NOWE TECHNOLOGIE I ZASTOSOWANIA W BIOMETRII– ANALIZA RYNKU

Anna KIEŁBUS, Karolina FURYK

Streszczenie: Identyfikacja osób jest niezwykle szerokim zagadnieniem wymagającym stosowania osiągnięć nauki i techniki z wielu dziedzin. W artykule przedstawiono różne techniki biometryczne i ich szeroką gamę zastosowań, zwłaszcza w zakresie identyfikacji tożsamości. Zwrócono uwagę na problemy występujące przy identyfikowaniu osoby czy denata oraz trendy panujące w rozwoju technologii biometrycznych.

Słowa kluczowe: identyfikacja osób, biometria, analiza rynku, metody identyfikacji osób

1. Wprowadzenie

Identyfikacja tożsamości jest zagadnieniem wymagającym stosowania osiągnięć nauki i techniki z wielu dziedzin. Interdyscyplinarna współpraca specjalistów może prowadzić do wprowadzenia metod identyfikacji o określonym zakresie stosowania uwarunkowanym stanem materiału badawczego, lokalnymi możliwościami oraz wieloma innymi aspektami wpływającymi na cały proces rozpoznania. Ciągle rosnące zainteresowanie systemami biometrycznymi w ciągu ostatnich 30lat i ich wykorzystanie w wielu dziedzinach sprawia, że wciąż trwają prace nad zmniejszeniem kosztów produkcji oraz zwiększenie poziomu technicznego, aby był wystarczająco satysfakcjonujący.
Autorzy podjęli próbę przeglądu technologii wykorzystywanych w biometrii ze względu na realizowane prace badawcze w projekcie dotyczącym wprowadzenia na rynek innowacyjnego systemu identyfikacji osób za pomocą analizy zatok. Analizowany obszar również wpisuje się w rozwój zagadnień z dziedziny inżynieria produkcji, a w szczególności w obszar komunikacja-maszyna, gdzie istotna jest identyfikacja operatora, uprawnionego do podejmowania decyzji.

2. Współczesne problemy identyfikacji osób

Problematyka identyfikacji osób czy szczątków ludzkich jest zagadnieniem szeroko i błyskawicznie rozwijającym się, wychodzącym naprzeciw potrzebom zarówno służb odpowiedzialnych za bezpieczeństwo w kontekście światowego zagrożenia atakami terrorystycznymi (będących nową formą wojny, jaką prowadzą organizacje ekstremistyczne na całym świecie), jak również dla potrzeb identyfikacji szczątków ludzkich, ofiar katastrof czy też identyfikacji tożsamości osób, którym to zagadnieniem są zainteresowane m.in. administracja rządowa, służby wymiaru sprawiedliwości czy jednostki ochrony osób i mienia. Identyfikacji osób staje się coraz ważniejszym problemem, gdyż jak wynika ze statystyk policyjnych, z roku na rok zwiększa się liczba osób zaginionych oraz zwiększa się liczba niezidentyfikowanych zwłok [20].

Systemy rozpoznawania i identyfikacji pozwalają na stwierdzenie tożsamości z pewnym prawdopodobieństwem. Jeśli sięga ono 100%, to mówi się o jednoznacznej

identyfikacji lub osobniczej polimorficzności w odniesieniu do określonego kryterium porównawczego. Niemniej jednak są warunki/przesłanki, w których trudne jest dokonania jednoznacznej identyfikacji danego osobnika, stąd ciągłe poszukiwania nowych rozwiązań, udoskonalanie systemów identyfikacji, a tym samym dynamiczny rozwój systemów biometrycznych.

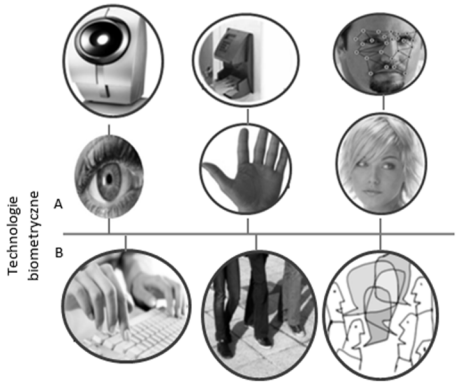
System biometryczny w zależności od przyjętego algorytmu identyfikacji może realizować dwa dość odmienne rodzaje zadań: proces autoryzacji, czyli pozwolenia na dostęp do określonego zasobu na podstawie pewnej przesłanki, czyli identyfikatora wskazującego wstępnie na personalia badanej osoby (np. użycie karty magnetycznej z zapisanymi danymi personalnymi, a następnie potwierdzenie – czyli właśnie autoryzacja – poprzez zbadanie np. odcisku papilarnego) oraz proces uwierzytelniania, czyli rzetelnego ustalenia tożsamości badanej osoby na podstawie stworzonego wcześniej repozytorium rozważanych osób. Począwszy od wczesnych lat 90. XX wieku zagadnienia automatycznego rozpoznawania twarzy wyraźnie zyskały na popularności, ponieważ obecnie odpowiednio wydajny sprzęt komputerowy stał się powszechnie dostępny, a jednocześnie pojawiło się duże zapotrzebowanie na stosowanie tej technologii w praktyce.

