Uniwersytet Technologiczno-Przyrodniczy
im. Jana i Jędrzeja Śniadeckich w Bydgoszczy

**Wydział Telekomunikacji,
Informatyki i Elektrotechniki**

ROZPRAWA DOKTORSKA

mgr inż. Agata Giełczyk

Rozpoznawanie osób na podstawie analizy obrazów dłoni za pomocą urządzeń mobilnych

Promotor
dr hab. inż. Michał Choraś, prof. uczelni

Promotor pomocniczy
dr hab. inż. Rafał Kozik, prof. uczelni

Bydgoszcz 2020

Spis treści

1. Wprowadzenie

1.1. Wstęp

Społeczeństwo XXI wieku jest społeczeństwem cyfrowym, ze stałym dostępem do Internetu i wszystkich jego zasobów. Postęp cywilizacyjny, który obecnie pędzi z niespotykaną wcześniej prędkością, jest doskonale widoczny w każdej z dziedzin naszego życia. W większości z nich od kilku lat obserwujemy rosnący udział komputerów, a w przyszłości ten udział prawdopodobnie będzie jeszcze większy. Co również jest bardzo istotne, od lat obserwuje się rosnącą liczbę aktywnych urządzeń mobilnych: telefonów, komputerów i tabletów, które zaczynają towarzyszyć ludziom już od najmłodszych lat. W tej chwili nie służą one już wyłącznie do dzwonienia, ale są podstawowym sprzętem wykorzystywanym do komunikacji, do rozrywki, a także do pracy. Umożliwiają więc dostęp do wielu zasobów, w tym do istotnych danych pojedynczego człowieka, organizacji, a nawet wielkich firm.

> *It will not be a world of man versus machine, it will be a world of man plus machine.*
>
> *Virginia Rometty*

Przytoczony wyżej cytat to słowa Virginii Rometty, pierwszej kobiety na stanowisku prezesa informatycznego potentata, firmy IBM, które skierowała do absolwentów jednej z amerykańskich uczelni wyższych podczas ceremonii wręczenia dyplomów w 2017 roku[1]. Zgodnie z jej wypowiedzią oraz aktualnie obserwowanymi trendami świat przyszłości, także tej bardzo bliskiej przyszłości, będzie się opierał na współpracy człowieka i maszyny. Współpraca ta nie jest niczym innym, jak wsparciem człowieka podczas podejmowania decyzji przez komputery. Jej przykładów można wymieniać bez końca: systemy eksperckie wspierające decyzje lekarskie, systemy analizy danych giełdowych i bankowych czy systemy rozpoznawania znaków instalowane w nowoczesnych samochodach. Współpraca ta może być również rozumiana jako każdy udział technologii w codziennym życiu człowieka: w urządzeniach nawigacji GPS, w technologii wspierającej aktywność sportową czy w komunikacji na odległość przez komunikatory internetowe.

[1] https://speakola.com/grad/virginia-rometty-ibm-northwestern-2017

Tematem tej pracy doktorskiej jest biometria, która wydaje się kwintesencją połączenia człowieka i inteligencji maszynowej. W biometrii bowiem wykorzystujemy ludzką różnorodność i odmienność elementów ciała lub szczególnego zachowania każdego z nas oraz moce obliczeniowe komputerów, aby zapewnić jak najwyższy poziom zabezpieczeń dla danych, zasobów czy pomieszczeń. W ten właśnie sposób biometria stała się jednym z bardziej istotnych problemów informatyki przełomu XX i XXI wieku, a od początku XXI wieku obserwowany jest stały wzrost zainteresowania jej aplikacjami w codziennym życiu.

1.2. Cel, zakres i teza pracy

Niniejsza rozprawa doktorska nie traktuje o biometrii w ogólnym jej znaczeniu, ale skupia się wyłącznie na analizie obrazów wewnętrznych części dłoni i wykorzystaniu ich do rozpoznawania użytkownika. Po przeanalizowaniu literatury tematu postawiono następującą tezę pracy:

> Wykorzystując informacje zawarte w obrazie wewnętrznej części dłoni, można przeprowadzić skuteczne rozpoznawanie osób za pomocą urządzenia mobilnego.

