

Norbert PAŁKA¹, Elżbieta CZERWIŃSKA¹, Mieczysław SZUSTAKOWSKI¹, Leon JODŁOWSKI¹, Marek PISZCZEK¹, Jarosław MŁYŃCZAK¹, Michał WALCZAKOWSKI¹, Marcin KOWALSKI¹, Artur GRUDZIEN¹, Wiesław CIURAPIŃSKI¹, Janusz WRÓBEL¹, Jacek OLEJNIK², Bartosz KOŚCIUG², Iwona BADACZEWSKA², Konrad PIOTROWSKI³, Paweł HOŁOWEŃKO⁴, Paweł POŹNIAK⁴, Szymon PACHLA⁴

Instytut Optoelektroniki, Wojskowa Akademia Techniczna (1), JAS Technologie Sp. z o.o. (2), Gemalto Sp. z o.o. (3), Straż Graniczna (4)

doi:10.15199/48.2018.06.21

Demonstrator biometrycznego systemu wjazdu/wyjazdu do strefy Schengen – badania eksperymentalne

Streszczenie. W pracy opisano budowę i podstawowe funkcjonalności biometrycznego demonstratora technologii inteligentnej granicy. Przeprowadzone testy potwierdzają, że aplikacje działają stabilnie, a system poprawnie realizuje wszystkie założone funkcjonalności. W testach rozpoznawania wizerunku twarzy skuteczność działania systemu wynosi 98%. Skuteczność weryfikacji osób na podstawie odcisków czterech palców jest bardzo wysoka (zbliżona do 100%) i warunkowana głównie przez jakość pobranych odcisków palców. Czasy poszczególnych odpraw są akceptowalne i zbliżone do wyników uzyskiwanych w innych badaniach.

Abstract. The paper describes the construction and basic functionalities of the biometric demonstrator of the smart border technology. Carried out tests confirm that the applications are stable and the system correctly implements all assumed functionalities. In the tests of facial image recognition, the effectiveness of the system is 98%. The effectiveness of verification of people based on fingerprints is very high (close to 100%) and conditioned mainly by the quality of finger images. Times of border checks are acceptable and similar to the results achieved in other studies. (**Entry Exit System – research on biometric verification**)

Słowa kluczowe: system wejścia wyjścia, weryfikacja wizerunku twarzy, weryfikacja odcisku palca, biometria.

Keywords: entry exit system, facial image verification, fingerprint verification, biometrics.

Wstęp

Od wielu lat prowadzone są w Unii Europejskiej analizy i prace legislacyjne dotyczące zagadnienia Inteligentnych Granic (ang. Smart Borders - SB), czyli pakietu regulacji oraz rozwiązań technicznych mających na celu usprawnienie i przyspieszenie odprawy granicznej, poprawę zarządzania zewnętrznymi granicami państw członkowskich Schengen, walkę z nielegalną imigracją oraz dostarczenie informacji na temat cudzoziemców bezprawnie przedłużających pobyt. W dniu 6 kwietnia 2016 roku, Parlament Europejski przedstawił projekt pierwszego rozporządzenia z pakietu Smart Borders, który ustanawia system wjazdu/wyjazdu (ang. Entry/Exit System – EES) [1-3]. Wdrożenie systemu planowane jest na rok 2020, a poprzedziły go analizy funkcjonalności i testy na wybranych przejściach granicznych tzw. "Pilot Smart Border" [4]. Według aktualnego stanu prawnego, dopuszczalne jest stosowanie automatycznych bramek kontroli granicznej opartych na technologiach biometrycznych w odniesieniu do obywateli strefy Schengen. Już w latach 2007-2010 zainstalowano takie bramki do obsługi odpraw granicznych na przejściach lotniskowych w Portugalii, Francji, Wielkiej Brytanii, Finlandii, Hiszpanii i Niemiec. W 2012 roku Frontex opublikował rekomendacje dotyczące aspektów technicznych i organizacyjnych systemów automatycznej kontroli granicznej [6,7].

W założeniach system EES będzie przeznaczony dla obywateli spoza strefy Schengen (tzw. państw trzecich - TCN Third Country Nationals), przekraczających granice zewnętrzne w trakcie wjazdu lub wyjazdu ze strefy Schengen. Obejmie on wszystkich podróżnych zarówno tych, którzy przy przekraczaniu granicy zobowiązani są do posiadania wizy (ang. visa holder – VH), jak i podróżnych zwolnionych z obowiązku wizowego (ang. visa exempt – VE). Bazę danych stanowi rejestr osobowy oraz rejestr przekroczeń granicy. W rejestrze osobowym przechowywane są dane osobowe, dane dokumentu podróży oraz informacje o odmowie wjazdu, przekroczeniach czasu pobytu oraz dane biometryczne (wizerunek twarzy, odciski 4 palców prawej dłoni bez kciuka). Rejestr wizowy (VIS) i baza EES są zintegrowane i

w przypadku osób posiadających wizę, baza EES wykorzystuje dane zgromadzone w rejestrze wizowym.