Konieczność ochrony przed zamachami terrorystycznymi, do której w ostatnim czasie przywiązuje się szczególną wagę, z pewnością przyczyniła się do wzrostu zainteresowania urządzeniami, zdolnymi do identyfikowania osób podejrzanych, pojawiających się w miejscach publicznych, takich jak: lotniska [17, 21], dworce, stadiony, stacje metra i wszelkie obiekty skupiające duże zgromadzenia ludzi [23].

Mając do czynienia z zadaniem uwierzytelniania, można wyróżnić kilka tradycyjnych jego środków. Pierwszym z nich jest operacja uwierzytelniania przeprowadzona na pewnego rodzaju mieniu, czyli pewnych przedmiotach fizycznych, takich jak klucz, paszport czy „inteligentne" karty. Należy zauważyć, że wadą powyższych środków jest duże narażenie na niepowołaną zmianę ich właściciela, zarówno w przypadku pożyczenia powyższych przedmiotów, jak i poza wiedzą właściciela. Kolejnym środkiem jest wiedza, która stanowi informację znaną tylko odpowiedniej osobie, np. hasło, kod PIN itp. (ale tu może nastąpić niekontrolowane przekazywanie informacji osobom nieuprawnionym do jej użytkowania np. podglądnięcie wprowadzanego kodu lub możliwość wymuszenia przekazania chronionej wiedzy poprzez element szantażu). Innym środkiem stosowanym do uwierzytelnienia są biometryki zwierające cechy osób pozwalające je odróżnić.

Biometria (ang. *biometrics*) obejmuje metody automatycznych pomiarów i porównywania cech fizycznych (antropometrycznych) lub zachowania człowieka. Celem jest identyfikacja ludzi lub weryfikacja przedstawianej tożsamości. Mierzone i porównywane cechy powinny być unikalne i stałe. Cechy biometryczne podzielić można na dwie kategorie: fizyczne (Rys.1. A) i behawioralne (Rys.1. B). Do pierwszej z nich zaliczane są: odcisk palca, geometria dłoni, obraz twarzy (tradycyjny, termogram, 3D lub inny), tęczówka i siatkówka oka, statyczny podpis (obraz podpisu), kształt małżowiny usznej, kształt warg, kod DNA. Do drugiej należą: dynamiczny podpis (siła nacisku, kolejność i szybkość pisania), styl pisania na klawiaturze, głos, sposób chodzenia, sposób mówienia (ruch warg) i inne. Wymienione cechy są unikalne dla każdego człowieka, jednak nie zawsze w tym samym stopniu. O ile trudno jest znaleźć osoby mające taki sam odcisk palca lub tęczówkę oka, to znalezienie osób mających podobną twarz lub głos jest

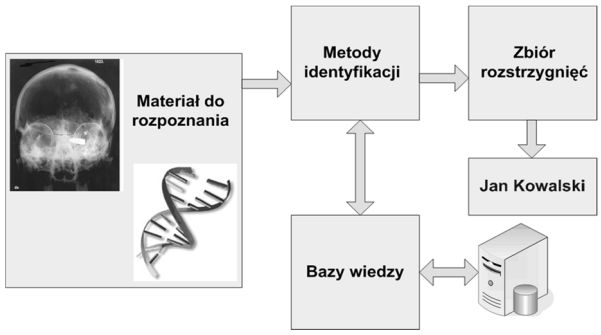
łatwiejsze. Drugim ważnym czynnikiem oceny cech biometrycznych jest ich stałość, czyli niezmienność w czasie. Pewne cechy biometryczne starzeją się szybciej (np. twarz), inne wolniej (np. małżowina uszna), jeszcze inne prawie wcale (tęczówka). Innym ważnym kryterium oceny cech biometrycznych jest łatwość ich pobrania. W przypadku twarzy – wystarczy zwykła kamera lub aparat fotograficzny. W przypadku np. odcisku palca wymagane jest użycie specjalistycznego urządzenia oraz współpraca (rozpoznawanego) człowieka z takim urządzeniem. Na uwagę zasługuje fakt, że możliwości identyfikacji są w istotny sposób związane z dostępnością materiału porównawczego znajdującego się w specjalizowanych bazach danych [18].