Celem tej dysertacji jest zaproponowanie nowych metod biometrycznego rozpoznawania osób na podstawie obrazu dłoni oraz ich przebadanie na urządzeniach mobilnych. Najważniejszym elementem badawczym pracy jest zaproponowanie nowego algorytmu wydobycia rejonu zainteresowań oraz sześciu autorskich metod analizy obrazu wewnętrznej części dłoni, którymi są:

1. metoda oparta na histogramie gradientów,
2. metoda hybrydowa Color-Texture,
3. metoda hybrydowa Geometric-Texture,
4. metoda 3-wartościowej maski,
5. metoda kodu binarnego,
6. metoda energii tekstury.

Metody te zostały opracowane, a następnie oceniono ich przydatność do zastosowania na urządzeniach mobilnych. Ponadto Autorka przebadała wpływ wybranych metod przetwarzania wstępnego na skuteczność rozpoznawania osób na podstawie obrazów dłoni. Zaproponowano również koncepcję bazy danych, która w przyszłości może zostać wykorzystana do tworzenia, testowania i rozwijania mobilnych systemów rozpoznawania osób na podstawie analizy obrazów dłoni.

1.3. Układ pracy

Praca składa się z siedmiu rozdziałów. W pierwszym określono cel, zakres oraz tezę rozprawy doktorskiej. Dokonano również wprowadzenia do biometrycznego rozpoznawania osób na podstawie analizy obrazu dłoni. W tym rozdziale znajduje się też spis publikacji Autorki w tematyce rozprawy doktorskiej. Jest to w sumie 12 prac o tematyce związanej z biometrią, ze szczególnym uwzględnieniem prac traktujących o biometrii obrazu dłoni. Prace były publikowane na konferencjach międzynarodowych oraz w czasopismach wykazanych na listach ministerialnych. Zostały umieszczone w kolejnej sekcji tego rozdziału.

Drugi rozdział opisuje biometrię jako skuteczną technikę umożliwiającą rozpoznawanie osób. Omówiono w nim biometrię klasyczną, mobilną, multimodalną, a także jej szerokie zastosowania w aplikacjach życia codziennego. Rozdział drugi kończy się krótką analizą prawną niektórych aspektów biometrycznych.

Rozdział trzeci stanowi opis obrazu wewnętrznej części dłoni jako cechy biometrycznej. Przytoczono w nim i scharakteryzowano wybrane metody dostępne w literaturze. Rozdział kończy się podsumowaniem, które jednoznacznie wskazuje i motywuje kierunki badań podejmowanych w tej pracy.

W kolejnym, czwartym rozdziale opisano wszystkie podejścia do biometrycznego rozpoznawania osób proponowane przez Autorkę. Jest to sześć autorskich metod identyfikacji, jeden algorytm wyznaczania ROI oraz opis wybranych metod przetwarzania wstępnego. Zakończenie tego rozdziału zawiera tabelę, w której zebrane zostały wszystkie proponowane metody wraz z wyszczególnieniem ich najważniejszych elementów.

Piąty rozdział zawiera opis stanowiska badawczego, urządzeń użytych do badań oraz protokół ich prowadzenia. Opisano również trzy klasyczne bazy danych, które są wykorzystywane do testowania systemów biometrycznych opartych na obrazach dłoni oraz do prowadzenia badań nad tą cechą biometryczną. Ten rozdział zawiera też opis koncepcji bazy danych, która mogłaby w przyszłości służyć jako baza do testowania i rozwoju mobilnych systemów opartych o identyfikację na podstawie obrazu dłoni.

Szósty rozdział przedstawia dalszą część własnego wkładu Autorki. Zostały w nim zamieszczone wyniki badań przeprowadzonych dla każdej z proponowanych i opisanych wcześniej metod oraz przedstawiono ich implementację na urządzeniach mobilnych.