Tożsamość podróżnego ustalana jest na podstawie cech biometrycznych przechowywanych w rejestrze osobowym bazy EES. Jeśli przy przekraczaniu granicy przez podróżnego okaże się, że w bazie EES nie ma jego rejestru osobowego (przekracza granicę po raz pierwszy), funkcjonariusz Straży Granicznej tworzy jego rejestr osobowy. Do ustalenia tożsamości podróżnego zarejestrowanego w bazie EES wymagana jest zgodność jednej cechy biometrycznej. W pierwszej kolejności weryfikowany jest wizerunek twarzy, a w przypadku braku dostatecznej zgodności - odciski palców. Każdorazowe przekroczenie granicy odnotowywane jest w rejestrze przekroczeń skojarzonym z rejestrem osobowym. Na podstawie danych z rejestru przekroczeń ustalany jest status podróżnego w zakresie legalności pobytu.

Wprowadzenie EES umożliwi zastosowanie w pełni automatycznej i półautomatycznej (kioski samoobsługowe) odprawy granicznej. Przy każdym przekroczeniu granicy przeszukiwane są unijne (SIS II), jak i krajowe bazy bezpieczeństwa, pod kątem zidentyfikowania osób poszukiwanych i zagrażających bezpieczeństwu Unii Europejskiej, baza dokumentów skradzionych i utraconych (SLTD), a także inne bazy Europolu i Interpolu.

Koncepcja EES została wstępnie sprawdzona na wybranych przejściach granicznych strefy Schengen ("Pilot Smart Border"), między marcem a listopadem 2015 roku [4]. W badaniach dokonano sprawdzenia możliwości technicznych wykorzystania cech biometrycznych do weryfikacji tożsamości podróżnych. Badaniem objęto 18 przejść granicznych, w 12 krajach strefy Schengen. Przebadano około 58 000 podróżnych. Jako wzorce biometryczne identyfikacji i weryfikacji podróżnych przebadano odciski palców (4, 8 i 10 palców) i wizerunek twarzy. Przebadano również wpływ elementów automatyki - bramki ABC i kioski samoobsługowe na usprawnienie procesu odprawy.

W testowanych systemach przedmiotem badań było pobieranie obrazu twarzy na żywo oraz weryfikacja tożsamości z wykorzystaniem obrazu przechowywanego w chipie dokumentu podróży. Pobieranie obrazu twarzy z

chipa nie przekraczało 3,5 sekundy, a pobieranie obrazu z kamery na żywo średnio zajmowało 5,5 sekundy. W przypadku pobrania obrazu twarzy o wymaganej jakości weryfikacja tożsamości trwała mniej niż jedną sekundę. Z tego powodu w dokumencie końcowym przyjęto jako wystarczającą weryfikację tożsamości na podstawie wizerunku twarzy. Największa zaobserwowana sprawność weryfikacji przy użyciu wizerunku twarzy nie przekraczała 93% (lit [4] str. 9), a jako bardzo dobry rekomendowano poziom 75%. W przypadku weryfikacji tożsamości na podstawie odcisków palców sprawność jest znacznie wyższa i już dla czterech palców (porównanie z własnymi odciskami umieszczonymi w bazie) osiąga wartość bliską 100%. Jednak średni czas skanowania dla skanerów "czteropalcowych" wahał się od 17 do 21 sekund, a dla "dwupalcowych" wynosił 34 sekundy (lit [4] str. 8). W czytnikach „czteropalcowych”, wszystkie palce skanowane są jednocześnie - w tym samym czasie. W czytnikach „dwupalcowych” skanowane są najpierw pierwsze dwa wskazane palce. Wyniki skanowania wysyłane są do programu i weryfikowane, pod względem jakości pobranego zdjęcia, a następnie skanowane są kolejne palce. Ostatecznie uznano, że jeśli czas skanowania odcisków palców nie przekracza 30 sekund, to nie opóźnia to istotnie odprawę osób i może być zaakceptowany.

Polska posiada wiele przejść lotniczych oraz długą granicę lądową, która jest jednocześnie granicą strefy Schengen i dlatego kwestie odpraw granicznych oraz nowych uregulowań prawnych są traktowane priorytetowo. W związku z tym równoległe z pracami UE, Polska Straż Graniczna ogłosiła projekt rozwojowy NCBiR dotyczący Inteligentnych Granic i systemu EES, który zrealizowało wybrane w konkursie konsorcjum naukowo-przemysłowe pod przewodnictwem WAT. Głównymi celami projektu była budowa demonstratora technologii inteligentnej granicy (DTIG), demonstracja funkcjonalności pakietu Smart Borders (procesy, przepływ informacji) oraz stworzenie platformy badawczej pod przyszłe projekty. Oprócz wytycznych europejskich system obsługuje także specyficzny dla Polski mały ruch graniczny – jest to bezwizowy ruch dla osób zamieszkujących strefę przygraniczną i posiadających kartę małego ruchu granicznego (MRG).