Rys. 1. Zestawienie najważniejszych technologii biometrycznych z podziałem na grupy: A(wykorzystanie cech anatomii) oraz B (wykorzystanie cech behawioralnych)

Do identyfikacji osoby niezbędny jest materiał badawczy o pożądanych właściwościach, np. odcisk palca z wyraźnymi liniami papilarnymi [7] czy materiał DNA lub zdjęcie RTG czaszki w przypadku zwłok. Celem metody identyfikacyjnej jest wskazanie właściwej osoby, od której materiał badawczy pochodzi, ale czasem także stwierdzenie pewnych wybranych cech takiej osoby np. płci [1], wieku [2, 20] czy kręgu etnicznego. Ze względu na różnorodność materiału badawczego oraz informacji, jakie planuje się uzyskać z materiału, stosowane są różne metody badawcze. Bez względu na wybraną metodę, tok postępowania pozostaje niezmienny (Rys. 2.) [12]:

1. wybór i przygotowanie odpowiedniego materiału badawczego.
2. identyfikacja na podstawie baz wiedzy i doświadczenia.
3. porównywanie otrzymywanych wyników z dostępnymi danymi.
4. wyodrębnienie zbioru prawdopodobnych informacji wynikowych.
5. wybór najbardziej prawdopodobnej identyfikacji lub identyfikacja osoby ze stuprocentową pewnością.



Rys. 2. Schematyczne uogólnienie dla metod identyfikacji osób [12].

Najbardziej pożądanymi metodami są te, które gwarantują jednoznaczną identyfikację osoby lub jej wybranych cech. Do metod spełniających kryteria jednoznaczności lub wysokiego prawdopodobieństwa (z wieloma ograniczeniami) należą m.in.: identyfikacja na podstawie linii papilarnych [9], weryfikacja geometrii dłoni [5], identyfikacja tęczówki oka [6], siatkówki oka [10], identyfikacja twarzy [11] oraz identyfikacja radiologiczna[13, 22].

3. Zastosowanie

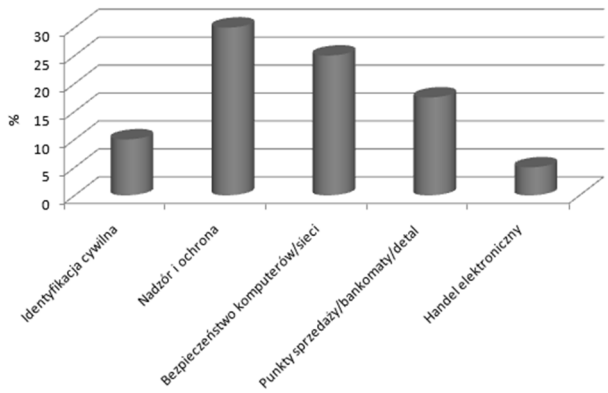
Międzynarodowa Grupa Biometryczna IBG [25] zaproponowała podział, gdzie rozróżniany jest pionowy podział, związany z charakterem wykorzystujących biometrię instytucji, bądź po prostu dziedzinami gospodarki, oraz podział poziomy, gdzie już nieco bardziej szczegółowo wylicza się najbardziej znane obszary zastosowań. Pierwszy obejmuje: agendy rządowe, podróże i transport, sektor finansowy, służba zdrowia, przestrzeganie prawa. Drugi natomiast to: identyfikacja cywilna, nadzór i ochrona, bezpieczeństwo komputerów/sieci, punkty sprzedaży/bankomaty/detal, handel elektroniczny i uwierzytelnianie abonentów, kontrola dostępu i rejestracja czasu pracy i identyfikacja kryminalna.

Nie sposób omówić wszystkich zastosowań, brak jest również wartości udziałowych poszczególnych zastosowań w rynku biometrycznym, zwłaszcza przy podziale pionowym. Zestawiono jednak procentowy udział publikacji , w roczniku 2008 Biometric Digest na temat poszczególnych zastosowań (Rys.3., Rys.4.)[16].

Tab. 1. Typowe zastosowania metod biometrycznych

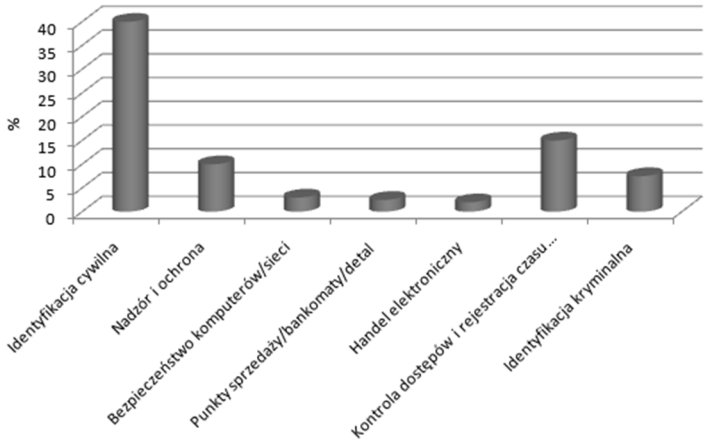
Obszary zastosowań	**Przykłady aplikacji**
karty z danymi biometrycznymi	- prawa jazdy, upoważnienia, karty wstępu - dokumenty imigracyjne, dowody osobiste, paszporty, rejestracja wyborców - ochrona przed nadużyciami w pomocy społecznej i służbie zdrowia

