BIOMETRIA MOBILNA. PERSPEKTYWY I WYZWANIA

Agata Giełczyk

1. WSTĘP

W dzisiejszych czasach każdy człowiek musi zapamiętać olbrzymią liczbę loginów, numerów PIN oraz haseł. Są one niezbędne do sprawdzania skrzynki mailowej, korzystania z bankowości elektronicznej, ale również do otwierania domofonu wielu klatek schodowych. Rozwój technologii może spowodować, że za jakiś czas w ogóle nie będzie to konieczne. Jest możliwy bowiem inny sposób weryfikacji użytkowników – biometria. Pozwala ona na użycie tego, „czym jesteśmy" zamiast tego „co pamiętamy" lub „co posiadamy" w procesie przyznawania lub odmawiania dostępu do danych lub zasobów objętych ochroną [Jain 2004]. Biometria zajmuje się mierzeniem organizmów żywych. Chociaż zazwyczaj jest rozumiana jako nauka jedynie o rozpoznawaniu i identyfikacji osób, może też być stosowana do identyfikacji bydła czy owadów.

Z drugiej strony w dzisiejszych czasach niemal każdy ma telefon komórkowy. Według statystyk opracowanych przez Międzynarodowy Związek Telekomunikacyjny (ang. International Telecommunication Union – ITU), w krajach wysoko rozwiniętych liczba aktywnych telefonów przekroczyła już wielkość populacji. Ma to związek z faktem posiadania przez sporą część osób więcej niż jednego aktywnego telefonu komórkowego. Smartfony, które są najbardziej popularnymi telefonami, już dawno przestały być jedynie urządzeniami do dzwonienia. Są wykorzystywane w praktycznie każdej strefie życia, np.: odbieranie i wysyłanie wiadomości elektronicznych, monitorowanie treningów, diety, planowanie wesela czy płatności mobilne. W związku z tak licznym zastosowaniem, przechowują one coraz to większą liczbę danych wrażliwych, których utrata byłaby bardzo kosztowna i kłopotliwa dla właściciela. Zastosowanie biometrii podczas odblokowania telefonu czy próbie dostępu do wybranej aplikacji może zabezpieczyć wrażliwe dane przechowywane w pamięci telefonu, a także odciążyć samego użytkownika. Nie będzie on bowiem musiał pamiętać skomplikowanego hasła do telefonu, a dostęp do swoich danych dostanie na przykład, gdy przyłoży palec do czytnika.

2. BIOMETRIA

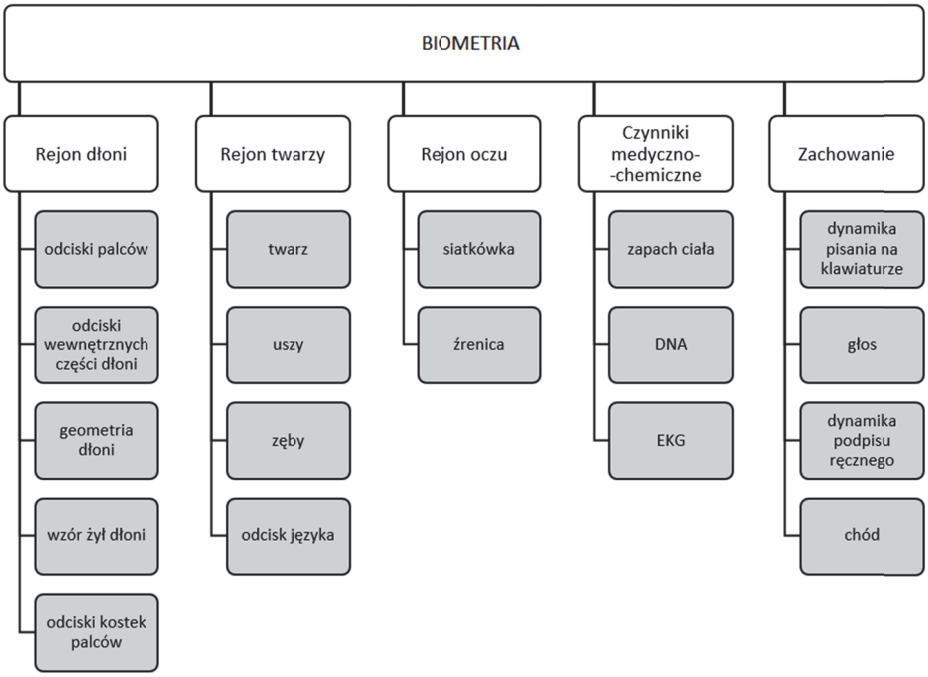
Z racji rosnącej popularności biometrii jej podział, który przedstawia Rys. 1, jest dość szeroki. Oczywistym wydaje się fakt, iż niektóre z cech biometrycznych są częściej wykorzystywane, a inne rzadziej. Mają też różne zastosowania.