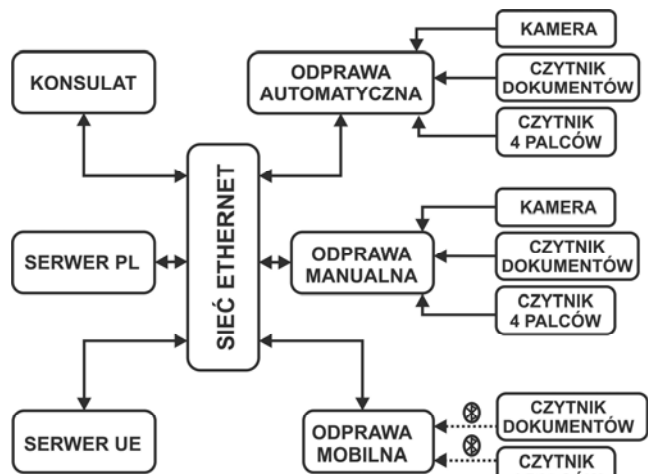
Niniejszy artykuł opisuje budowę i podstawowe funkcjonalności opracowanego demonstratora. Jednakże podstawowym celem niniejszej pracy jest analiza działania systemu pod kątem sprawności biometrycznej weryfikacji tożsamości podróżnych. Dla tego celu opracowano i wykonano testowy zestaw paszportów biometrycznych. W pracy poddano badaniom skuteczność weryfikacji podróżnego za pomocą wizerunku twarzy, jak i odcisków palca na różnych stanowiskach. Zbadano także bardzo ważny parametr, a mianowicie czas odprawy.

Demonstrator technologii inteligentnej granicy (DTIG)

Zbudowany DTIG (rys. 1), składa się z czterech stanowisk roboczych: konsulatu, odprawy manualnej, odprawy automatycznej, odprawy mobilnej oraz dwóch serwerów (Serwer-PL, Serwer-UE).

Z punktu widzenia rozpatrywanych badań i działania systemu najważniejsze są zastosowane czytniki. I tak w odprawie stacjonarnej i automatycznej do akwizycji wizerunku twarzy zastosowano kamerę Microsoft LifeCam Cinema HD o rozdzielczości 1280 x 720 pikseli wraz z oświetlaczem diodowym. Jako czytnik palców zastosowano stacjonarny nabiurkowy czytnik odcisków czterech palców Dermalog LF10, o rozdzielczości optycznej 500 dpi zapewniającej jakość obrazu zgodną z FBI IAFIS IQS certyfikat Dodatek F [8]. Do porównywania wizerunku

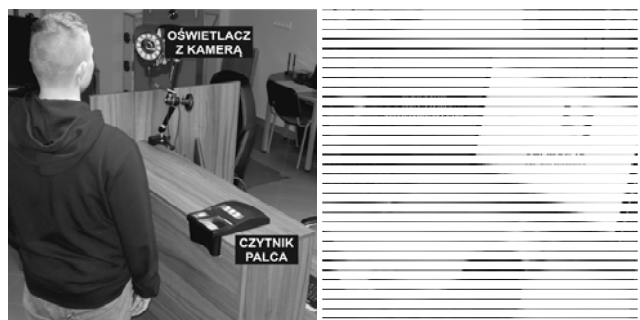
twarzy i odcisków palców służy oprogramowanie MegaMatcher firmy Neurotechnology [5]. Za odczyt danych z dokumentów odpowiada czytnik Regula 7028M spełniający stosowne wymagania [6]. W odprawie manualnej kamera jest umieszczona na regulowanym przez operatora wysięgniku. Przy odprawie automatycznej kamerę umieszczono na monitorze, a jej wysokość podróżny mógł ustawiać samodzielnie.



Rys. 1. Schemat demonstratora technologii inteligentnej granicy (DTIG).

Odprawy mobilne to odprawy graniczne realizowane w środkach transportu (pociągi, autobusy), a także na terenie otwartym (parkingi, miejsce odpraw specjalnych). Wymaga to nie tylko zastosowania bezprzewodowej transmisji danych, ale także sprzętu mobilnego (specjalne laptopy, inne skanery linii papilarnych i czytniki dokumentów).

Ponieważ w warunkach odprawy mobilnej trudno jest zapewnić właściwą jakość wizerunku twarzy (problemy z pozycjonowaniem kamery, oświetleniem, warunkami klimatycznymi itp.), do identyfikacji podróżnego wykorzystuje się tylko odciski palców. Odciski palców rejestruje czytnik pojedynczego palca Ibis firmy Morpho o rozdzielczości 500 dpi. Czytnik dokumentów Vicomp VPR-460e pobiera dane z paszportów. Oba czytniki komunikują się z systemem bezprzewodowo interfejsem bluetooth.



Rys. 2. Widok stanowiska odprawy manualnej od strony podróżnego (po lewej) oraz od strony operatora (po prawej).

Łączność między elementami DTIG odbywa się za pomocą przewodowej i bezprzewodowej sieci LAN. Każde z wymienionych stanowisk posiada własne oprogramowanie (aplikacje), które umożliwiają spełnienie wymagań stawianych systemowi inteligentnej granicy.