Siódmy, a zarazem ostatni rozdział zawiera podsumowanie całej pracy i wyciągnięte wnioski. Zawiera tabelę, w której dokonano porównania proponowanych metod oraz metod znanych z literatury pod kątem skuteczności działania

oraz czasu wykonywania pojedynczej weryfikacji użytkownika na urządzeniu mobilnym. W tym rozdziale opisano również możliwe dalsze kierunki prowadzonych badań. Ostatnie elementy pracy to spis literatury, rysunków oraz tabel.

1.4. Publikacje Autorki

Część wyników opisanych i wykorzystanych w tej pracy była publikowana w formie artykułów. Ponadto Autorka prezentowała wyniki swoich badań na konferencjach krajowych oraz międzynarodowych (Włochy, Francja, Irlandia), ze szczególnym uwzględnieniem konferencji z listy CORE. Część badań została przeprowadzona podczas 3-miesięcznego stażu zagranicznego, na który Autorka wyjechała w ramach programu Erasmus+ do Włoch, do *Universitá degli Studi di Cagliari* na Sardynii. Staż ten odbył się w grupie *Pattern Recognition and Applications LAB*, która prowadzi badania nad biometrią oraz cyberbezpieczeństwem, oraz zaowocował wspólną polsko-włoską publikacją. Dotychczas w dziedzinie biometrii dłoni ukazały się następujące prace Autorki:

1. **Giełczyk A.** 2018. Bezpieczeństwo wybranych systemów biometrycznych. Nauka niejedno ma imię VI. Wydawnictwa Uczelniane UTP, ss. 37–44.
2. **Giełczyk A.**, Marcialis G.L., Choraś M. 2019. Binary Code for the Compact Palmprint Representation Using Texture Features. [W:] International Conference on Computer Analysis of Images and Patterns (CAIP), Springer, ss. 132–142 (CORE B).
3. **Giełczyk A.** 2017. Biometria mobilna. Perspektywy i wyzwania. Nauka niejedno ma imię V. Wydawnictwa Uczelniane UTP, ss. 21–28.
4. **Giełczyk A.**, Choraś M., Kozik R. 2018. Biometria obrazu dłoni jako część systemu wielopoziomowego uwierzytelniania użytkownika. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne 8–9, ss. 593–596.
5. **Giełczyk A.**, Choraś M., Kozik R. 2018. Hybrid Feature Extraction for Palmprint-Based User Authentication. [W:] International Conference on High Performance Computing & Simulation (HPCS), IEEE, ss. 629–633 (CORE B).
6. **Giełczyk A.**, Choraś M., Kozik R. 2019. Lightweight Verification Schema for Image-Based Palmprint Biometric Systems. Mobile Information Systems, Hindawi (IF=1,635).
7. **Giełczyk A.**, Choraś M., Kozik R. 2019. The mobile palmprint-based verfication based on three-value masks. [W:] International Conference on High Performance Computing & Simulation (HPCS), IEEE, ss. 909–914 (CORE B).

8. **Giełczyk A.**, Dembińska K., Choraś M., Kozik R. 2019. Towards Mobile Palmprint Biometric System with the New Palmprint Database. [W:] International Conference on Image Processing and Communications (IP&C), Springer, ss. 149–157.
9. **Wojciechowska A.**, Choraś M., Kozik R. 2018. Evaluation of the pre-processing methods in image-based palmprint biometrics. [W:] International Conference on Image Processing and Communications (IP&C), Springer, ss. 43–48.
10. **Wojciechowska A.**, Choraś M., Kozik R. 2017. The method and an exemplary biometric system to verify users. Journal of Machine Construction and Maintenance. Problemy Eksploatacji 106(3), ss. 97–101.
11. **Wojciechowska A.**, Choraś M., Kozik R. 2017. The overview of trends and challenges in mobile biometrics. Journal of Applied Mathematics and Computational Mechanics 16(2), ss. 173–185.
12. **Wojciechowska A.**, Choraś M., Kozik R. 2018. Recent Advances in Image Pre-processing Methods for Palmprint Biometrics. [W:] International Conference on Computer Recognition Systems (CORES), Springer, ss. 268–275.