zabezpieczenie informacji	- kontrola rodzicielska dostępu do kanałów TV, logowanie do urządzeń osobistych i kont w systemach operacyjnych - ochrona dostępu do programów, baz danych, plików - bezpieczeństwo połączeń internetowych, kontrola dostępu do Internetu, ochrona danych medycznych - bezpieczne zakupy w sieci
wymiar sprawiedliwości, ochrona budynków	- zaawansowane systemy ochrony, telewizja przemysłowa - kontrola dostępu, analiza danych do celów śledztwa - eliminowanie kradzieży w sklepach, śledzenie podejrzanych, prowadzenie dochodzeń
rozrywka	- gry komputerowe, rzeczywistość wirtualna, programy szkoleniowa - współpraca człowieka z robotami i komputerami



Rys. 3. Procentowy udział zastosowań (podział pionowy) w rynku biometrycznym [%] w roku 2008 [26].

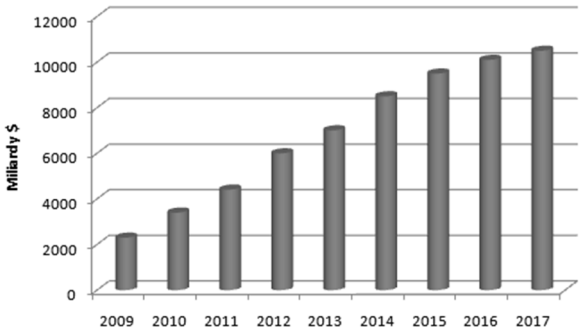
Do typowych obszarów zastosowań metod biometrycznych należą: karty z danymi biometrycznymi, zabezpieczenie informacji, wymiar sprawiedliwości, ochrona i rozrywka, dla których w poniższej tabeli przedstawiono przykłady aplikacji.



Rys. 4. Udział zastosowań (podział poziomy) w publikacjach i rynku [%] w 2008 roku [26].

4. Analiza rynku biometrycznego

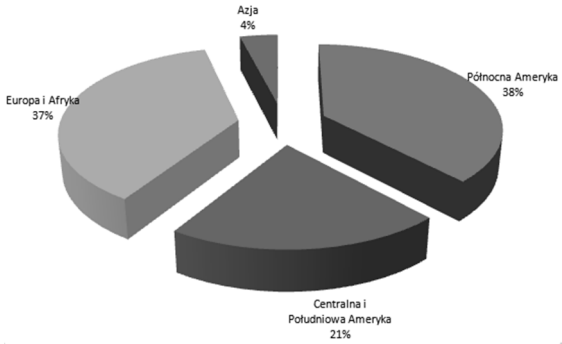
Systemy biometryczne to wciąż rozwijająca się branża nie tylko na rynku polskim, ale i światowym. Odkąd zostały wprowadzone pierwsze rozwiązania identyfikacji wciąż rośnie dochód z ich sprzedaży. Od roku 2009 do roku 2012 wzrósł on na rynku światowym o ok. 200%. Rocznie wzrasta on o ok. 40%.



Rys. 5. Przychody (miliardy $) ze sprzedaży biometrii wraz z prognozą na przyszłe lata [25].

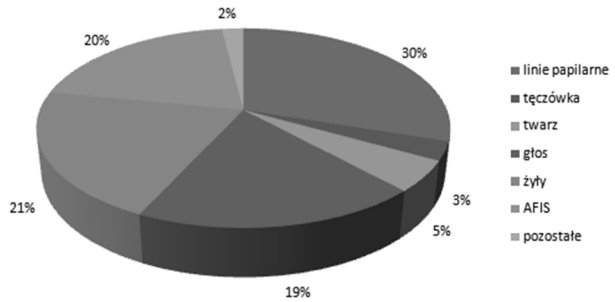
Przewiduje się, że globalne przychody z rynku biometrycznych technologii w 2017 mogą wynosić aż 11 miliardów dolarów (Rys. 5). Systemy identyfikacji osób zdobywają światowy rynek dzięki nowoczesnym rozwiązaniom, jak np.: łatwość użycia, dokładność i wydajność oraz rozszerzenie wykorzystania do zastosowań indywidualnych , komercyjnych oraz rządowych. Rozwój rynku biometrii jest napędzany przez wpływ globalnego rozwoju przemysłu IT.

Systemy biometryczne najbardziej rozpowszechnione są w regionie Ameryki Północnej oraz w Europie (Rys. 6). Jednak około 2017 roku dominującyn rynkiem w powyższym zakresie będzie Azja. (wraz z terenami na Pacyfiku).



