Norbert PAŁKA[1], Elżbieta CZERWIŃSKA[1], Mieczysław SZUSTAKOWSKI[1], Marek PISZCZEK[1], Jarosław MŁYŃCZAK[1], Krzysztof FIRMANTY[1], Michał WALCZAKOWSKI[1], Marcin KOWALSKI[1], Artur GRUDZIEŃ[1], Leon JODŁOWSKI[1], Wiesław CIURAPIŃSKI[1], Janusz WRÓBEL[1], Mikołaj SOBCZAK[2], Mateusz NAWROCKI[2], Paweł HOŁOWEŃKO[3], Paweł POŹNIAK[3], Szymon PACHLA[3]

Instytut Optoelektroniki, Wojskowa Akademia Techniczna (1), Mlabs Sp. z o.o. (2), Straż Graniczna (3)

doi:10.15199/48.2017.11.32

Weryfikacja osób na podstawie wizerunku twarzy i odcisku palca – badania eksperymentalne

Streszczenie. *W pracy opisano wyniki badań eksperymentalnych dotyczące weryfikacji osób na podstawie wizerunku twarzy i odcisku palca. Opracowany system automatycznie odczytuje z polskiego paszportu biometrycznego powyższe dane, określa ich jakość i porównuje z danymi pobranymi od podróżnego na żywo. Dla 621 podróżnych eksperymentalnie wyznaczona skuteczność weryfikacji na podstawie obu cech wynosi 88%. Stosując logikę ważoną tę skuteczność można podnieść do 94%.*

Abstract*. The paper describes the results of experimental research on the verification of persons based on facial image and fingerprints. The developed system automatically acquires data from the Polish biometric passport, determines their quality and compares with the data collected from the live traveller. For 621 travellers, the experimentally determined verification efficiency basing on both features equals to 88%. This efficiency can be increased to 94% by means of the weighted logic.* ***(Verification of people based on facial image and fingerprints - experimental studies)***

Słowa kluczowe: dokument biometryczny, weryfikacja wizerunku twarzy, weryfikacja odcisku palca, czytniki biometryczne
Keywords: biometric document, facial image verification, fingerprint verification, biometric readers

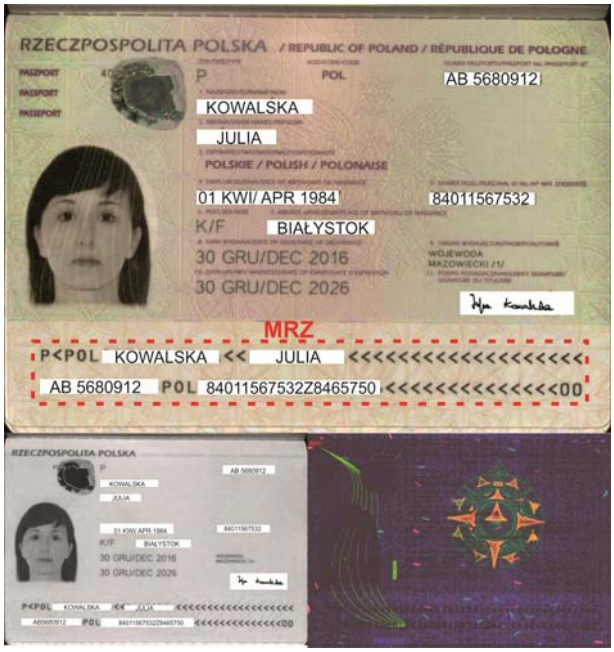
Wstęp

Ostatnie 25 lat to burzliwy rozwój technik biometrycznych związany z możliwością identyfikacji i weryfikacji osób [1, 2]. Biometria pozwala na identyfikację osób na podstawie cech fizjologicznych i behawioralnych. Fizjologia niesie informacje o cechach fizycznych ludzi, które można zmierzyć lub odczytać w danym momencie, m.in. odciski palców, wizerunek twarzy czy obraz tęczówki. Mają one charakter statyczny. Z kolei cechy behawioralne mają charakter dynamiczny i opisują jak dana czynność wyuczona bądź nabyta jest wykonywana np.: sposób chodzenia czy głos w trakcie mówienia [3, 4].

Głównymi zastosowaniami biometrii jest identyfikacja i weryfikacja osób. Identyfikacja pozwala ustalić, kim jest dana osoba, poprzez pobranie od niej próbki danej cechy (np. odcisku palca) i wyszukaniu w bazie danych próbek do niej podobnych. Weryfikacja sprawdza czy dana osoba jest tą, za którą się podaje. Biometria znajduje zastosowanie w systemach bezpieczeństwa, gdzie wymagane jest potwierdzenie tożsamości osoby takich jak np. banki, specjalne strefy dostępu w budynkach czy odprawa graniczna [5]. Niewątpliwą jej zaletą jest eliminacja wad jakie mają inne systemy uwierzytelniania wymagające okazania dokumentu, bądź podania hasła dostępu. Kody pin do kart bankomatowych mogą być zapomniane lub skradzione tak samo jak dowody tożsamości i paszporty. W biometrii to sam człowiek jest nośnikiem informacji, gdyż to on zawiera określony przez naturę unikatowy klucz identyfikacji [6].