Pierwszym stosowanym śladem biometrycznym był odcisk palca [Jain i in. 2016]. Historia jego użycia sięga końca XIX wieku, kiedy to po raz pierwszy został użyty do rozpoznania sprawcy przestępstwa. Jednak na automatyczne systemy rozpoznające osoby po odciskach palców należało czekać aż do 1963 roku, w którym Michell Trauring opublikował swój artykuł na ten temat. Następnie systemy te zostały zaimplementowane przez FBI i do dziś są bardzo ważnym elementem walki z przestępczością. Obecnie odcisków palców nie stosuje się jednak wyłącznie w kryminalistyce. W ich

Uniwersytet Technologiczno-Przyrodniczy, Wydział Telekomunikacji, Informatyki i Elektrotechniki, Zakład Techniki Cyfrowej, Al. prof. S. Kaliskiego 7, 85-796 Bydgoszcz,
e-mail: agata.gielczyk@utp.edu.pl

czytniki są wyposażone telefony, a poprawna weryfikacja użytkownika pozwala na odblokowanie urządzenia, logowanie do aplikacji lub potwierdzenie przelewu podczas wykonywania operacji bankowości mobilnej.

Innym śladem biometrycznym jest twarz, która jest wykorzystywana przez każdego człowieka w sposób naturalny. Właśnie tak poznajemy naszych znajomych czy rodzinę. Pierwsze próby przeniesienia tego schematu do pamięci komputera zostały podjęte w latach 60. XX wieku. Za pierwszy w pełni automatyczny system rozpoznawania twarzy uważa się ten zaproponowany przez Takeo Kanade w jego rozprawie doktorskiej opublikowanej w 1973 roku. Rozpoznawanie twarzy zostało również zaimplementowane w systemach mobilnych. Pierwszą taką próbę podjęli twórcy Androida w wersji 4.0, który zadebiutował na rynku 19 października 2011 roku. Niestety implementacja ta była bardzo prosta do oszukania – wystarczyło przed przednim aparatem telefonu umieścić zdjęcie właściciela i telefon odblokowywał się. W późniejszych wersjach tego systemu wprowadzono dalsze zabezpieczenia, np. konieczność mrugnięcia w wyznaczonym czasie.



Rys. 1. Podział biometrii [Unar i in. 2014]

Inną bardzo ważną cechą biometryczną jest tęczówka oka. Znalazła ona swoje zastosowanie m.in. podczas kontroli paszportowych w krajach na całym świecie, kontroli pasażerów na największych portach lotniczych czy narodowych systemach identyfikacji obywateli (Indie, Meksyk). W rozwoju tęczówki jako cechy biometrycznej podstawową rolę pełnił rozwój urządzeń do pobierania próbek. Pierwsze takie urządzenia były bardzo drogie, nieporęczne i wymagały sporego doświadczenia od osoby, która miała pobierać próbki. Zazwyczaj wszystkie potrzebne do rozpoznania elementy tęczówki są widoczne w świetle tzw. bliskiej podczerwieni (ang. NIR), o zakresie 0,8 -2,5 μm długości.