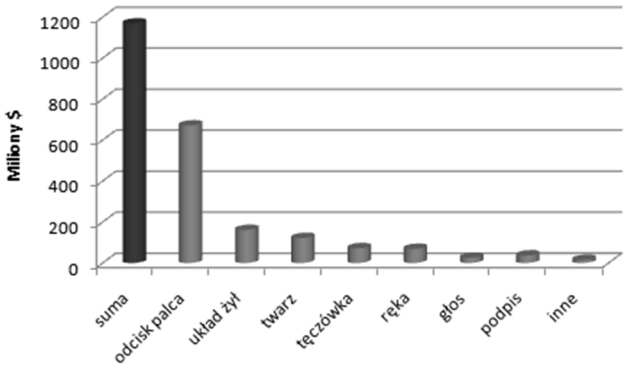
Rys. 6. Udział w dochodach ze sprzedaży biometrii z podziałem na regiony w 2011 r. [25].

Udział poszczególnych technik w światowym rynku biometrycznym ustabilizował się w 2003 roku. Nadal największą pozycję stanowią linie papilarne i to z udziałem prawie dwukrotnie wyższym od drugiej w kolejności techniki rozpoznawania twarzy (Rys. 7). W następnych latach przewiduje się jednak spadek udziału linii papilarnych. Jeśli chodzi o pozostałe techniki, to również nie odnotowuje się większych zmian w stosunku do ubiegłego roku. Udział pozostałych technik mieści się w zakresie 8%. Wśród omawianych w ciągu ostatniego roku realizacji kilkakrotnie mówiło się o rozpoznawaniu według siatki żył, lecz prawdopodobnie technika ta nie będzie miała w przyszłym roku znaczącego udziału. Jeśli chodzi o linie papilarne, to najczęściej wymienianą firmą jest Bioscrypt [27], który oferuje m.in. moduł OEM o nazwie MV—Lite, charakteryzujący się mniejszymi wymiarami i niższą ceną. Urządzenia Bioscryptu wykorzystywane są na największym rosyjskim lotnisku Domodiedowo i w Dubaiu, w amerykańskim dowództwie na Pacyfiku, bankach chińskich i na Mauritiusie, a także 75 centrach danych rządu Malty [28]. Do roku 2004 zainstalowano ponad 75 tysięcy czytników tej formy. Drugim znaczącym dostawcą tej techniki jest Identix, który oferuje też wyroby związane z rozpoznawaniem twarzy. Identix specjalizuje się przede wszystkim w systemach bezpośredniego skanowania (ok.70% na rynku USA).

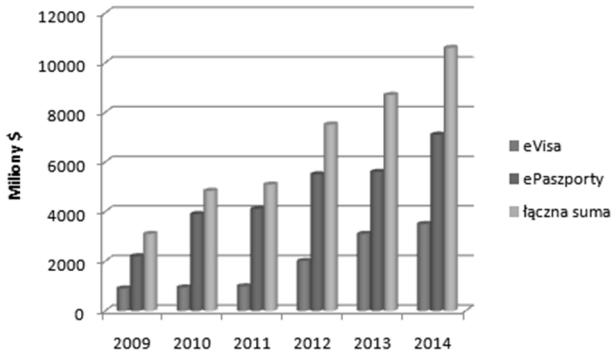


Rys. 7. Udział poszczególnych technik w światowym rynku biometrycznym w roku 2012[25].

Technologie biometryczne są coraz szerzej wykorzystywane w zakresie kontroli granicznej, ochrony porządku publicznego, eAdministracji oraz obrony narodowej. Powszechne wprowadzanie paszportów biometrycznych wpłynie na wdrożenie systemu eGate, który w najbliższych latach będzie głównym źródłem przychodów cywilnego i wojskowego rynku biometrycznego na świecie (Rys.8). Rada Unii Europejskiej uznała, że zabezpieczenia biometryczne w sposób wiarygodny udowadniają związek między dokumentem i jego właścicielem. Wprowadzenie paszportów biometrycznych wprowadzono, aby ograniczyć liczbę przestępstw związanych z kradzieżą tożsamości. Paszporty biometryczne są trudniejsze do sfałszowania. W związku z zarządzeniem Unii Europejskiej, od czerwca 2009 roku każda osoba ubiegająca się o wydanie paszportu musi złożyć odciski linii papilarnych dwóch placów wskazujących. Dlatego też każdy urząd odpowiedzialny za przyjmowanie wniosków paszportowych jest wyposażony w nowoczesny czytnik elektroniczny.