Na rys. 2 przedstawiono zdjęcia stanowiska odprawy manualnej, która jest odprawą pierwszej linii, przez którą podróżny może zarówno wejść, jak i wyjść ze strefy Schengen. Tutaj podróżny podaje dokumenty operatorowi,

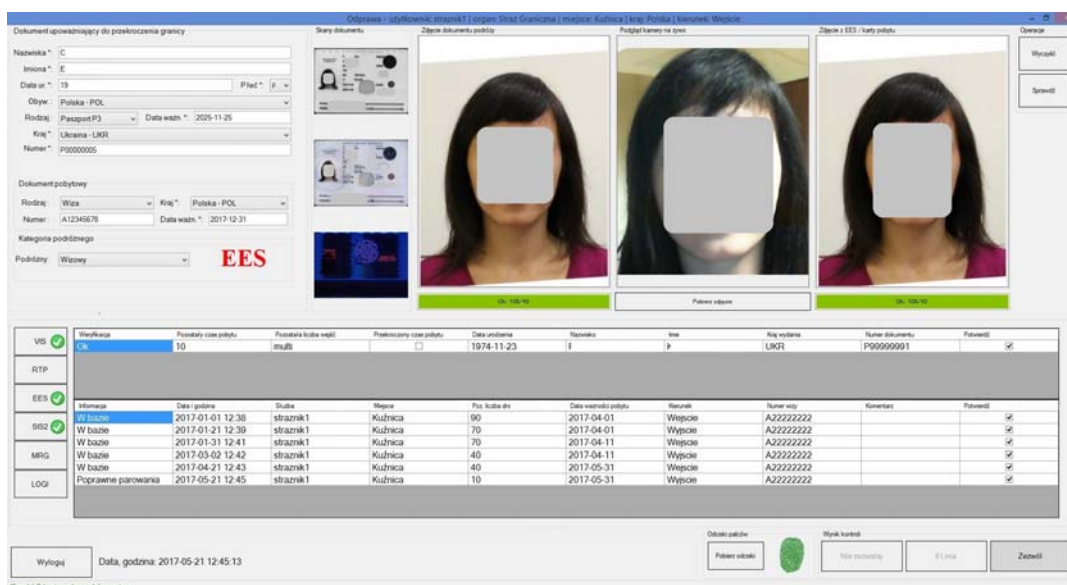
a on wydaje mu polecenia, aby patrzył w kamerę lub przyłożył wybrane palce do czytnika linii papilarnych. W pierwszym kroku operator przykłada dokument podróży (paszport, karta MRG) i ewentualnie dokument pobytowy (karta pobytu, wiza) do czytnika, a w aplikacji *CheckIn* automatycznie ukazują się dane podróznego odczytane z dokumentu podróży. W tle program sprawdza poprawność i spójność danych. W następnym kroku pobierany jest wizerunek twarzy podróznego za pomocą kamery. Obraz ten jest weryfikowany z wizerunkiem pobranym z paszportu. Dla podróznego kategorii TCN+VH, TCN+VE pobierane są cztery odciski palców, a dla MRG tylko jeden. Dla pozostałych kategorii nie pobiera się odcisków palców. „Paczka” danych składająca się z danych osobowych i biometrycznych jest wysyłana do odpowiednich baz danych w celu ich weryfikacji. Na poszczególnych stanowiskach dane wysyłane są siecią Ethernet do Serwerów poprzez aplikację Smart Border. Odpowiedzi z baz danych z Serwerów przesyłane są do stanowisk sieci Ethernet i widoczne są w aplikacji Smart Border. Dane powracające do aplikacji Smart Border zawierają informacje o weryfikacji podróznego w bazach, ewentualnych zastrzeżeniach i pozostałej liczbie dni do wykorzystania w strefie Schengen i

są wizualizowane na ekranie monitora. Operator podejmuje ostateczną decyzję – zezwól na przejście, nie zezwalaj na przejście, skieruj na II linię odprawy, gdzie przeprowadza się bardziej szczegółowe badania.

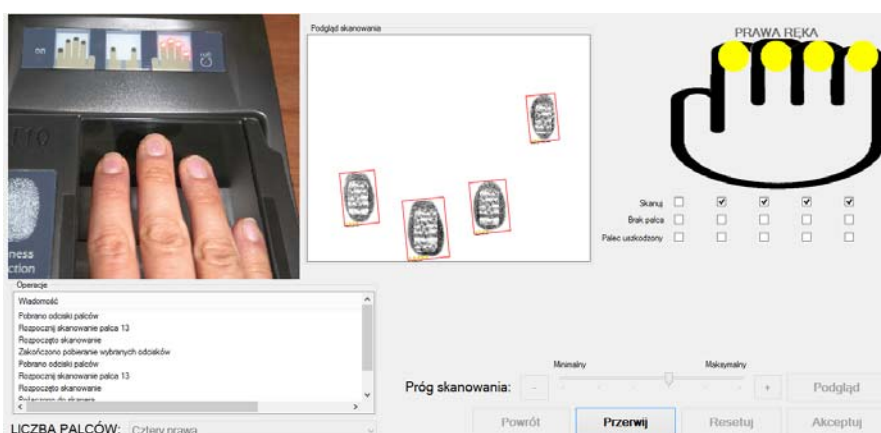
Podobnie działa stanowisko odprawy mobilnej z tą różnicą, iż nie pobiera się w nim wizerunku twarzy od podróznego, a pobieranie odcisków palców odbywa się jeden po drugim.