Aby dana cecha mogła być używana jako ślad biometryczny, powinna spełniać cztery podstawowe wymagania. Przede wszystkim musi być uniwersalna, czyli posia-

dana przez każdego użytkownika podlegającego rozpoznaniu. Musi również być odmienna, czyli różnić się dla każdej z osób. Najlepiej byłoby, gdyby była różna nawet w przypadku bliźniąt. Ważna jest również łatwość zbierania próbek, którą określa się przez dostępność urządzeń, które taką próbkę mogą dostarczyć do systemu. Kolejnym wymaganiem jest trwałość, czyli niezmienność w czasie. Tabela 1 przedstawia ocenę czterech najważniejszych wymagań dla różnych cech biometrycznych. Poza wymienionymi czterema należy również wspomnieć o trzech innych wymaganiach, szczególnie jeśli chodzi o praktyczne implementacje systemów biometrycznych [Jain 2004]. Są to wydajność (czas działania, skuteczność rozpoznania), akceptacja użytkowników (czy pobieranie próbek nie narusza prywatności bądź uczuć religijnych), a także odporność na ataki czy próby oszukania systemu.

Tabela 1. Charakterystyka wybranych cech biometrycznych [Sequeira i in. 2014]

Wymagania				
Cecha	Uniwersalność	Odmienność	Łatwość zbierania	Trwałość
DNA	wysoka	wysoka	niska	wysoka
ucho	średnia	średnia	średnia	wysoka
twarz	wysoka	niska	wysoka	średnia
termiczny obraz twarzy	wysoka	wysoka	wysoka	niska
wzór żył dłoni	średnia	wysoka	wysoka	średnia
odciski palców	średnia	wysoka	wysoka	średnia
chód	niska	niska	wysoka	niska
geometria dłoni	średnia	średnia	wysoka	średnia
źrenica oka	wysoka	wysoka	średnia	wysoka
odcisk wewnętrznej części dłoni	średnia	wysoka	średnia	wysoka
siatkówka oka	wysoka	wysoka	niska	średnia
podpis	średnia	niska	wysoka	niska
głos	średnia	niska	średnia	niska

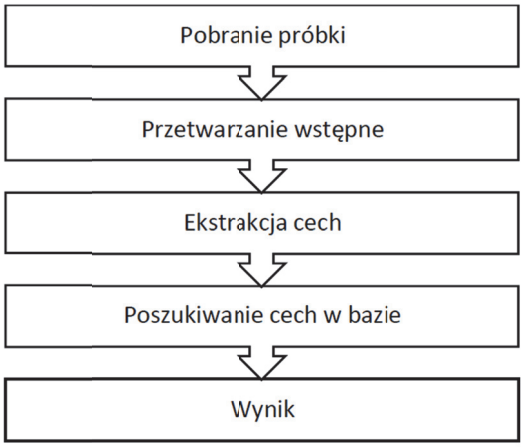
3. AKTUALNE ROZWIĄZANIA MOBILNE

Spośród wszystkich cech biometrycznych, tylko nieliczne zostały zaimplementowane w systemach mobilnych, czyli w systemach działających na urządzeniach przenośnych (telefon komórkowy, tablet). Tymi cechami są obecnie: odciski palców, wzór tęczówki oka oraz rozpoznawanie twarzy. Schemat korzystania z biometrii w telefonach jest dość prosty. Na samym początku należy wykonać proces uczenia, który polega na dostarczeniu próbek do porównania. Zostają one zapisane w bezpiecznym miejscu w pamięci telefonu. Następnym krokiem jest oczywiście weryfikacja użytkownika, której poszczególne kroki przedstawia rysunek 2. Aby wykonać weryfikację, należy pobrać nową próbkę od użytkownika. Następnie jest ona poddawana przetwarzaniu (np. usunięcie szumów). Kolejnym krokiem jest wydobycie charakterystycznych cech z próbki (np. cech tekstury czy cech geometrycznych) i porównanie ich z cechami wydobytymi z wzorców. Ostatnim elementem jest wynik. Pozytywny, jeśli cechy próbki są zgodne z cechami wzorca lub negatywny, jeśli cechy się nie zgadzają.