Rys. 8. Globalne przychody na rynku opieki zdrowotnej z podziałem na technologie w 2012 roku [26]



Rys. 9. Rynek e Paszportów i e Wiz [27]

W Polsce pierwsze paszporty biometryczne wydane zostały w 2006, jednak dokumenty te zawierały tylko jedną cechę biometryczną. Od 29 czerwca 2009 roku wszystkie wydawane w Polsce paszporty, oprócz systemu identyfikacji twarzy, zawierają również

dane odnośnie linii papilarnych. Rozwój przemysłu biometrycznego w Polsce jest bardzo dynamiczny (Rys.9), zwłaszcza, że coraz więcej firm prywatnych korzysta z takich rozwiązań. Należy tutaj dodać, że Polskie firmy produkują nie tylko dla kraju, ale również dla państw zagranicznych, np. biometryczne paszporty trafiają na Litwę.

Przychody z rynku ePaszportów i eWiz do końca 2014 osiągną ponad 10 mld USD rocznie (Rys.10).

	Liczba dok.	Liczba krajów	Przychód	Udział [%]		
	mln USD		mln USD	e-dok we wszyst. wydanych	e-dok. we wsz. w obiegu	w łącz. rynku e-paszp. i e-wiz
e-paszp. 2009	61,1	65	2337	52	28	73
e-wiz 2009	13,7	9	856	28		27
e-paszp. 2014	130	105	7179	87		67
e-wiz 2014	61	66	3542	87		33

Rys. 10. Rynek e- paszportów i e – wiz w roku 2009 i 2014 [29]

5. Podsumowanie

Obecne systemy biometryczne wykorzystują do pomiaru różne części ludzkiego ciała oraz cechy ludzkiego zachowania. Do najpopularniejszych biometrii wykorzystujących cechy fizyczne zaliczyć można: biometrię linii papilarnych, naczyń krwionośnych dłoni lub palca, tęczówki lub siatkówki oka, geometrii dłoni, twarzy, zmienności genetycznej DNA oraz identyfikację metodami radiologicznymi, np. na podstawie kształtu zatok czołowych.

Najbardziej rozpowszechnione są systemy identyfikacji dla administracji rządowej, służb wymiaru sprawiedliwości czy jednostek ochrony osób i mienia. Przykładem takiego systemu jest ewidencja (Rejestr PESEL,), ewidencja paszportowa (SEP), ewidencja pojazdów i uprawnień komunikacyjnych (Centralna Ewidencja Pojazdów i Kierowców), czy ewidencja w systemach opieki społecznej (np. POMOST) i wielu innych - niestety zgromadzone tam dane nie pozwalają na jednoznaczne zidentyfikowanie obywatela pod względem jego cech biologicznych. Nieco większe możliwości identyfikacji dają cechy biometryczne związane z rejestrowaniem odcisków palców zarówno w rejestrach kryminalnych, jak i paszportowych, ale opis ten niesie wiele ograniczeń i trudności [7]. Zagadnienie identyfikacji osób staje się coraz ważniejszym problemem, gdyż jak wynika ze statystyk policyjnych, z roku na rok zwiększa się liczba osób zaginionych oraz zwiększa się liczba niezidentyfikowanych zwłok.

Należy również pamiętać, iż biometria łączy się nierozerwalnie z zagadnieniami bezpieczeństwa, zarówno w kontekście zwiększania bezpieczeństwa wynikającego z właściwego zastosowania tych technik (dokładniejsza identyfikacja osób, powiązanie innych, istniejących identyfikatorów z ich właścicielem), jak i zapewniania bezpieczeństwa samej biometrii (m.in. bezpieczeństwo przechowywania i transmisji danych biometrycznych oraz test żywotności).Przechowywanie danych rozpatruje się w trzech obszarach: terminali i czytników biometrycznych, centralnych baz danych i kart mikroprocesorowych.

Surowe dane, przetworzone cechy biometryczne, wzorce biometryczne, a nawet wyniki weryfikacji mogą zostać zamienione przez niepowołane osoby lub skradzione i wykorzystane ponownie w celu uwierzytelnienia. Z tego powodu konieczne jest

stosowanie dodatkowych zabezpieczeń wzorców biometrycznych. W tym celu najczęściej wykorzystuje się typowe techniki kryptograficzne. Badania z raportu Unisys wskazują, że największą przychylność do zastosowania biometrii wykazali mieszkańcy Ameryki Północnej - 71 proc., następnie Europy - 69 proc. oraz Azji i Pacyfiku - 68 proc. Co ciekawe, co 10 respondent wyraził zgodę na wszczepienie specjalnych układów scalonych do swojego organizmu. Dla 83% badanych, główną zaletą identyfikacji biometrycznej jest niezawodność technologii oraz jednoznaczność jej wyników. 75 proc. respondentów jako praktyczną zaletę biometrii wskazało szybkość autoryzacji konkretnej osoby i uproszczenie procedur. Badania te wykazują, że coraz mniej respondentów obawia się utraty części swojej prywatności na skutek wdrożenia rozwiązań biometrycznych. Biometria może być wykorzystywane do różnych celów, ale nie bez przyczyny jest przedmiotem szczególnego zainteresowania sektora usług finansowych. Sektor ten posiada szczególne doświadczenia w zakresie wykorzystywania danych osobowych i restrykcyjnym podejściu do ich ochrony. Postrzega on biometrię, jako sposób na podniesienie bezpieczeństwa, także w zakresie ochrony danych osobowych i uniemożliwieniu wykorzystania danych wrażliwych przez osoby do tego nieuprawnione [14].