Stanowisko odprawy automatycznej zostało wzorowane na istniejących systemach automatycznej kontroli wykorzystywanych w wielu krajach UE do kontroli obywateli strefy Schengen. Stanowisko odprawy automatycznej działa podobnie do stanowiska odprawy manualnej. Różnica jest taka, iż podróżny postępuje wg instrukcji wyświetlanych na ekranie monitora, a operator nadzoruje proces odprawy i może zaangażować w proces odprawy, kierując podróznego do odprawy manualnej.

Zadaniem Konsulatu jest wydawanie wizy dla "obywateli" TCN+VE - pobranie i przesłanie danych osobowych i biometrycznych do bazy VIS (wizerunek twarzy i odcisków 10 palców).



Rys. 3. Widok okna aplikacji *CheckIn* – okno główne aplikacji z danymi podróznego.



Rys. 4. Okno aplikacji do pobierania odcisków palców oraz zdjęcie palców przyłożonych do czytnika.

Oprogramowanie

Wszystkie aplikacje zostały napisane w języku C# przy wykorzystaniu platformy .NET oraz środowiska programistycznego Visual Studio 2015. Wykonano

dokładny spis bibliotek, API, SDK oraz dodatkowych narzędzi użytych przy implementacji oprogramowania aplikacji Smart Borders. Do implementacji struktury relacyjnej baz danych wykorzystano strukturalny język

zapytań SQL, który służy do tworzenia modyfikowania oraz przeszukiwania baz danych. Jako narzędzie zarządzania bazami danych wybrano *SQL Management Server*, który grupuje, zabezpiecza i umożliwia wykonywanie podstawowych operacji na bazach danych.

Główne okno aplikacji *CheckIn* zaprezentowane jest na rys. 3. W lewym górnym rogu znajdują się dane osobowe podróżnego odczytane z paszportu. Obok są umieszczone zdjęcia paszportu wykonane w świetle widzialnym, podczerwieni i UV. System automatycznie sprawdza, czy paszport nie został sfalszowany. Pierwsze zdjęcie z lewej przedstawia wizerunek twarzy podróżnego odczytany z chipa paszportu. W środku znajduje się zdjęcie podróżnego zarejestrowane „na żywo”. Zdjęcie po prawej pochodzi z bazy danych EES. Poniżej na zielonych paskach znajduje się wynik weryfikacji – system określa poziom zgodności pomiędzy wizerunkiem zrobionym „na żywo” a wizerunkami referencyjnymi. Jeśli wynik weryfikacji jest poniżej progu – pasek zmienia kolor na czerwony.

W dolnej części okna aplikacji znajdują się odpowiedzi z baz danych wraz z informacjami o wydanych wizach, zastrzeżeniach w bazie SIS oraz historią wejść/wyjść. Wynik porównania odcisków palców jest zaznaczony zieloną lub czerwoną ikoną na dole okna.

Rysunek 4 przedstawia obsługę procesu pobierania odcisków palców. Podróżny przykładą dłoń do czytnika odcisków palców (Dermalog LF10), a aplikacja wyświetla zarejestrowane odciski. Dłoń w prawej części ekranu pokazuje, które palce należy przyłożyć. Suwakiem umieszczonym w prawym dolnym rogu można zmieniać próg skanowania, czyli ustawiać akceptowalną jakość rejestrowanych odcisków palców. Dane wrażliwe zostały przysłonięte.

Rodzaje podróży i dokumentów

Badania DTIG przeprowadzono symulując proces przekraczania granicy przez pięć kategorii podróżnych pochodzących: ze strefy Schengen, państwa trzeciego (TCN) z kartą pobytu, TCN z kraju bezwizowego (TCN+VE), TCN z kraju wizowego (TCN+VH) oraz kartą małego ruchu granicznego (MRG). W trakcie odprawy granicznej przeszukiwano bazę SIS II w odniesieniu do wszystkich podróżnych, obywatele TCN+VH byli sprawdzani w bazie VIS, a obywatele TCN+VH i TCN+VE w bazie EES. Obywatele z kartą MRG byli sprawdzani w bazie MRG. Na potrzeby badań wykonano w pełni funkcjonalne dokumenty biometryczne. Przykładowy paszport obywatela TCN zaprezentowany jest na rys. 5. Jest to paszport z chipem zawierającym dane biometryczne, ale spersonalizowany dla jednego z członków zespołu badawczego.



Rys. 5. Zdjęcie pierwszej strony przykładowego paszportu wytworzonego na potrzeby badań.