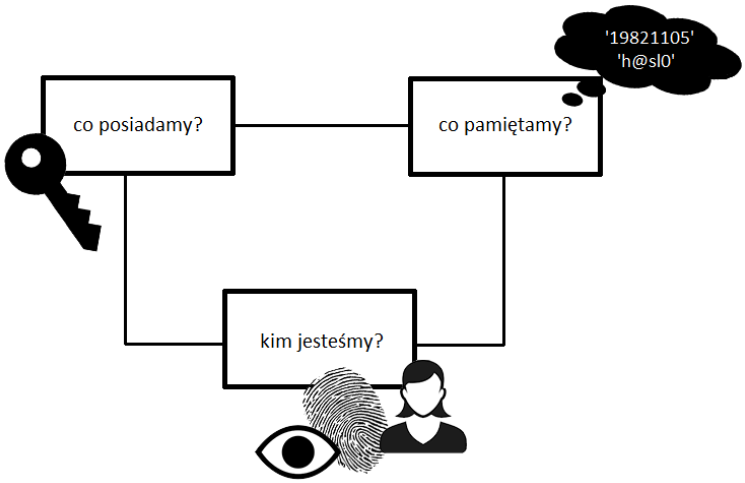
2. Biometria

W nowoczesnym społeczeństwie XXI wieku człowiek jest zmuszony do pamiętania niezliczonych loginów, haseł czy numerów PIN, które są wykorzystywane niemal na każdym kroku naszego codziennego życia. Wśród przykładów można wymienić: otwieranie domofonu na kod, logowanie się do konta poczty elektronicznej, sprawdzanie karty i hasła przy bankomacie, czy nawet wejście na teren niektórych klubów sportowych. Zawsze musimy podać konkretne, najlepiej w każdym przypadku inne dane. Właśnie z powodu natłoku informacji dotyczących logowania zaczęto stosować biometrię, która pozwala na zmniejszenie ilości niezbędnych do zapamiętania haseł przez zastosowanie techniki weryfikacji użytkowników „*kim jesteśmy?*" w zamian za technikę „*co pamiętamy?*" (tutaj można wymienić hasła i numery PIN) lub „*co posiadamy?*" (klucze, tokeny, karty dostępu). Techniki te w sposób schematyczny zostały przedstawione na rysunku 1. Wśród zalet biometrii możemy wymienić [72]:

- łatwość użycia – łatwiej jest zetknąć opuszek palca z czytnikiem linii papilarnych niż wpisywać długie hasło;
- szybkość działania – obecnie stosowane rozwiązania pozwalają na uzyskanie dostępu do chronionych zasobów praktycznie w czasie rzeczywistym, czyli bez zauważalnego dla osoby weryfikowanej opóźnienia;
- nowoczesność – jest to technika znacznie nowsza niż używanie kluczy, kłódek czy haseł i ostatnio staje się coraz bardziej powszechna.

Mimo istnienia wielu zalet stosowania biometrii, należy pamiętać, że cech tych praktycznie nie można zmienić. To oznacza, że utracenie wzoru jednej z nich może grozić poważnymi konsekwencjami. Biometria w ogólnym ujęciu jest nauką o mierzeniu organizmów. Najczęściej jednak jest wykorzystywana do tworzenia automatycznych systemów identyfikacji i weryfikacji osób, w których wykorzystuje jedną bądź kilka z cech. W przypadku, kiedy wykorzystuje się więcej niż jedną cechę, można powiedzieć o biometrii multimodalnej [61]. Cechy, na których opiera się weryfikacja, muszą spełniać następujące wymagania [39, 35]:

- uniwersalność – każda osoba identyfikowana posiada daną cechę;
- odmienność – cecha jest różna dla każdej z osób;
- trwałość – cecha jest niezmienna w czasie;
- łatwość pozyskania – cechę łatwo pobrać od identyfikowanej osoby.