Celem przeprowadzonych testów było praktyczne określenie parametrów biometrycznej weryfikacji osób na podstawie wizerunku twarzy i odcisków palca. Prace były wykonywane na zlecenie Straży Granicznej, która chciała poznać praktyczne aspekty weryfikacji na podstawie powyższych danych zawartych w polskich paszportach biometrycznych. Do badań zbudowano system, który pozwolił na odczyt obu cech biometrycznych i porównanie ich z realnie pobranym od właściciela paszportu. System był badany przez dwa tygodnie w Mazowieckim Porcie Lotniczym Warszawa-Modlin z udziałem ponad 600 osób.

W artykule opisano opracowany system i przeprowadzone testy oraz poddano analizie wyniki badań. Określono jakość zdjęć wizerunku twarzy i odcisków palca pobieranych z paszportów i także rejestrowanych na żywo od pasażerów. Następnie określono skuteczność weryfikacji osoby na podstawie pojedynczych cech biometrycznych jak i ich sumy. Podano analizie także przyczyny błędów weryfikacji. Dodatkowo celem było sprawdzenie, która z cech biometrycznych daje lepszą skuteczność weryfikacji i jaki jest wynik w wypadku połączenia sprawdzenia obu cech



Rys.1. Zdjęcie pierwszej strony paszportu wykonane przez czytnik dokumentów w świetle: widzialnym (zdjęcie górne), podczerwonym (zdjęcie lewe dół) i ultrafioletowym (zdjęcie prawe dół). *Ze względu na ochronę danych osobowych prawdziwe dane wycięto i zastąpiono fikcyjnymi.*

Paszport biometryczny

Paszport biometryczny to dokument wydawany polskim obywatelom od 2009 roku, który oprócz danych osobowych podróżnego zwiera także jego cechy biometryczne - zdjęcie wizerunku twarzy i odcisku palca. Informacje cyfrowe przechowywane są w chipie EEPROM w standardzie ISO14443. Chip znajduje się w tylnej okładce paszportu

Odczyt danych następuje poprzez komunikację RFID czytnika dokumentów z anteną chipu. Dane biometryczne pozwalają automatycznie zweryfikować tożsamość właściciela paszportu.

Czytnik dokumentów odczytuje dane osobowe z paska MRZ (ang. machine readable zone – strefa odczytu maszynowego) [7]. Jest to obszar zawierający zapisane czcionką do odczytu maszynowego (najczęściej OCR-B), dane zawarte w paszporcie w sposób skrócony. Ułatwia to komputerowy odczytu dokumentu w portach lotniczych.

Strona z danymi i zdjęciem może być odczytana w trzech różnych typach oświetlenia: VIS, IR i UV. Szczególne cechy obrazu pojawiają się tylko przy pewnym oświetleniu, co umożliwia wykrycie potencjalnych fałszerstw dokumentów.

Budowa systemu

W celu przeprowadzenia eksperymentu zbudowano system, w którym osoby zaproszone do badań mogły same w przeciągu 30 sekund zweryfikować swoje dane biometryczne. Na rys. 2 przedstawione są najważniejsze, elementy systemu: monitor podpowiedzi, dwie kamery, dwa oświetlacze oraz czytniki: dokumentów i palca.

Rys.2. System do automatycznej weryfikacji osób.

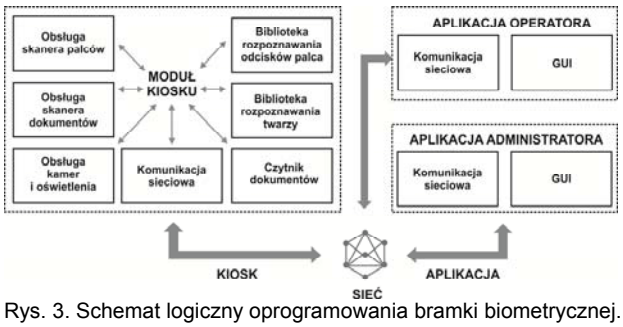
Monitor podpowiedzi służy do wyświetlania komunikatów instruujących i wskazówek graficznych. Monitor w pierwszej kolejności informuje, w jaki sposób należy przyłożyć paszport biometryczny do czytnika dokumentów. Czytnik wykonuje całostronicowe skany stron przy trzech typach oświetlenia: VIS, IR, UV i odczytuje dane osobowe z paska MRZ. Następnie przy wykorzystaniu certyfikatów zabezpieczających czytnik łączy się z chipem RFID paszportu, skąd również pobiera dane osobowe oraz zdjęcia wizerunku twarzy i odcisku palca. Całość odczytu trwa około 15 sekund.