Testy funkcjonalne przeprowadzono wykorzystując 10 paszportów i 10 kart MRG wytworzonych na potrzeby badań (1 kobieta, 9 mężczyzn) oraz 113 oryginalnych

paszportów polskich i 7 zagranicznych (38 kobiet i 82 mężczyzn). Większe zróżnicowanie ze względu na kraj pochodzenia uzyskano zmieniając ustawienia w aplikacji tak, że osoby z paszportem polskim były traktowane jako osoby z poza strefy Schengen (TCN VE lub TCN VH).

Testy funkcjonalne

Prezentowany DTIG umożliwia m.in. biometryczną weryfikację podróżnego w bazach danych, automatycznie wylicza ilość dni pozostałych do wykorzystania w strefie Schengen, uzupełnia pary wejścia/wyjścia. Przy pierwszym przekraczaniu granicy dane osobowe i biometryczne podróżnych TCN+VH, TCN+VE są zapisywane w rejestrze osobowym bazy EES, a dane o każdorazowym przekroczeniu granicy zapisywane w rejestrze przekroczeń bazy EES. Przy kolejnych przekroczeniach granicy funkcjonariusz SG może przeglądać i weryfikować historię wejść/wyjść odprawianego podróżnego.

Podłączony do systemu duży ekran wizualizuje sytuację na przejściu granicznym, pokazując funkcjonowanie poszczególnych komponentów.

Weryfikacja funkcjonalności DTIG odbywała się zgodnie z opracowanymi scenariuszami zakładającymi różne przypadki, uwzględniając zarówno poprawne przekroczenia granicy, jak i sytuacje w których należało podjąć inne czynności wynikające z Kodeksu Granicznego Schengen.

W wyniku przeprowadzonych testów stwierdzono, że działanie aplikacji na wszystkich stanowiskach jest stabilne, a system poprawnie realizuje wszystkie założone funkcjonalności.

W przypadku odprawy manualnej i automatycznej czas pomiędzy przyłożeniem paszportu do czytnika a wyświetleniem informacji w aplikacji funkcjonariusza SG wynosi średnio 6 sek. Dla odprawy mobilnej czas ten rośnie do 7 sek., co prawdopodobnie jest spowodowane zastosowaniem interfejsu bluetooth.

W tabeli 1 podano średnie czasy odprawy na poszczególnych stanowiskach przy badaniu różnych dokumentów. Najkrócej trwa odprawa dla paszportu Schengen i TCN z kartą pobytu, gdyż sprawdzamy tylko bazę SIS. Najdłużej operacja trwa dla TCN z wizą, bowiem należy dodatkowo wpisać wizę i sprawdzić bazę VIS. W przypadku odprawy mobilnej nie jest pobierany wizerunek twarzy na żywo, co mogłoby sugerować, że czas odprawy powinien być najkrótszy. Jednak tak nie jest, ponieważ w tym przypadku dane dotyczące wizy (numer, data ważności, kraj wydania) wprowadzane są ręcznie, a palce są skanowane pojedynczo jeden po drugim.

Tabela. 1. Czas odprawy w sekundach dla różnych typów dokumentów i różnych stanowisk.

Odprawa	Paszport Schengen	TCN + karta pobytu	TCN+VH	TCN+VE	MRG
Manualna	17 ± 5	20 ± 5	37 ± 10	24 ± 5	28 ± 6
Automatyczna	28 ± 8	32 ± 6	34 ± 8	30 ± 5	35 ± 10
Mobilna	14 ± 2	22 ± 2	90 ± 15	42 ± 3	39 ± 2

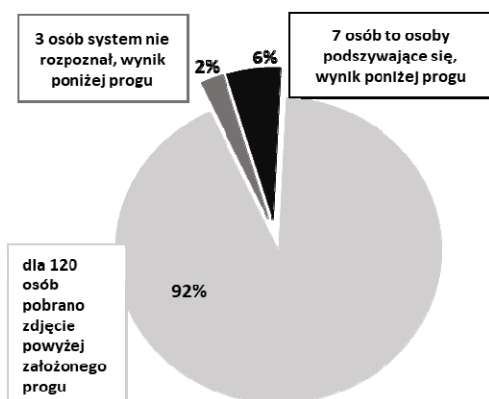
Biometryczna weryfikacja wizerunku twarzy

Badania przeprowadzono na grupie 130 osób, wśród których było 7 osób podszywających się, czyli osób posługujących się cudzym paszportem. W pierwszym etapie badań skanowano dokumenty podróży. Czytnik przesyłał dane do aplikacji i formularze automatycznie wypełniały się danymi osobowymi. Z dokumentu było pobierane zdjęcie wizerunku twarzy, zapisane w formie