Rysunek 1. Diagram weryfikacji użytkowników [9]

W systemach implementowanych w życiu codziennym, nie tylko w celach badawczych, do podstawowych wymagań dodaje się kolejne, którymi są [39]:

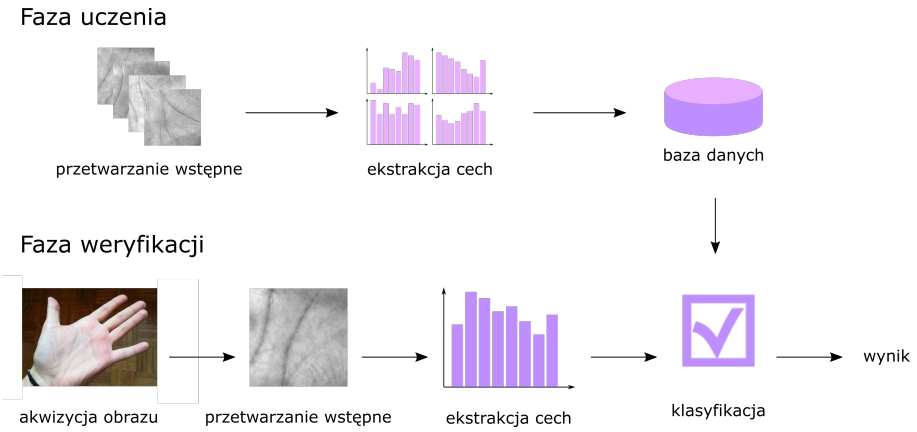
- wydajność – system musi dawać odpowiedź w akceptowanym czasie, czas ten jest jednak różny dla różnych systemów biometrycznych;
- możliwość przyjęcia przez użytkowników – system nie może ingerować nadto w prywatność osoby identyfikowanej, a podczas wyboru cechy należy kierować się również różnicami kulturowymi;
- trudność ominięcia – system musi być maksymalnie trudny do oszukania przez osoby, które chciałyby uzyskać dostęp do chronionych zasobów, a nie są do tego upoważnione.

Systemy biometryczne w zakresie ich przeznaczenia można podzielić na systemy identyfikacji oraz weryfikacji, które różnią się przede wszystkim otrzymywanym wynikiem. W systemie identyfikacji otrzymuje się konkretną informację o osobie, jeśli szukana próbka została odnaleziona w bazie lub informację, że żadna podobna próbka nie istnieje w bazie. Oczywiście są także systemy, które typują kilka najbardziej podobnych do szukanej osób z bazy [10]. Z kolei w systemach weryfikacji wynik jest znacznie prostszy. Zawsze otrzymujemy bowiem wynik „*prawda*” dla użytkownika, który powinien uzyskać dostęp do chronionych zasobów lub „*fałsz*” dla użytkownika, który go uzyskać nie powinien. Systemy te często różnią się metodami wykorzystywanymi w kolejnych etapach działania, wielkością bazy danych, a także ilością zasobów obliczeniowych komputera, który podejmuje decyzje.

Cecha biometryczna jest zazwyczaj dostarczana do systemu weryfikacji bądź identyfikacji w postaci obrazu albo nagrania (m.in. głosowego lub audiowizualnego), które są nazywane próbkami. Rysunek 2 przedstawia ogólny schemat działania systemu biometrycznego. Każdy z etapów działania tego systemu jest bardzo istotny. Pobranie próbki następuje za pomocą dedykowanego urządzenia (np. skaner tęczówki oka, skaner linii papilarnych) lub urządzenia uniwersalnego, mogącego służyć do wielu czynności (np. żyroskop, aparat fotograficzny). Próbki mogą zostać zniekształcone przez: niedoskonałości urządzenia pobierającego, zmiany w fizycznej strukturze próbki (rany lub blizny na opuszku palca), zmienne warunki środowiska zewnętrznego (wilgotność, temperatura) czy też inną interakcję z urządzeniem pobierającym (inne położenie palca na czytniku) [39]. Dlatego próbka zostaje poddana metodom wstępnego przetwarzania. Ten etap ma dwojakie znaczenie. Przede wszystkim jest to poprawa jakości próbki, czyli usunięcie powstałych szumów. Dla próbek w postaci obrazów wykonuje się też ograniczenie wielkości próbki poprzez wyznaczenie rejonu zainteresowań (ang. *Region Of Interest*), zwanego również ROI. Zmniejszona wielkość analizowanego obrazu wpływa pozytywnie na złożoność obliczeniową całego systemu. Kolejnym etapem jest wydobycie cech, czyli zmiana próbki na wektor cech - najczęściej liczb. Następnie utworzony wektor jest porównywany z innymi wektorami, które są przechowywane w bazie. Literatura tematu wskazuje, że w tym etapie stosuje się różnorodne metody uczenia maszynowego np. SVM (ang. *Support Vector Machine*) i sieci neuronowe albo miary odległości (odległość Euklidesa, Hamminga czy Minkowskiego). Metody stosowane w tej części systemu wymagają wcześniej dostarczonych próbek wzorcowych, którym należy wcześniej nadać etykiety: pozytywną lub negatywną. Proces nadawania etykiet i wprowadzania do systemowej bazy danych można nazwać procesem uczenia.