W drugim kroku komunikat na ekranie prosi o zdjęcie okrycia głowy, okularów i nakazuje patrzeć w środek ekranu. W tym momencie zapalają się obydwa oświetlacze, które równomierne oświetlają twarz podróżnego, gdy dwie kamery o rozdzielczości 2046 px x 1086 px umieszczone na różnych wysokościach wykonują zdjęcia statyczne, które są analizowane pod kątem jakości biometrycznej, czyli zawartości użytecznych parametrów - pewnych miar (np. odległości między oczami), które można odczytać ze zdjęcia twarzy. Zasłonięcie części twarzy (np. włosami) lub pochylenie/obrót twarzy może utrudnić lub nawet uniemożliwić akwizycję tych danych. Jeśli zdjęcie przekracza próg jakości biometrycznej (tj. 20 pkt w skali 1-100), to jest ono dalej porównywane ze zdjęciem wzorcowym odczytanym z paszportu. Pierwsze przekroczenie progu weryfikacji przez zdjęcie z którejkolwiek kamery uznane jest za weryfikację pozytywną. Gwarantuje to poprawne działanie systemu zarówno dla osób niskich, jak i wysokich.

W trzecim kroku ekran podpowiedzi wskazuje, który palec należy przyłożyć do optycznego czytnika linii papilarnych o rozdzielczości 500 dpi i wymiarach okienka pomiarowego 24 mm x 16 mm. Na koniec system wyświetla wynik weryfikacji. Na tablecie operatora systemu pojawiały się informacje o jakości zdjęć oraz dane liczbowe z wynikami weryfikacji. System był także testowany na próby oszustwa (m.in. na zdjęcie wydrukowane na kartce papieru), gdzie wykazał się wysoką odpornością.

Oprogramowanie

Oprogramowanie sterujące systemem zostało wykonane w technologii Microsoft .Net. Na rys. 3 przedstawiono ogólny schemat logiczny budowy oprogramowania.



Rys. 3. Schemat logiczny oprogramowania bramki biometrycznej.

Można wyróżnić tu odrębne aplikacje:

- Oprogramowanie kiosku
- Aplikację Operatora
- Aplikację Administratora

Moduł kiosku to oprogramowanie sterujące procesem odprawy i czuwające nad prawidłową pracą urządzeń wykorzystywanych w procesie automatycznej odprawy, takich jak czytnik paszportu czy czytnik palca. Dodatkowo jego zadaniem jest również synchronizacja pracy urządzeń i sterowanie przepływem informacji między nimi. Przykładowa sekwencja przepływu informacji to odczytanie z paszportu, w procesie *Extended Access Control,* challenge, podpisanie go certyfikatem zapisanym na kluczu sprzętowym, a następnie zwrócenie podpisanej odpowiedzi do chipu paszportu.

Kolejnym zadaniem modułu kiosku jest przesyłanie informacji o automatycznej odprawie do aplikacji operatora i administratora. Oprogramowanie kiosku charakteryzuje się modułową budową, co pozwala na łatwe dostosowywanie go do zmieniających się potrzeb i wymagań, np. wymiany czytnika na nowszy. Przykładowo – w momencie zmiany któregoś urządzenia wystarczy wymienić również software'owy moduł jego obsługi. Nie jest konieczna modyfikacja całego oprogramowania. Odrębnym zadaniem oprogramowania bramki biometrycznej jest prowadzenie analizy biometrycznej. Jest to proces wieloetapowy, wymagający doskonałej integracji ze sprzętem i dostępnymi bibliotekami. Do najważniejszych elementów kontroli biometrycznej należą:

- Odczyt paszportu – wymaga zawansowanej obsługi uwierzytelniania i certyfikatów uzyskanych od wystawcy paszportu.

- Pozyskanie cech biometrycznych – najtrudniejszy element kontroli biometrycznej. Wymaga reagowania na różne, często trudne do przewidzenia, zachowania podróżnych. Czasem wymagane jest kilkukrotne wykonanie zdjęcia twarzy, czy też dłuższego oczekiwania na prawidłowe przyłożenie palca. Wymaga to ciągłej kontroli jakości pozyskiwanych danych i reagowania online, poprzez zaawansowane algorytmy
- Porównanie cech pozyskanych od podróżnego i odczytanych z paszportu – realizowane przez bibliotekę MegaMatcher firmy Neurotechnology [8].

Zadaniem Aplikacji Operatora jest prezentowanie osobie uprawnionej (np. funkcjonariuszowi Straży Granicznej) informacji o przebiegu automatycznej kontroli biometrycznej. Prezentowane są: dane osobowe, dane biometryczne, wyniki porównania danych biometrycznych z paszportu z tymi pobranymi od podróżnego oraz status sprawdzenia autentyczności paszportu.

Aplikacja Administratora różni się nieznacznie od Aplikacji Operatora. Jej użytkownikiem jest osoba nieuprawniona do zarządzania danymi osobowymi, w związku z czym nie mogą być one prezentowane na ekranie. Zamiast tego aplikacja oferuje podstawowe dane statystyczne odnośnie odpraw przeprowadzonych danego dnia. Dodatkowo administrator ma do dyspozycji przycisk „błędna kontrola", czym może zasygnalizować błędne zachowanie się systemu. Pozwala to odnotować w logach urządzenia błędną decyzję systemu. Na tej podstawie w sposób automatyczny może zostać wyznaczona skuteczność działania i trafność podejmowanych decyzji.

Komunikacja pomiędzy poszczególnymi elementami systemu odbywa się przy pomocy protokołu TCP/IP, co pozwala na wykorzystanie istniejącej infrastruktury sieciowej i dowolne rozmieszczenie elementów systemu. Możliwe jest również użycie sieci Wi-Fi, co umożliwia użytkowanie aplikacji na urządzeniach mobilnych. Wyniki badań

Do badań przystąpiło 621 osób, w tym 31 to osoby podszywające się – posługujące się paszportem innej osoby.