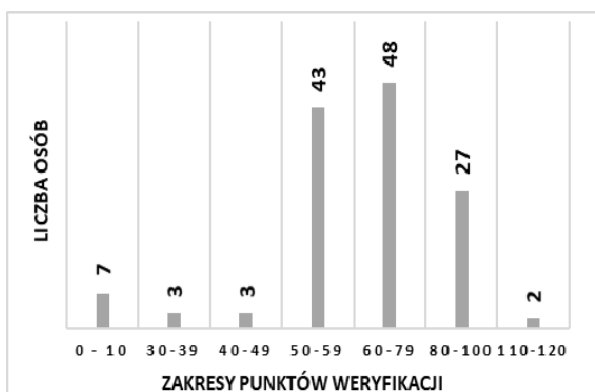
elektronicznej i wyświetlane było w lewym oknie aplikacji (rys. 3). Następnie było pobierane zdjęcie wizerunku twarzy „na żywo”. Dla odprawy manualnej system pobierał zdjęcie twarzy i porównywał ze wzorcem. Średni czas weryfikacji twarzy wynosił 4 sek. Natomiast w przypadku odprawy automatycznej osoba miała 5 sekund na zajęcie prawidłowej postawy. Następnie rozpoczynała się weryfikacja wizerunku twarzy, która trwała średnio 2 sek. Jeśli nie udało się pobrać wizerunku i przekroczono czas odprawy, należało powtórzyć procedurę od początku.

Zdjęcia pobrane „na żywo” zostały porównane ze zdjęciami odczytanym z chipu dokumentu podróży. Próg weryfikacji ustawiono na 40 punktów, co odpowiada prawdopodobieństwu fałszywej akceptacji nieuprawnionej osoby (FAR – False Acceptance Rate) poniżej 0,1%.

Spośród 130 osób, które wzięły udział w testach (patrz rys. 6), od 120 osób poprawnie pobrano zdjęcie wizerunku twarzy „na żywo” i dla tych osób uzyskano wynik weryfikacji powyżej progu 40 pkt, czyli zostały poprawnie zweryfikowane. Dla wszystkich siedmiu osób podrywających się wynik weryfikacji był dużo poniżej progu (w przedziale 0 - 10), a więc system podał poprawną decyzję - weryfikacja negatywna. Pozostałe trzy osoby miały własne dokumenty, ale celowo lub nieświadomie przyjęły złą pozycję przed kamerą: albo ich twarze były nieodpowiednio skierowane, albo uśmiechały się lub mrugały oczami. System wykrył pewne podobieństwo mieszczące się w przedziale 30-39 punktów, ale nie przekraczało ono założonego progu, więc z punktu widzenia skuteczności systemu, wydał on niepoprawną decyzję.



Rys. 6. Weryfikacja na podstawie wizerunku twarzy – reprezentacja procentowa i liczbowa.



Rys. 7. Weryfikacja na podstawie wizerunku twarzy – liczba osób w poszczególnych przedziałach.

Na rys. 7 przedstawiono wykres prezentujący, ile osób miało wynik w poszczególnych przedziałach punktów weryfikacji. Najwięcej osób mieści się w przedziale 60-79 punktów. Jedynie dla 2 osób udało się uzyskać wynik z

przedziału 110-120 punktów. Trzy osoby, których system nie rozpoznał poprawnie, mają wynik lekko poniżej progu 30-39 punktów. Skuteczność systemu rozumiana jako liczba decyzji poprawnych do wszystkich decyzji, dla rozpoznawania wizerunku twarzy wynosi zatem $(127/130) \cdot 100\% = 98\%$.

Biometryczna weryfikacja odcisków palców

Ze względu na fakt, iż w systemie EES należy weryfikować podróżnego na podstawie odcisków czterech palców, w pracy zrezygnowano z analizy liczbowych wyników dla poszczególnych palców, a skupiono się na całościowym wyniku weryfikacji w kategorii pozytywna/negatywna. Próg weryfikacji ustawiono na 40 punktów, co odpowiada prawdopodobieństwu fałszywej akceptacji nieuprawnionej osoby (FAR – False Acceptance Rate) poniżej 0,1%. Przy tych wartościach progu weryfikacji i progu skanowania 4 nie stwierdzono błędnej weryfikacji podróżnego.

Dla odprawy manualnej testowano wpływ progu skanowania (rys. 4) na działanie systemu. W tym przypadku przetestowano ponad 100 osób, a wyniki wskazują, że optymalnym progiem skanowania jest wartość 4. Poniżej tego progu jakość odcisku palca może być niewystarczająca i może prowadzić do pojedynczych przypadków weryfikacji negatywnej. Powyżej tego progu zdarza się, że czytnik nie może pobrać odcisku o zadanej jakości i prosi ponownie o przyłożenie jednego lub kilku palców. Jest to operacja znacznie wydłużająca proces odprawy. Dla ustawień suwaka od 1 do 4 czas skanowania 4 palców wynosi 3-4 sekund. Dla progu 5 - 6 czas ten rośnie nieznacznie do 4-5 sekund, ale wzrasta ilość niezaakceptowanych skanowań.

Dla odprawy mobilnej i progu 1 - 5, niezależnie od liczby palców, czas od przyłożenia palca do pobrania przez czytnik jednego odcisku, wynosił 3 sekundy. Czasami (około 1 raz na 50 skanów) wymagana była poprawka ułożenia trwająca 1-2 sek., która wynikała z faktu, iż czytnik jest trzymany w ręku przez operatora. Czas transferu zdjęcia odcisku palca po bluetooth wynosił ok. 9 sek., co daje łącznie 12 sek. (+/-2 sek.). Dla progu 6 czas skanowania palca przez czytnik wynosił także 3 sek., natomiast czas odbioru to ok. 10 sek., co daje łącznie 13 sek. Również w tym przypadku wybrano próg 4 jako optymalny.