Przyszłość biometrii kryje się również w zastosowaniu biometrii przez klienta banku oraz w rozwijającym się nowym obszarze zastosowań, a mianowicie identyfikacji cech biometrycznych operatora w komunikacji "człowiek - maszyna". Na świecie, w tym sektorze istnieją wdrożenia systemów biometrycznych wykorzystywanych do uwierzytelniania klientów banków i autoryzacji transakcji. Dotychczas największy sukces we wdrożeniach biometrycznych w systemach samoobsługowych odniosły technologie biometrii naczyniowej: biometria naczyń krwionośnych palca (ponad 33 tys. bankomatów w Japonii) i naczyń krwionośnych dłoni (ok. 7 tys. bankomatów w Japonii). Przewaga tych technologii wynika z faktu, że zostały one opracowane specjalnie na potrzeby biometrycznej autoryzacji transakcji bankomatowych. Spełniają one wygórowane metody bezpieczeństwa w połączeniu z szybkością, wygodą użytkowania oraz małym rozmiarem czytników. Inną technologią, która była szeroko testowana w światowej bankowości, była biometria odcisku palca, którą wdrażano głównie w krajach Ameryki Południowej (Kolumbia, Chile, Brazylia). Głównym napotkanym problemem tej technologii okazał się bardzo duży współczynnik błędnych odrzuceń (od 8-30%), szczególnie wśród osób starszych i narażonych na zniszczenie naskórka dłoni. Na świecie testowano również bankomaty wykorzystujące biometrię tęczówki oka (m.in. USA i Wielka Brytania) i biometrię kształtu twarzy (np. USA). Zainteresowanie biometrią tęczówki oka wynika z wysokiego poziomu bezpieczeństwa. Główną barierą dla masowego wykorzystania tego rozwiązania okazała się cena kamer biometrycznych i wygoda użytkowania tego rozwiązania [4]. Po analizie stosowanych na świecie rozwiązań biometrycznych, można wyciągnąć wniosek, że do autoryzacji transakcji bankomatowych należy wybrać takie, które spełniają następujące kryteria: zapewniają najwyższe możliwe bezpieczeństwo, zapewniają szybkie uwierzytelnianie, są wygodne w użyciu, gwarantują niezawodny odczyt, mają rozmiar umożliwiający integrację z bankomatem [24].

Skomplikowanie ludzkiego organizmu i wciąż niedostatecznie poznane procesy wewnętrzne organizujące życie komórek we wzajemnej symbiozie dają wiele możliwości do poszukiwania nowych metod identyfikacji. Niestety, w przypadku tak skomplikowanego organizmu, proporcjonalnie duża jest również ilość niebezpieczeństw chorobowych czy wrodzonych patologii, które mogą zburzyć tezy o poprawności reguł rozpoznania, badanych na „standardowych" przedstawicielach gatunku. Nie bez znaczenia jest również ludzka natura, w sensie jednostki będącej częścią większej grupy – narodu, społeczeństwa

czy rasy. Niektóre z metod identyfikacji, takie jak np. wykorzystanie informacji genetycznych, właśnie ze względów społecznych nie będą mogły być nigdy wykorzystane w niektórych częściach świata [12]. Najbardziej odpornymi na warunki środowiskowe są metody radiologiczne. Kościec człowieka może być szeroko wykorzystywany w metodach identyfikacji osób. Rośnie zainteresowanie identyfikacją osób na podstawie zatok czołowych. Brak jednak narzędzi technicznych i metodyk identyfikacji z obszaru objętego zakresem zaproponowanego tematu. Taki stan daje podstawę do stwierdzenia, że celowe jest podjęcie próby rozwiązania tego problemu [12, 15].

Podjęcie próby opracowania metodyki, zaimplementowanie jej, stworzenie prototypu urządzenia i wprowadzenie tego innowacyjnego produktu na rynek jest narzędziem przedsiębiorczości, za pomocą którego ze zmiany czyni się okazję do podjęcia w przedsiębiorstwie nowego działania gospodarczego lub świadczenia nowego rodzaju usług. Zmiany te otwierają nowe perspektywy działania dla wielu przedsiębiorstw, także kooperujących np. w zakresie rozwoju nowego produktu, pod warunkiem, że podmioty te potrafią skutecznie wykorzystać innowacyjną orientację w swojej strategii rozwoju [8]. **S**ystemy biometryczne to wciąż rozwijająca się branża nie tylko na rynku polskim, ale i światowym. Odkąd zostały wprowadzone pierwsze rozwiązania identyfikacji, wciąż rośnie dochód z ich sprzedaży. Od roku 2007 do roku 2012 wzrósł on na rynku światowym o ok. 105%. Rocznie wzrasta on o ok. 30%. Zatem wyzwania biometrii w zakresie identyfikacji osób są jedną z szans dla przedsiębiorczych i innowacyjnych.