W pierwszym etapie testów czytnik dokumentów odczytywał dane z paszportu. Z dokumentu pobrano zdjęcia twarzy. W skali 1-100, średnia jakość zdjęć (zgrubnie utożsamiana z liczbą cech biometrycznych) wynosiła około 55±8, najgorszy wynik to 33, najlepszy to 87. Oznacza to, że zdjęcia twarzy odczytane z paszportu mają średnią jakość „biometryczną", co jest dość istotne z punktu widzenia dalszej weryfikacji.

Następnie z paszportu pobrano odciski palców. W skali o zakresie 1-100, średnia jakość zdjęć (zgrubnie utożsamiana z liczbą cech biometrycznych), wynosiła około 89±7, najgorszy wynik to 43, najlepszy to 100. Oznacza to, że zdjęcia odcisków palców odczytane z paszportu mają wysoką jakość „biometryczną", co jest istotne z punktu widzenia dalszej weryfikacji. W jednym przypadku osoba nie miała odcisków palców w paszporcie, gdyż ich stan nie umożliwiał ich pobrania.

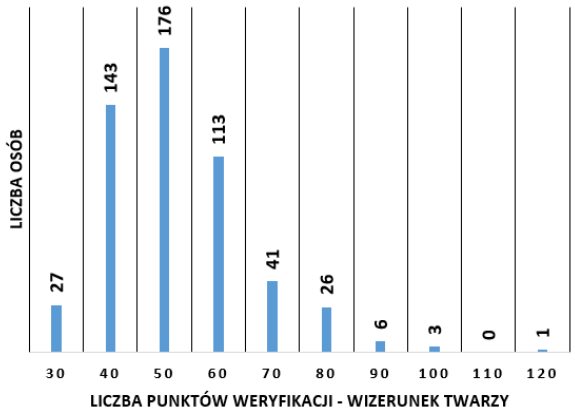
A. Weryfikacja wizerunku twarzy

Po zakończeniu procesu odczytu danych z paszportu system przez 3 sekundy pokazywał ekran, który prosi podróżnego o zdjęcie okularów i czapki oraz odsłonięcie włosów. Po czym system przechodzi do wykonywania zdjęcia twarzy i ocenia jego jakość. Jeśli jakość zdjęcia przekroczyła próg jakości (20 pkt. wg skali 1-100), zdjęcie dalej klasyfikowano do porównania ze zdjęciem odczytanym z paszportu.

Dla 596 z 621 podróżnych udało się przekroczyć próg jakości zdjęcia. Średnia jakość biometryczna tych zdjęć to 55±12 punktów. Najgorsze zdjęcie posiada wartość 20, najlepsze 86. Dla 25 osób system nie był w stanie wykonać zdjęcia, którego jakość przekracza próg, co spowodowane było m.in. elementami przesłaniającymi/modyfikującymi twarz (np. grubymi okularami, których podróżny nie zdjął, mocnym makijażem, dużą brodą, szalikiem, czapką, kolczykami w wielu miejscach na twarzy) lub niewłaściwą pozycją człowieka (np. przekrzywienie lub pochylenie głowy, niemożliwość ustawienie twarzy pionowo (np. człowiek mocno pochylony w przód, garbaty).

Zdjęcia otrzymane ze skanowania „na żywo" zostały porównane ze zdjęciem odczytanym z chipu paszportu. Do porównania został zastosowany pakiet VeriLook SDK firmy Neurotechnology [8]. Wiarygodność technik biometrycznych jest charakteryzowana przez dwa najważniejsze wskaźniki:
– fałszywej akceptacji nieuprawnionej osoby (FAR – *False Acceptance Rate*),
– fałszywego odrzucenia uprawnionej osoby (FRR – *False Rejection Rate*).

Im współczynnik FAR jest niższy i urządzenie rzadziej wpuszcza nieuprawnione osoby, tym współczynnik FRR jest wyższy i odrzucanych jest więcej osób uprawnionych i odwrotnie. W badaniach twarzy przyjęto FAR na poziomie 0,3%, co wg producenta oprogramowania odpowiada FRR około 1,8%, ale w idealnym przypadku weryfikacji twarzy niezasłoniętych i właściwie ustawionych. Odpowiada to progowi 30 punktów uzyskanych w zastosowanym programie weryfikującym. Wyżej opisana skala jakości zdjęcia jest liniowa w zakresie 1-100 i ocenia liczbę cech biometrycznych na zdjęciu. Skala weryfikacji jest nieliniowa (logarytmiczna) i określa jak bardzo twarze są podobne. Na podstawie skali weryfikacji można teoretycznie wyznaczyć FAR i FRR.