Podsumowanie

W pracy opisano budowę i podstawowe funkcjonalności demonstratora technologii inteligentnej granicy. Przeprowadzone testy potwierdzają, że aplikacja działa stabilnie, a system poprawnie realizuje wszystkie założone funkcjonalności. W testach rozpoznawania wizerunku twarzy wzięły udział 123 osoby z własnymi paszportami oraz 7 osób posługujących się paszportami innej osoby. Skuteczność weryfikacji tożsamości wynosiła 98% i jest nieznacznie wyższa niż uzyskana w testach pilota Smart Border. Skuteczność weryfikacji osób na podstawie odcisków czterech palców jest bardzo wysoka i warunkowana głównie przez jakość pobranych odcisków palców. Próg skanowania 4 - 6 jest optimum pomiędzy jakością i czasem skanowania palca. Czasy poszczególnych odpraw są akceptowalne i zbliżone do wyników uzyskiwanych w Pilocie [4].

Prezentowany system powstał w ramach realizacji projektu rozwojowego na rzecz bezpieczeństwa i obronności państwa DOB-BIO6/07/40/2014, finansowanego przez Narodowe Centrum Badań i Rozwoju, pt. „Opracowanie środowiska do wdrożenia koncepcji Smart

Borders". Liderem projektu była Wojskowa Akademia Techniczna (Instytut Optoelektroniki). W skład konsorcjum weszła firma Jas Technologie Sp. z o.o. oraz Gemalto Sp. z o.o. Gestorem projektu była Polska Straż Graniczna.

Autorzy: dr hab. inż. Norbert Pałka, E-mail: norbert.palka@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa
Elżbieta Czerwińska, E-mail: elzbieta.czerwinska@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, prof. dr hab. Mieczysław Szustakowski, E-mail: mieczyslaw.szustakowski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Leon Jodłowski E-mail: Jodle2@o2.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908, Marek Piszczek, E-mail: marek.piszczek@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Jarosław Młyńczak, E-mail: jaroslaw.mlynczak@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Michał Walczakowski, E-mail: michal.walczakowski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Marcin Kowalski, E-mail: marcin.kowalski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Artur Grudzień, E-mail: artur.grudzien@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Wiesław Ciurapiński E-mail: wieslaw.ciurapinski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Warszawa, Wiesław Ciurapiński E-mail: wieslaw.ciurapinski@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Janusz Wróbel, E-mail: janusz.wrobel@wat.edu.pl, Wojskowa Akademia Techniczna, Instytut Optoelektroniki, ul. W. Urbanowicza 2, 00-908 Warszawa, Jacek Olejnik, E-mail: jacek.olejnik@jastechnologie.pl, Jas Technologie sp. z o.o., ul. Modularna 3a, 02-238 Warszawa, Bartosz Kościąg, E-mail: bartosz.kosciug@jastechnologie.pl, Jas Technologie sp. z o.o., ul.

Modularna 3a, 02-238 Warszawa, Iwona Badaczewska, E-mail: iwona.badaczewska@jastechnologie.pl, Jas Technologie sp. z o.o., ul. Modularna 3a, 02-238 Warszawa, Konrad Piotrowski, E-mail: konrad.piotrowski@gemalto.com, Gemalto sp. z o.o., 83-110 Tczew, ul. Skarszewska 2, Paweł Hołowieńko, E-mail: pawel.holowienko@strazgraniczna.pl, Komenda Główna Straży Granicznej ul. Al. Niepodległości 100, 02-514 Warszawa, Paweł Poźniak, E-mail: pawel.pozniak@strazgraniczna.pl, Komenda Główna Straży Granicznej ul. Al. Niepodległości 100, 02-514 Warszawa, Szymon Pachła E-mail: szymon.pachla@strazgraniczna.pl, Komenda Główna Straży Granicznej ul. Al. Niepodległości 100, 02-514 Warszawa.

LITERATURA

- [1] "Kodeks graniczny Schengen" Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r.
- [2] „Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie 2016/399 z dnia 9 marca 2016 r w zakresie korzystania z systemu wjazdu /wyjazdu (EES)” 2016/105 z dnia 6.4.2016.
- [3] „Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające system wjazdu/wyjazdu w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich i danych dotyczących odmowy wjazdu w odniesieniu do obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich Unii Europejskiej oraz określające warunki dostępu do systemu wjazdu/wyjazdu na potrzeby ścigania” z dnia 6.4.2016, Komisja EU 2016/0106 (COD), Bruksela.
- [4] "Smart Borders Pilot Project Report on the technical conclusions of the Pilot", November 2015, PWC.
- [5] <http://www.neurotechnology.com/>
- [6] "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", 31.8.2012, Frontex.
- [7] „Best Practice Operational Guidelines for Automated Border Control (ABC) Systems” 31.8.2012, Frontex.
- [8] <https://www.fbibiospecs.cjis.gov/certifications>