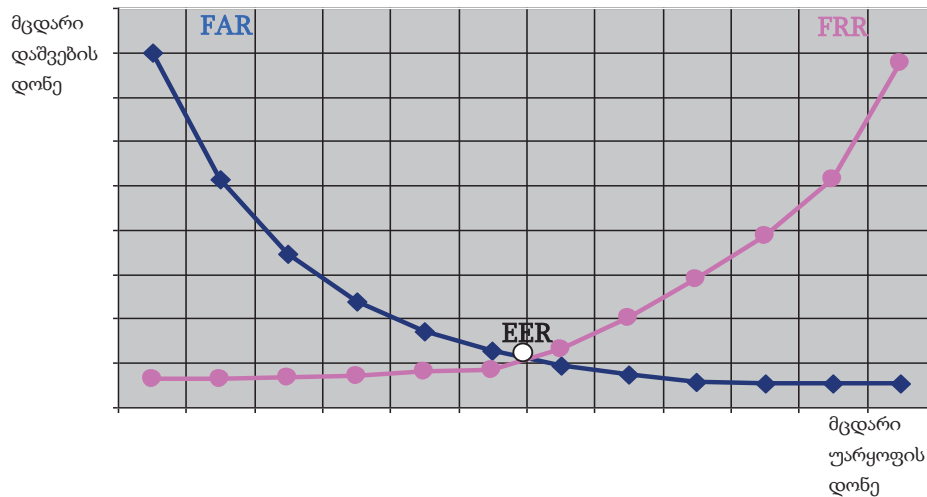
პირველი რიგის შეცდომა (FRR – False Rejection Rate) – მცდარი უარყოფის დონე. „ვერ ცნობს თავისიანს“, ე.ი. მიიღება გადაწყვეტილება, რომ „სხვა“, მიუხედავად იმისა, რომ სუბიექტი არის დარეგისტრირებულია მონაცემთა ბაზაში.

მეორე რიგის შეცდომა (FAR – False Acceptance Rate) – მცდარი დაშვების დონე. „დაშვებული იქნას უცხო“, ე.ი. მიიღება გადაწყვეტილება, რომ „თავისიანია“, მიუხედავად იმისა, რომ სუბიექტი არ არის დარეგისტრირებულია მონაცემთა ბაზაში.

მესამე რიგის შეცდომა (FER-Failure to Enroll Rate) – რეგისტრაციის შეუძლებლობის დონე. მიიღება გადაწყვეტილება, რომ „უცხოა“ იმის გამო,

რომ ვერ ხერხდება დაქტილოსკოპიური სკანერით პაპილარული ხაზების სურათის მიღება და, შესაბამისად, ვერ ახერხებს ბიომეტრიული მახასიათებლის აღქმას. მაგალითად, დაქტილოსკოპიურ სკანერს არ შეუძლია თითის ანაბეჭდის გამოსახულების მიღება კანის ხარვეზების, განსაკუთრებული წერტილების მცირე რაოდენობის ანდა პაპილარული ხაზების არ არსებობის გამო. თითის ანაბეჭდის გამოსახულებაზე განსაკუთრებული წერტილების რაოდენობის შემცირება შეიძლება გამოწვეული იყოს კანის მექანიკური დაზიანებებით. მესამე დონის შეცდომასთან გვაქვს საქმე, როცა მომხმარებლის რეგისტრაცია სისტემაში ხდება ერთი ტიპის დაქტილოსკოპიური სკანერით და აუტენტიფიკაციას გადის მეორე ტიპის დაქტილოსკოპიური სკანერით.