Biometria została włączona również do systemów wielopoziomowego uwierzytelniania użytkownika (ang. *Multifactor Authentication System - MFA*). Uważa się go za jeden z najbardziej bezpiecznych sposobów autoryzacji użytkowników [19]. Zasadniczo wymaga on więcej niż jednego sposobu weryfikacji tożsamości, czyli np. karty, hasła lub numeru PIN oraz cechy biometrycznej. Brak implementacji MFA w dużym przedsiębiorstwie może ułatwić atak na jego system informatyczny, a w konsekwencji narazić firmę na utratę danych o procesie technologicznym, danych klientów, a także spowodować utratę dobrego imienia. Wszystkie te konsekwencje zaś w prostej linii doprowadzą do utraty pieniędzy. Przykłady udanych ataków na systemy informatyczne można długo wymieniać. Do najbardziej głośnych tego typu spraw z pewnością można zaliczyć wyciek danych należących do 76 mln gospodarstw domowych i 7 mln małych przedsiębiorstw w Stanach Zjednoczonych, klientów banku JPMorgan Chase[1]. Okazało się, że

[1] www.nytimes.com/2014/10/04/your-money/jpmorgan-chase-hack-ways-to-protect-yourself.html



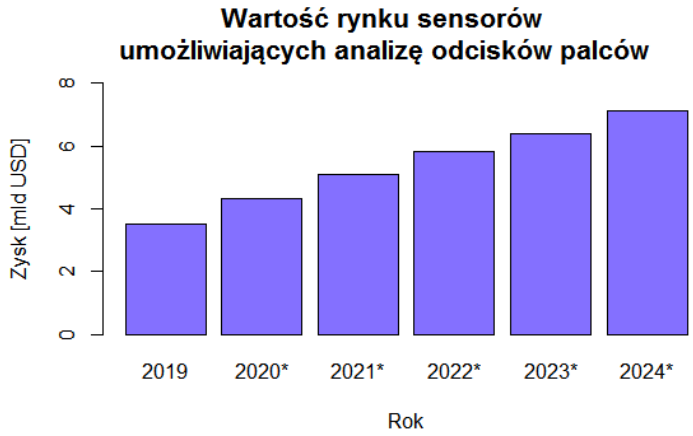
Rysunek 2. Schemat działania systemu biometrycznego opartego na biometrii dłoni [opracowanie własne]

wyciek danych rozpoczął się w czerwcu 2014 roku, jednak jego istnienie odkryto dopiero w połowie sierpnia. Dostęp do systemu banku umożliwiła kradzież danych logowania od jednego z pracowników. Innym głośnym atakiem, któremu mogło zapobiec zastosowanie MFA, było włamanie się na serwery firmy Uber. Zastosowano tam atak siłowy na platformę GitHub, dzięki czemu uzyskano dostęp do kodu oprogramowania, a następnie do danych logowania do serwerów kopii zapasowych. Hakerzy, którym udało się uzyskać nieautoryzowany dostęp, mieli dostęp do danych 57 mln pasażerów Ubera[2]. Dane jednak nie wyciekły do publicznej wiadomości, gdyż firma zgodziła się zapłacić olbrzymi okup. Innym przykładem może być wyciek danych amerykańskiej korporacji konsultingowej, Deloitte[3]. W tym przypadku hakerzy uzyskali dane logowania administratora, a następnie mogli przejrzeć i wykraść dane wielu klientów.