Jak już wspomniano, jedną z pierwszych prób rozpoznawania twarzy na telefonach podjęli twórcy Androida w wersji 4.0. Ostatnio jednak inne rozwiązanie tego problemu przedstawiła firma Apple, a mianowicie funkcję Face ID dostępną w najnowszym

iPhone X. Rozwiązanie to jest o tyle ciekawe, że nie używa zwykłego porównywania twarzy, ale porównuje obraz widziany w świetle podczerwonym z wcześniej zapisaną w pamięci telefonu trójwymiarową mapą twarzy.

Odciski palców są rozpoznawane przez coraz większą liczbę urządzeń. Ich czytniki są umieszczane w różnych miejscach urządzeń, m.in. w przycisku głównym, w przycisku wyłączania, a także z tyłu obudowy. Należy jednak pamiętać, że czytnik taki zajmuje dodatkowe miejsce na pokładzie telefonu i jest niezbędny do tego typu weryfikacji. Inną cechą biometryczną, którą obecnie wykorzystuje się w urządzeniach mobilnych jest wzór tęczówki oka. Urządzenia korzystające z tego sposobu weryfikacji są wyposażone w diodę światła podczerwonego umieszczoną w pobliżu przedniego aparatu. Weryfikacja najczęściej następuje przez przytrzymanie wzroku na dwóch kółkach wyświetlonych na ekranie.



Rys. 2. Poszczególne kroki wykonywane podczas biometrycznej weryfikacji użytkownika

4. WYZWANIA

Wprawdzie biometria stosowana w urządzeniach mobilnych jest coraz bardziej popularna, ciągle istnieją pewne problemy, których rozwiązanie może spowodować jeszcze większe zainteresowanie użytkowników tymi funkcjami.

4.1. Ochrona próbki

Pierwszym poważnym problemem jest ochrona próbki. Cechy biometryczne są niezmienne w czasie, a to niesie ze sobą pewne konsekwencje [Siddique i in. 2017]. Przede wszystkim cechy biometrycznej z zasady nie można zmienić. Odcisk palca, który trafi w niepowołane ręce, może zostać wykorzystany do czynów zabronionych, np. podrabiania biometrycznych paszportów. Dlatego próbki pobrane od użytkownika w procesie uczenia należy przechowywać w bezpiecznym miejscu w pamięci telefonu. Można przywołać niechlubną historię jednej z firm telekomunikacyjnych, która pobrane próbki przechowywała w ogólnodostępnym folderze w pamięci telefonu w powszechnie znanym formacie bitmapy BMP. Obecnie jednak takie przypadki pojawiają się znacznie rzadziej, a zamiast przechowywania całej próbki przechowuje się jedynie zaszyfrowane dane z niej pobrane.

4.2. Akceptacja użytkowników

Innym bardzo ważnym problemem systemów opartych na biometrii jest akceptacja ich potencjalnych użytkowników [Giarimi i Magnusson 2002, El-Abed i in. 2010, Lancelot Miltgen i in. 2013]. W pojęciu tym można zmieścić nie tylko to, czy użytkownik chce korzystać z danej funkcji, ale też to, czy jest ona przyjazna w użytkowaniu. Niezwykle ważna jest więc skuteczność działania takich systemów. Nie ma bowiem chyba nic bardziej irytującego niż kilkakrotne skanowanie odcisku palca i kolejna nieuzasadniona odmowa dostępu. Istotnym czynnikiem jest również to, czy funkcja biometryczna będzie dostępna dla każdego użytkownika. Warto wspomnieć chociażby o Muzułmankach, które zgodnie z tradycją zasłaniają swoje twarze. Dla nich funkcja rozpoznawania twarzy będzie zupełnie bezużyteczna. Aby uzyskać akceptację użytkowników, należy również zagwarantować odpowiednio niski czas działania całego systemu weryfikacji. Niedopuszczalną wydaje się sytuacja, w której czas weryfikacji jest zauważalny. Czas działania systemu jest związany oczywiście z optymalizacją stosowanych algorytmów.