შემდგომი განხილვის გამარტივების მიზნით, დავუშვათ, რომ ბიომეტრიული სისტემის შეფასება ხდება მეორე რიგის შეცდომაზე (FAR) დაყრდნობით. თუ გავზრდით სისტემაში FAR-ის დონეს (როგორც წესი, ბიომეტრიულ სისტემაში FAR ექვემდებარება ადმინისტრირებას), მაშინ სისტემაში უპრობლემოდ იქნებიან დაშვებული დარეგისტრირებული მომხმარებლები, მაგრამ გაიზრდება საფრთხე „რომ დაშვებული იქნას უცხო“. თუ მოვახდენთ FAR-ის შემცირებას, მაშინ „უცხოს“ დაშვების საფრთხის ალბათობა შემცირდება, მაგრამ იმავდროულად შეიძლება მივიღოთ სიტუაცია: „ვერ ცნობს თავისიანს“ (ნახ. 5). შესაბამისად, მკვეთრად შემცირდება სისტემის მოხმარებელთა კომფორტულობა. მათ მოუწევთ დაქტილოსკოპიურ სკანერზე თითის რამოდენიმეჯერ დადება, ან კიდევ უფრო უარესი, საქმე გვექნება მესამე დონის შეცდომასთან.



ნახ. 5. პირველი და მეორე რიგის შეცდომების ურთიერთდამოკიდებულება

ამ ლოგიკიდან გამომდინარე, შეიძლება ვივარაუდოთ, სისტემა საუკეთესოდ იმუშავებს FAR-ის იმ მნიშვნელობაზე, როცა გვაქვს პირველი და მეორე რიგის შეცდომების ერთნაირი დონე (EER). მაგრამ, რეალურ სისტემაში ასეთი მიდგომა არ ამართლებს, ანუ ვერ ვიღებთ საიმედოების იმ დონეს, რომელიც ჩვენთვის მისაღებია.

არსებობს მიდგომა, როცა FAR-ის მნიშვნელობის შერჩევა ხდება სისტემის დანიშნულებიდან გამომდინარე: თუ ბიომეტრიული სისტემა განკუთვნილია მკაცრი დაშვებისათვის, მაშინ $FAR \leq EER$. თუ ამ შემთხვევაში ადგილი ექნება FER-ს, მაშინ სისტემაში გამოყენებული უნდა იქნას უფრო მაღალი ხარისხის აპარატურული და პროგრამული საშუალებანი, ან იდენტიფიცირება მოვახდინოთ სხვა ბიომეტრიული მახასიათებლის საშუალებით.

თუ ბიომეტრიული სისტემა არაა განკუთვნილი მკაცრი დაშვებისათვის, მაშინ შეიძლება, რომ $FAR \geq EER$. შესაბამისად გაიზრდება სისტემით სარგებლობის კომფორტულობაც. $FAR \geq EER$ -ის შემთხვევაში უკვე დიდი მნიშვნელობა ენიჭება FAR-ის დონის ადმინისტრირებას, ანუ FAR-ის დონის სწორ შერჩევას.

დაქტილოსკოპიური იდენტიფიცირების პრობლემები

- „რთული თითების“ პრობლემა. თითის პაპილარული ხაზების სურათის სკანირებისას ადამიანების 1%-ს აქვთ პრობლემები, რაც დაკავშირებულია მექანიკურ დაზიანებებთან, დამწვრობასთან, კანის დაავადებებთან და სხვა. თუ პროცენტის თითიდან საერთოდ შეუძლებელია სურათის მიღება დაქტილოსკოპიური სკანერის საშუალებით, მაშინ უმჯობესია გადავიდეთ თვალის ფერადი გარსის

სკანირებაზე, ან სხვა რომელიმე იდენტიფიკატორზე.

- „იმიტაციის“ პრობლემა. შესაძლებელია თითის პაპილარული სურათის იმიტაცია სხვადასხვა საშუალებებით, მათ შორის სილიკონის მოდელის გამოყენებით. ამ შემთხვევას ებრძვიან სითბური სკანერის გამოყენებით, რომელიც რეაგირებს გამოსახულებაზე და სითბოზე ერთდროულად.
- პიროვნების უფლებათა დარღვევა (Privacy Violation)

ბიომეტრიულ სისტემაში პაპილარული ხაზების უშუალოდ გამოსახულების (ან თუნდაც მცირე ნაწილის) შენახვა.