Rys.4. Weryfikacja pozytywna na podstawie wizerunku twarzy – liczba osób w poszczególnych przedziałach: 30-39, 40-49,…

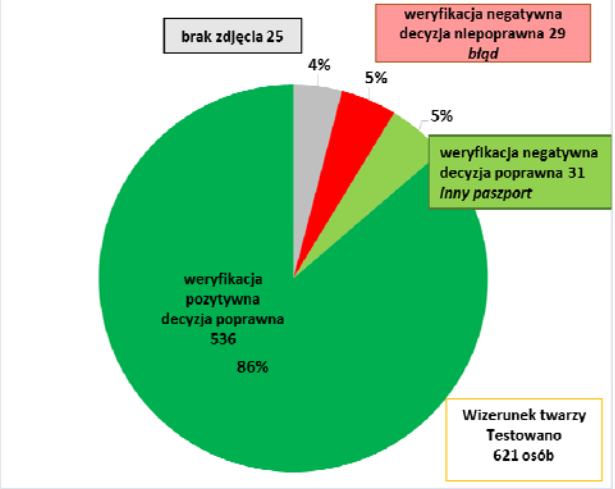
Z 596 osób, dla których udało się uzyskać zdjęcie twarzy na żywo ponad progiem jakości 20 pkt.:

➢ 565 to prawowici właściciele paszportów. Wśród nich:
- pozytywną weryfikację przeszło **536** osób (decyzja poprawna). Średnia wartość punktowa weryfikacji to 48±9. Wartość minimalna to 30, a maksymalna to 112. Na rys.4 przedstawiono histogram wyników weryfikacji na podstawie wizerunku twarzy.
- 29 osób zaklasyfikowano jako negatywną weryfikację (decyzja niepoprawna). Tu przeważały wartości weryfikacji w zakresie 20-30. Te liczby oznaczają, iż istnieje podobieństwo pomiędzy osobami z obu zdjęć, jednakże jest ono zbyt małe, żeby taka osoba została pozytywnie zweryfikowana z zadanym poziomem FAR.

Istnieje pewna korelacja pomiędzy jakością zdjęcia i wynikiem weryfikacji, natomiast nie zawsze niska jakość zdjęcia oznacza niski wynik weryfikacji.

- **31** próby weryfikacji z cudzym paszportem, gdzie nigdy nie uzyskano przekroczenia progu weryfikacji. Jest to poprawna decyzja systemu. Wartości punktowe nie przekraczały 8. Jest to bardzo ważny wynik – żadna nieuprawniona osoba nie przeszła badań pozytywnie, a wynik weryfikacji jest odległy od progu. Jest to weryfikacja negatywna, ale decyzja poprawna.

Rysunek 5 przedstawia liczbowo i procentowo wynik weryfikacji na podstawie wizerunku twarzy. Skuteczność z wykorzystaniem wizerunku twarzy, rozumiana jako stosunek decyzji poprawnych do wszystkich badań wynosi (536+31)/621=91%.



Rys.5. Weryfikacja na podstawie wizerunku twarzy – reprezentacja procentowa i liczbowa.

B. Weryfikacja odcisku palca

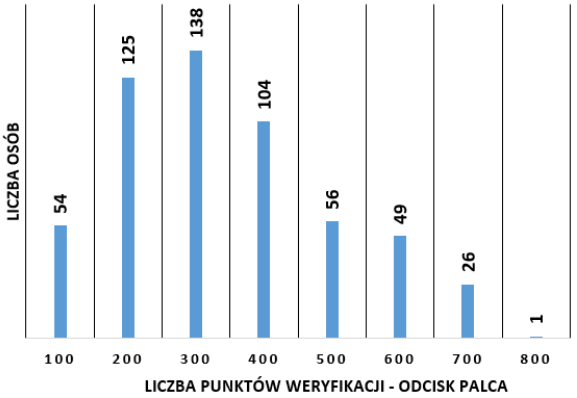
W kolejnym kroku ekran wskazywał, który palec należy przyłożyć do czytnika. W tym przypadku system czeka, aż zdjęcie odcisku palca będzie miało dostateczną jakość, czyli wystarczającą liczbę cech biometrycznych. Próg jakości wynosił 25 w skali 1-100.

Wśród 621 podróżnych dla 6 przypadków powstał błąd w skanerze palca (który trzeba wyjaśnić z producentem) i zdjęcie odcisku nie zostało przesłane dalej do analizy. W dwóch przypadkach podróżny w trakcie badania zrezygnował z testu i nie przyłożył palca, a w 1 przypadku nie zdążył przyłożyć palca do skanera – był pochłonięty zakładaniem okularów. W związku z tym pobrano odcisk palca od 612 osób. Średnia jakość pobranego odcisku palca w skali 1-100 wynosi 81±11. Wartość minimalna to 25, a maksymalna to 100. Oznacza to, że generalnie zdjęcia odcisków palca posiadają dość wysoką jakość biometryczną, niewiele ustępującą zdjęciom odcisku palca pobranym z paszportu.

Pobrane na żywo zdjęcia odcisku palca weryfikowane były ze zdjęciami pobranymi z paszportu za pomocą oprogramowania VeriFinger 6.0 firmy Neurotechnology [8]. Jako próg weryfikacji przyjęto FAR na poziomie 0,1%, co odpowiada FRR na poziomie 1,2% i progowi punktowemu 36.