4.3. Optymalizacja

Urządzenia mobilne są bardzo specyficzne. Mimo iż od wielu lat mają one moce obliczeniowe przekraczające znacznie możliwości dawnych komputerów osobistych, nadal są one ograniczone. Wobec tego dalsza optymalizacja wykorzystywanych algorytmów jest niemal niezbędna. Obecnie najlepsze rezultaty osiąga się, stosując systemy multimodalne, czyli analizujące jednocześnie dwie lub więcej cech biometrycznych [Ross i Jain 2004, Taouche i in. 2014]. Takie systemy są tworzone dla scenariusza klasycznego [Gochade i in. 2017], jak i mobilnego [Tresadern i in. 2013]. Jednak te ostatnie, jak do tego pory, nie zostały zaimplementowane w rozwiązaniach komercyjnych.

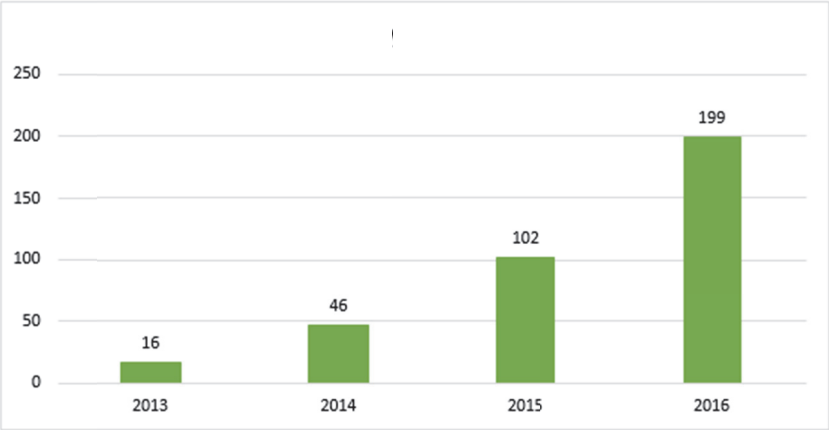
Oczywiście optymalizacja wszystkich poszczególnych kroków systemu weryfikacji jest możliwa. Etap pobierania próbek jest zazwyczaj rozwijany przez zaproponowanie nowego urządzenia [Qu i in. 2016]. Etap przetwarzania wstępnego został wykorzystany do poprawy skuteczności działania całego systemu w badaniach Zhang i in. [2017], gdzie zwiększono ostrość pobieranej próbki. Etap wydobywania cech został poprawiony przez Yoruka i in. [2006], którzy zaproponowali nowe cechy bazujące na geometrii dłoni, czyli jej kształcie. Z kolei do porównania cech zazwyczaj stosuje się różne metody sztucznej inteligencji, takie jak: SVM [Harb i in. 2015, Xu i in. 2016] czy sztuczne sieci neuronowe [Khellat-Kihel i in. 2016] oraz ich rozwinięcia.

4.4. Ataki

Analizując systemy odpowiadające za bezpieczeństwo, nie sposób zapomnieć o możliwych atakach na nie. Wśród ataków występujących w przypadku systemów biometrycznych można wymienić: sztuczne gumowe palce z odciskami, zdjęcie twarzy, wydruk tęczówki oka czy wydruki wykonane w technologii 3D, które mają posłużyć jako próbki podczas weryfikacji [Pravallika i Prasad 2016]. Tradycyjną metodą ochrony przed tego typu atakami jest kontrola żywotności (ang. liveliness detection). Zabezpieczenie to polega na sprawdzeniu, czy próbka pobrana do systemu pochodzi od żywego organizmu czy też nie. W tym celu stosuje się różne metody. Bardzo intuicyjne jest sprawdzenie ruchów źrenicy [Killioglu i in. 2017]. Innym sposobem jest wykorzystanie technik uczenia maszynowego, co zostało wykorzystane w [Bhilare i in. 2017].