ადამიანებს, რომლებსაც უხდებათ ბიომეტრიულ სისტემებთან შეხება ან არიან მისი მომხმარებლები, უჩნდებათ „ბუნებრივი“ კითხვა: ინახება თუ არა მისი თითის ანაბეჭდი სისტემაში? დაქტილოსკოპიური ბიომეტრიული სისტემები შეიძლება გაიყოს ორ ჯგუფად: დაქტილოსკოპიური გამოსახულების შენახვით და მის გარეშე. პირველი ტიპის სისტემებით სარგებლობენ მხოლოდ კრიმინალისტიკაში, ხოლო ყველა დანარჩენ შემთხვევაში გამოიყენება დაქტილოსკოპიაზე დაყრდნობილი ბიომეტრიული სისტემები გამოსახულების შენახვის გარეშე.

ნახ.4-ზე წარმოდგენილი სქემა ხსნის დაქტილოსკოპიური ბიომეტრიული სისტემის მოქმედების პრინციპს. თითის ანაბეჭდიდან მიიღება ე.წ. „ანაბეჭდის რუკა“, სადაც უკვე გამოყოფილია საკვანძო (დალტონის) დეტალები. შემდგომი მათემატიკური გარდაქმნებით მიიღება თითის ანაბეჭდის მათემატიკური მოდელი – შაბლონი. აქვე უნდა აღინიშნოს, რომ შაბლონიდან თითის ანაბეჭდის მიღება შეუძლებელია (ყოველ შემთხვევაში, დღეისათვის ასეთი მათემატიკური მეთოდი არ არსებობს).

დასკვნა. გაანალიზებულია და დასაბუთებულია ადამიანის იდენტიფიცირებისათვის ბიომეტრიული მეთოდების საიმედოობა ტრადიციულ მეთოდებთან (პლასტიკური ბარათის, პაროლის და ა.შ. გამოყენებით) შედარებით. ამასთან ნაჩვენებია, რომ ბიომეტრიული მეთოდების გამოყენება ადამიანის იდენტიფიცირებისათვის იძლევა კარგ შედეგებს, მხოლოდ ბიომეტრიული სისტემის სწო-

რად ადმინისტრირების შემთხვევაში. მიუხედავად იმისა, რომ ბიომეტრიული სისტემების გამოყენებასთან დაკავშირებული ხარვეზები ხასიათდება ობიექტური და სუბიექტური მიზეზებით, მისი გამოყენების არეალი და მამტაბები დღითიდღე ფართოვდება და იზრდება, რაც უდავოდ მეტყველებს მის ეფექტურობაზე.

LEVAN IMNAISHVILI
MAGULI BEDINEISHVILI
ALINA TITVINIDZE

BIOMETRICS : MYTHS AND REALITY

Summary

The article describes the essence of biometrics and purpose, the advantages and disadvantages of biometric systems.

It is shown, that now, biometric methods are most effective and reliable way to identification the people. Particular attention is paid to the administration of biometric systems, in order to ensure their reliability. Because of rapid pace of development "Biometric Market" and expanding the area of human identification using biometric methods, the conclusion is made, that in recent years biometrics not only to raise reliability of human identification, but will have a significant impact on human life style.

გამოყენებული ლიტერატურა:

1. Anil K. Jain, Arun Ross, Salil Prabhakar. An Introduction to Biometric Recognition. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.
2. The Fingerprint Sourcebook. Chapter 1. HISTORY, Jeffery G. Barnes, National Institute of Justice, 2011.
3. http://www.acuity-mi.com/FOB_Report.php
4. Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. Handbook of Fingerprint Recognition. Springer-Verlag, New York, Berlin, Heidelberg, 2003.
5. Technical Document about FAR, FRR and EER. by SYRIS Technology Corp., 2004.