Wśród 612 osób, dla których udało się pobrać odcisk palca ponad progiem 25 pkt.:

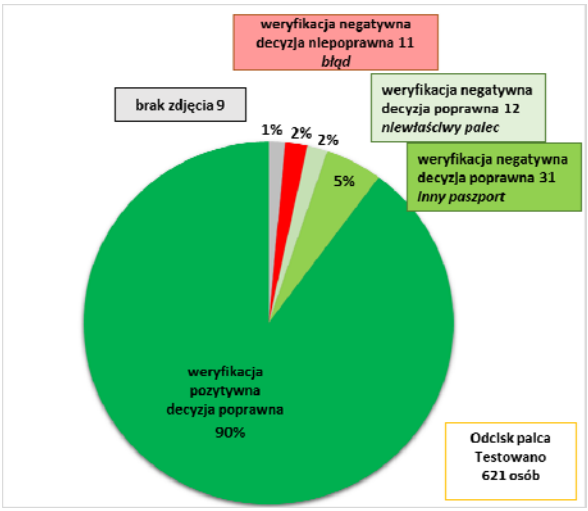
- **12** osób przyłożyło nie ten palec, który był wskazywany przez system, uzyskując oczywiście weryfikację negatywną, ale jest to decyzja poprawna z punktu widzenia działania systemu. Problemy te dotyczyły najczęściej palca środkowego.
- **31** osób miało cudzy paszport. Weryfikacja była negatywna, gdyż osoby uzyskały liczbę punktów poniżej 10. Jest to weryfikacja negatywna (decyzja poprawna).
- 569 to osoby, które miały swój paszport i dla których pobrano odpowiednie odciski palców. W tym przypadku:
  - system pozytywnie zweryfikował **558** osób. Tu rozrzut wyników jest dość duży – średnia wynosi około 300±120 punktów. Zdarzały się wyniki weryfikacji ponad 500, jaki i poniżej 50 punktów. Na rys. 6 przedstawiono histogram wyników weryfikacji na podstawie odcisku palca.
  - 11 osób zostało błędnie zweryfikowanych. To weryfikacja negatywna (decyzja niepoprawna). Mogło zdarzyć się, że osoba przyłożyła inny palec niż wskazany, ale badacze tego nie zauważyli.



Rys.6. Weryfikacja pozytywna na podstawie odcisku palca – liczba osób w poszczególnych przedziałach: 40-99, 100-199,…

Błędy weryfikacji wynikają m.in. z: przyłożenie palca w niewłaściwy sposób – czubkiem, bokiem, zbyt głęboko, czasem zbyt długi paznokieć przeszkadzał w prawidłowym ułożeniu palca na czytniku, przyłożenia ubrudzonego palca, np. w smarze oraz kłopotów z właściwym przyłożeniem kciuka do czytnika ze względów anatomicznych.

Rysunek 7 przedstawia liczbowo i procentowo wynik weryfikacji na podstawie odcisku palca. Skuteczność weryfikacji z wykorzystaniem odcisku palca, rozumiana jak stosunek decyzji poprawnych do wszystkich badań wynosi (558+12+31)/621~96%.



Rys.7. Weryfikacja na podstawie odcisku palca – reprezentacja procentowa i liczbowa.

C. Weryfikacja ludzi na podstawie obu cech biometrycznych

Analizując wyniki z punków A i B można wyznaczyć parametry liczbowe dla przypadku, kiedy pozytywna weryfikacja bazuje łącznie na pozytywnej weryfikacji na

podstawie wizerunku twarzy i odcisku palca (logika „i"). W ujęciu całościowym, z 621 osób, które przystąpiły do eksperymentu:

- dla 549 osób, którzy mieli poprawnie uwierzytelniony paszport system wydał poprawną decyzję, w tym:
  - weryfikację pozytywną przeszło 506 osób, którzy mieli łącznie poprawnie zweryfikowany wizerunek twarzy i odcisk palca,
  - weryfikację negatywną uzyskało 31 osób (podszywających się pod inną osobę), którzy mieli łącznie negatywnie zweryfikowany wizerunek twarzy i odcisk palca,
  - weryfikację negatywną uzyskało 12 osób (którzy pomylili palec), którzy mieli pozytywnie zweryfikowany wizerunek twarzy, a negatywnie zweryfikowany odcisk palca,
- dla 38 osób, którzy mieli poprawnie uwierzytelniony paszport, system podjął niepoprawną (błędną) decyzję, w tym:
  - 27 osób miało negatywnie zweryfikowaną twarz i pozytywnie zweryfikowany odcisk palca,
  - 9 osób miało pozytywnie zweryfikowaną twarz i negatywnie zweryfikowany odcisk palca,
  - 2 osoby miały negatywnie zweryfikowane obie cechy.

Skuteczność weryfikacji z wykorzystaniem dwóch cech biometrycznych (wizerunku twarzy i odcisku palca), rozumiana jak stosunek decyzji poprawnych do wszystkich badań wynosi (506+43)/621 ~88%.

D. Weryfikacja ważona na podstawie wizerunku twarzy lub odcisku palca

Analiza opracowana w punkcie C działa w trybie logicznego „i" (koniunkcja), czyli wyniki obu weryfikacji muszą być pozytywne, żeby cały proces weryfikacji był pozytywny. Powoduje to obniżenie skuteczności działania systemu do 88%. Jednakże wtedy prawdopodobieństwo błędnej decyzji i przepuszczenia niewłaściwej osoby jest bardzo niskie.