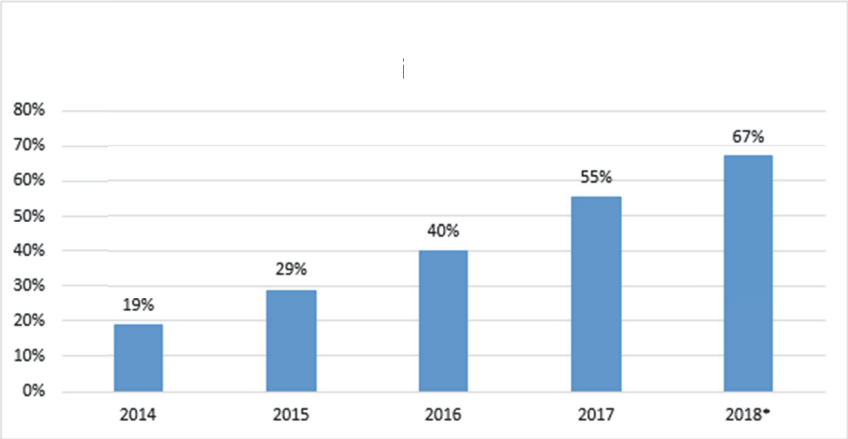
5. PERSPEKTYWY

Mimo iż w dziedzinie biometrii mobilnej stale jest wiele do poprawienia, niewątpliwie jej przyszłość rysuje się optymistycznie. Przedstawiono to na wykresach zaprezentowanych na rysunkach 3 i 4. Pierwszy z nich pokazuje jak zmieniała się liczba produkowanych telefonów, które korzystały z jakiejkolwiek cechy biometrycznej na przestrzeni ostatnich lat. Trend jest zauważalny, od czterech lat liczba takich telefonów z roku na rok rośnie.



Rys. 3. Smartfony korzystające z biometrii (opracowanie własne)

Biometryczną cechą, z której korzysta się najczęściej, są odciski palców. Drugi z rysunków (Rys. 4) pokazuje procentowy udział telefonów wyposażonych w czytniki odcisków palców wraz z prognozowaną wartością na 2018 rok. W 2014 roku takie telefony nie stanowiły nawet 1/5 części wszystkich modeli, podczas gdy w 2017 przekroczyły już połowę.



Rys. 4. Światowy udział telefonów wyposażonych w czytniki linii papilarnych (opracowanie własne)

6. PODSUMOWANIE

Analizując przedstawione wykresy popularności biometrycznych rozwiązań stosowanych w telefonach komórkowych, można stwierdzić, że biometria od dłuższego czasu jest i nadal będzie rozwijana, a w konsekwencji coraz częściej implementowana w urządzeniach przenośnych. Warte podkreślenia są również niedawno zaprezentowane flagowe modele telefonów: iPhone X (rozpoznawanie twarzy) oraz Samsung Galaxy S8, w którym zaimplementowane zostały aż 3 oddzielnie weryfikowane cechy biometryczne: odciski palców, twarz i tęczówka oka. Takie posunięcia dwóch potentatów branży telekomunikacyjnej mogą jedynie potwierdzać, że biometria jest przyszłością dla użytkowników telefonów komórkowych.

Należy jednak pamiętać, że rozwiązania biometryczne nie są w 100% odporne na ataki. Fakt ten jest też podkreślany przez producentów telefonów komórkowych, którzy jako najbezpieczniejszą metodę zabezpieczenia telefonu podają używanie hasła. Z drugiej strony jednak hasła silnie zależą od tzw. czynnika ludzkiego. To od użytkownika zależy długość używanego hasła, poziom skomplikowania czy jego bezpieczeństwo (np. zapisanie hasła na kartce papieru). Właśnie wykluczenie tego czynnika ludzkiego można wskazać jako jedną z głównych zalet rozwiązań biometrycznych.

LITERATURA

Bhilare S., Kanhangad V., Chaudhari N., 2017. A study on vulnerability and presentation attack detection in palmprint verification system. Pattern Anal. Appl, 1-14.