Literatura:

1. Asala S.A.: The efficiency of the demrking point of the femoral head as a sex determining parameter. ELSEVIER, Forensic Science International, No127, 2002.
2. Bednarek J., Bloch-Bogusławska E., Śliwka K.: Rozwój współczesnych metod oceny wieku na podstawie zarastania szwów czaszkowych, Z Archiwum Medycyny Sadowej i Kryminologii, Wydawnictwo Instytutu Ekspertyz Sądowych, nr 4, 2002.
3. Boratyńska-Sala A.: Zastosowanie teorii rozwiązywania innowacyjnych zadań w dziedzinie biznesu i zarządzania. Zarządzanie Przedsiębiorstwem; PTZP, XI Nr 1, 2008
4. Brzostowski T.: Innowacje, technologie, zagrożenia w świecie XXI wieku – z perspektywy finansów. Warszawa 2012
5. Czajka A., Pacut A.: Biometria dłoni. Warszawa 2009.
6. Czajka A., Pacut A.: Biometria tęczówki. Warszawa 2009.
7. FMSZ RFN: Paszport biometryczny: Zapis odcisków palców od dnia 01.11.2007 roku - Krótka instrukcja dla Działów Paszportowych. Federalne Ministerstwo Spraw Zagranicznych Republiki Federalnej Niemiec 2007.
8. Gawlik J., Kiełbus A.: Chosen aspects of innovative projects management. Archives of Foundry Engineering, Polish Academy of Sciences, Katowice 2010.
9. Kapczyński A.: Biometria linii papilarnych palca. Warszawa 2009.
10. Kapczyński A.: Biometria siatkówki oka. Warszawa 2009.
11. Kapczyński A.: Biometria twarzy. Warszawa 2009.
12. Karpisz D.: Komputerowa analiza obrazu RTG zatok czołowych jako podstawa identyfikacji osób. Rozprawa doktorska, Politechnika Krakowska, Kraków 2008.
13. Karpisz D., Kowalski P.: Mocowanie i pozycjonowanie czaszek do zdjęć radiologicznych. Czasopismo Techniczne, Nr 7 (108), 2011.

14. Kaszubski R.: Społeczne i prawne aspekty biometrii, Człowiek i dokument. Warszawa 2009.
15. Kowalski P., Karpisz D.: Numerical description of X-ray fronto-orbiculo-maxillary shape in image analysis as a high distinctive tool for development of the system of identification of persons and human remains. Rechtsmedizin, Volume 20, Number 4, SPRINGER Medizin Verlag, Berlin 2010.
16. Palfrey J., Gasse U., Digital B.: Understanding the First Generation of Digital Natives. 2010.
17. Poole R.W. Jr.: Airport Security: Time for a New Model. Reason Foundation, 2006.
18. Prinz M., Shaler R.: Der terroranschlag auf das World Trade Centre und die resultierenden rechtsmedizinischen aufgaben. Rechtsmedizin, 12/4, 2002.
19. Palfrey J., Gasse U., Digital B.: Understanding the First Generation of Digital Natives. 2010.
20. Ritz-Timme S., Cattaneo C., Collins M.J., Waite E.R., Schütz H.W., Kaatsch H.-J., Borrman H.I.M.: Age estimation: The state of the art in relation to the specific demands of forensic practice. Intetrnational Journal of Legal Medicine, 113(8), 2000.
21. Stefani A.M.: Testimony on Aviation Security. Federal Aviation Administration, U.S. Department of Transportation, 2000.
22. Tabor Z, Karpisz D, Wojnar L, Kowalski P: An automatic recognition of the frontal sinus in x-ray images of skull. IEEE Trans Biomed Eng, vol. 56, no. 2: 2009.
23. Townsend M., Revill J., Kelbie P.: Terror threat critical as Glasgow attacked. The Observer, Sunday July 1, 2007.
24. Związek Banków Polskich, Forum Technologii Bankowych, Biometria w bankowości i administracji publicznej, Warszawa 2009.
25. www.ibgweb.com XII 2013.
26. www.biometricgroup.com XII 2013.
27. www.koettersecurity.com XI 2013.
28. www.bioscrypt.eu X 2013.
29. www.imm.org.pl X 2013.

Dr inż. Anna Kiełbus
Mgr Karolina Furyk
Instytut Technologii Maszyn i Automatyzacji Produkcji
Politechnika Krakowska
31-155 Kraków, ul. Warszawska 24
tel./fax: (0-12) 374 32 83
e-mail: kielbus.anna@gmail.com
karolafur@gmail.com