Przy pracy z dwoma cechami biometrycznymi można również stosować znane z literatury rozwiązania pośrednie [6], gdzie brak lub niska liczbowa wartość weryfikacji na podstawie jednej cechy jest kompensowana wyższymi wymaganiami dla drugiej cechy biometrycznej. Pozwala to to zmniejszyć FRR zachowując niski FAR.

W przeprowadzonych badaniach 27 razy równocześnie negatywnie zweryfikowano wizerunek twarzy i pozytywnie odcisk palca, a 9 razy miała miejsce sytuacja odwrotna. Jak widać problem z weryfikacją twarzy jest 3 razy częstszy niż z palcem. Wśród tych 27 przypadków, 20 to przypadki, kiedy wartość weryfikacja na podstawie twarzy znajduje się nieco poniżej progu i wynosi 20-29 punków, co odpowiada FAR 3%-0,3%. Stosując dla tych przypadków niższy próg weryfikacji wizerunku twarzy o wartości 20 punktów i ustalając równocześnie wysoki próg dla weryfikacji na podstawie palca na poziomie 72 punktów (FAR rzędu 0,0001%), uzyskuje się dodatkowe 19 weryfikacji pozytywnych (decyzja poprawna).

Idąc dalej, w 25 przypadkach nie udało się wykonać zdjęcia twarzy o odpowiednich parametrach, a w 9 odcisku palca. Ponownie dominuje problem z weryfikacją twarzy. Dla tych 25 przypadków, kiedy nie mamy żadnej informacji o weryfikacji na podstawie twarzy, można założyć, że w celu podjęcia decyzji bazujemy tylko na odcisku palca, ale z bardzo wysokim progiem. Dla progu równego 96 punktów FAR wynosi 0,000001%. Powyżej tego progu mieści się 21 z 25 przypadków, które stanowią dodatkowe 21 weryfikacji pozytywnych (decyzja właściwa).

Stosując powyższy algorytm nazwany ważonym, otrzymuje się następujące dane:

- 546 osoby – weryfikacja pozytywna, decyzja poprawna,
- 79 osób - weryfikacja negatywna, z czego:
  - 43 przypadki to decyzja poprawna, gdyż te osoby nie miały prawa przejść przez kontrolę graniczną,
  - 19 przypadków to decyzja niepoprawna, gdyż osoby te miały prawo przejść przez kontrolę graniczną,
  - 13 przypadków to brak decyzji, z powodu nieposiadania wystarczającej ilości danych.

Skuteczność weryfikacji z wykorzystaniem weryfikacji ważonej, rozumiana jak stosunek decyzji poprawnych do wszystkich badań wynosi (546+43)/621=94%. Dla 3% osób system wydał decyzję niepoprawną, a dla 2% nie był w stanie wypracować decyzji i dlatego podjął decyzję o weryfikację negatywnej.

Tabela 1. Zestawienie liczbowe wykonane dla weryfikacji na podstawie obu i jednej cechy biometrycznej.

Weryfikacja (decyzja)	Wizerunek twarzy	Odcisk palca	Obie cechy „i"	Obie cechy ważone
weryfikacja pozytywna (decyzja poprawna)	536	558	506	546
weryfikacja negatywna (decyzja poprawna)	29	43	43	43
weryfikacja negatywna (decyzja niepoprawna)	31	11	38	19
weryfikacja negatywna (brak decyzji)	25	9	34	13
Skuteczność [%]	**91**	**96**	**88**	**94**

Jak widać z tabeli 1, najwyższa skuteczność została osiągnięta przy weryfikacji bazującej na odcisku palca; nieco mniejsza wykorzystując wizerunek twarzy. Jest to wynik zgodny z przewidywaniami, gdyż:

- Odcisk palca ma lepszą jakość biometryczną (większą ilość danych) niż wizerunek twarzy zarówno w paszporcie, jak i przy akwizycji na żywo.
- Przy akwizycji twarzy występuje większa liczba problemów związanych z różnymi elementami przysłaniającymi twarz.
- Dla obu metod weryfikacji istnieją problemy związane z niewłaściwym ułożeniem twarzy i palca względem czytnika.
- W przypadku pobierania odcisku palca, można pomylić palec.
- Przy tej samej skali weryfikacji, dla wizerunku twarzy wartości mieszczą się w przedziale 30-112, a dla odcisku palca w przedziale 40-706.
- Wizerunek twarzy jest często preferowany przez podróżnych ze względu na bezdotykowość.
- Zasadniczo odcisk palca nie zmienia się w czasie, a wizerunek twarzy może się zmieniać.

Podsumowanie

Do właściwych testów podeszło 621 osób, wśród których 31 osób to osoby specjalnie podszywające się pod osobę z cudzym paszportem. Skuteczność z wykorzystaniem dwóch cech biometrycznych (wizerunku twarzy i odcisku palca), rozumiana jako stosunek decyzji poprawnych do wszystkich wynosi 88%. Dla 6% osób system wydał decyzję niepoprawną, a dla 5% nie był w stanie wypracować decyzji, więc zweryfikował to jako przypadki negatywnie. Żadna nieuprawniona osoba nie przeszła pozytywnie weryfikacji.