El-Abed M., Giot R., Hemery B., Rosenberger C., 2010. A study of users' acceptance and satisfaction of biometric systems. [In:] Security Technology (ICCST), 2010 IEEE International Carnahan Conference, 170-178.

Giarimi S., Magnusson H., 2002. Investigation of User Acceptance for Biometric Verification/Identification Methods in Mobile Units. Department of Computer and Systems Sciences Stockholm University/Royal Institute of Technology.

Gochade C., Rajput A., Daundkar V., 2017. Recognition of Iris & Palm-Print for Security of User Identification. Int. Educ. Res. J. 3.

Harb A., Abbas M., Cherry A., Jaber H., Ayache M., 2015. Palm print recognition. [In:] 2015 International Conference on Advances in Biomedical Engineering (ICABME). IEEI, 13-16.

Jain A.K., 2004. Biometric recognition: how do I know who you are? [In:] Signal Processing and Communications Applications Conference, Proceedings of the IEEE 12th, 3-5.

Jain A.K., Nandakumar K., Ross A., 2016. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognit. Lett. 79, 80-105.

Khellat-Kihel S., Abrishambaf R., Monteiro J.L., Benyettou M., 2016. Multimodal fusion of the finger vein, fingerprint and the finger-knuckle-print using Kernel Fisher analysis. Appl. Soft Comput. 42, 439-447.

Killioğlu M., Taşkiran M., Kahraman N., 2017. Anti-spoofing in face recognition with liveness detection using pupil tracking. [In:] Applied Machine Intelligence and Informatics (SAMI), 2017 IEEE 15th International Symposium, 87-92.

Lancelot Miltgen C., Popovič A., Oliveira T., 2013. Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. Decis. Support Syst. 56, 103-114.

Pravallika P., Prasad K.S., 2016. SVM classification for fake biometric detection using image quality assessment: Application to iris, face and palm print. [In:] Inventive Computation Technologies (ICICT). International Conference IEEE, 1-6.

Qu X., Zhang D., Lu G., 2016. A Novel Line-Scan Palmprint Acquisition System. IEEE Trans. Syst. Man Cybern. Syst. 46, 1481-1491.

Ross A., Jain A.K., 2004. Multimodal biometrics: An overview. [In:] Signal Processing Conference, 2004 12th European IEEE, 1221-1224.

Sequeira A.F., Monteiro J.C., Rebelo A., Oliveira H.P., 2014. Mobbio: a multimodal database captured with a portable handheld device. [In:] Computer Vision Theory and Applications (VISAPP). International Conference IEEE, 133-139.

Siddique K., Akhtar Z., Kim Y., 2017. Biometrics vs passwords: a modern version of the tortoise and the hare. Comput. Fraud Secur. 2017, 13-17.

Taouche C., Batouche M.C., Berkane M., Taleb-Ahmed A., 2014. Multimodal biometric systems. [In:] Multimedia Computing and Systems (ICMCS). International Conference IEEE, 301-308.

Tresadern P., Cootes T.F., Poh N., Matejka P., Hadid A., Lévy C., McCool C., Marcel S., 2013. Mobile Biometrics: Combined Face and Voice Verification for a Mobile Platform. IEEE Pervasive Comput. 121. 79-87.

Unar J.A., Seng W.C., Abbasi A., 2014. A review of biometric technology along with trends and prospects. Pattern Recognit. 47, 2673-2688.

Xu X., Lu L., Zhang X., Lu H., Deng W., 2016. Multispectral palmprint recognition using multiclass projection extreme learning machine and digital shearlet transform. Neural Comput. Appl. 27, 143-153.

Yoruk E., Konukoglu E., Sankur B., Darbon J., 2006. Shape-based hand recognition. IEEE Trans. Image Process. 15, 1803-1815.

Zhang K., Huang D., Zhang D., 2017. An optimized palmprint recognition approach based on image sharpness. Pattern Recognit. Lett. 85, 65-71.