System był również testowany w logice „i”, czyli obie cechy biometryczne muszą być pozytywnie zweryfikowane, aby decyzja była poprawna. Oznacza to, że liczba błędów jest sumą błędów obu typów weryfikacji, co wraz z jednorazowym sposobem pobierania danych bez powtórek, usprawiedliwia dość wysoką liczbę niepoprawnych decyzji lub ich brak.

W rzeczywistych badaniach systemu liczbę niepoprawnych decyzji można dość łatwo zmniejszyć poprzez zdyscyplinowanie podróżnych, wydłużenie czasu na wykonywanie zdjęć w razie potrzeby, wyświetlenie dodatkowych instrukcji, jeśli system wykryje okulary, włosy lub czapkę, które przeszkadzają przy identyfikacji i wprowadzenie dodatkowej pętli w programie, która po raz drugi nakazywałaby przyłożenie właściwego palca. Drugim ze sposobów zmniejszenia liczby niepoprawnych decyzji jest zastosowanie ważonej logiki „i”, gdzie można zwiększyć skuteczność weryfikacji do 94%. Na skuteczność wpływ ma też zastosowane oprogramowanie weryfikujące firmy Neurotechnology.

Prezentowany system powstał w ramach realizacji projektu rozwojowego na rzecz bezpieczeństwa i obronności państwa DOBR/0017/R/ID1/2012/03, finansowanego przez Narodowe Centrum Badań i Rozwoju, pt. „Usprawnienie procesu odprawy granicznej osób przy wykorzystaniu biometrycznych urządzeń do samokontroli osób i kontroli środków transportu przekraczających granicę zewnętrzną UE”. Liderem projektu i głównym wykonawcą była Wojskowa Akademia Techniczna (Instytut Optoelektroniki). W skład konsorcjum weszła firma Mlabs Sp. z o.o. z Poznania. Gestorem projektu była Polska Straż Graniczna.

Literatura i autorzy

***Autorzy**: dr hab. inż. Norbert Pałka, E-mail: norbert.palka@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa Elżbieta Czerwińska, E-mail: elzbieta.czerwinska@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, prof. dr hab. Mieczysław Szustakowski, E-mail: mieczyslaw.szustakowski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Marek Piszczek, E-mail: marek.piszczek@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Jarosław Młyńczak, E-mail: jaroslaw.mlynczak@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Michał Walczakowski, E-mail: michal.walczakowski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Marcin Kowalski, E-mail: marcin.kowalski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Artur Grudzień, E-mail: artur.grudzien@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Leon Jodłowski E-mail: Jodle2@o2.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Wiesław Ciurapiński E-mail:* wieslaw.ciurapinski@wat.edu.pl*, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Janusz Wróbel, E-mail: janusz.wrobel@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. S. Kaliskiego 2, 00-908 Warszawa, Mikołaj Sobczak, E-mail:* mikolaj.sobczak@mlabs.pl*, MLabs sp. z o.o. ul. Kaliska 21, 61-131 Poznań, Mateusz Nawrocki, E-mail: Mateusz.nawrocki@mlabs.pl, MLabs sp. z o.o. ul. Kaliska 21, 61-131 Poznań, Paweł Hołoweńko, E-mail: pawel.holowienkso@strazgraniczna.pl, Komenda Głowna Straży Granicznej ul. Al. Niepodległości 100, 02-514 Warszawa, Paweł Poźniak, E-mail: pawel.pozniak@strazgraniczna.pl, Komenda Głowna Straży Granicznej ul. Al. Niepodległości 100, 02-514 Warszawa, Szymon Pachla E-mail: szymon.pachla@strazgraniczna.pl, Komenda Głowna Straży Granicznej ul. Al. Niepodległości 100, 02-514 Warszawa.*

LITERATURA

[1] Sarhan S., Alhassan S., Elmougy S., Multimodal Biometric Systems: A Comparative Study, *Arabian Journal For Science And Engineering*, 42,2, [2017], 443-457

[2] Labati R. D., Genovese A., Munoz E., Piuri V. Scotti F. Sforza, G., Biometric Recognition in Automated Border Control: A Survey, *Acm Computing Surveys*, 49, 2(24), [2016].

[3] Rinaldi A., Biometrics' new identity—measuring more physical and biological traits, *EMBO reports*, 17,1, [2017], 22-26

[4] Lumini A., Nanni L., Overview of the combination of biometric matchers, *Information Fusion*, 33, [2017], 71-85

[5] Vinothkanna R., Santhi K., A cross-correlated feature fusion technique for multimodal biometric system, International Journal of Biomedical Engineering and Technology, 23, 2-3-4, [2017], 180-190

[6] del Rio J.S, Moctezuma D., Conde C., de Diego I.M, Cabello E., Automated border control e-gates and facial recognition systems, *Computers & Security*, 62, [2016], 49-72.

[7] "ICAO Document 9303, Part 1, Volume 1 (OCR machine-readable passports)" (PDF). ICAO. Retrieved 21 February 2017.

[8] http://www.neurotechnology.com/