2.1. Biometria tradycyjna

Pierwsza naukowa wzmianka o istnieniu odcisków palców pochodzi z czasopisma Nature, w którym w 1880 roku Henry Faulds opublikował swój artykuł [40]. Następnie znalazły one swoje zastosowanie jako dowód w śledztwach prowadzonych przez argentyńską policję (1893 r.), brytyjski Scotland Yard (1901 r.)

[2] www.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html
[3] www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails



Rysunek 3. Wartość rynku sensorów umożliwiających analizę odcisków palców

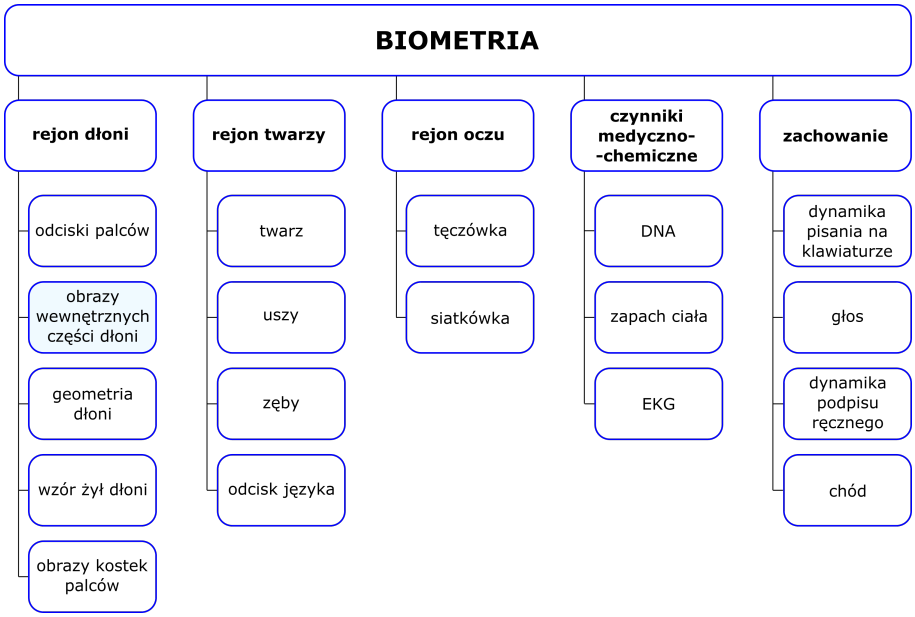
czy FBI (1924 r.). Pierwsza naukowa publikacja na temat automatycznej identyfikacji biometrycznej została opublikowana przez Mitchella Trauringa w czasopiśmie Nature w 1963 roku. Jako cechę biometryczną wykorzystywał odciski palców i to właśnie one stały się jedną z częściej wykorzystywanych cech. Stało się tak przede wszystkim ze względu na łatwość dostępu do tej części ciała – nie należą ani do stref intymnych, ani zastrzeżonych przez wielkie religie świata. Na początku próbki odcisków palców były pobierane przy pomocy papieru i tuszu, jednak w latach 90 XX w. zaczęły się pojawiać pierwsze cyfrowe czytniki odcisków palców. Po latach zostały one zminiaturyzowane. Obecnie, od 28 sierpnia 2006 roku odciski palców są jedną z dwóch cech rejestrowanych w trakcie wydawania paszportu w Polsce. Sposób przechowywania danych biometrycznych w paszportach został zdefiniowany w normie ICAO9303 wydanej przez Organizację Międzynarodowego Lotnictwa Cywilnego [34]. Odciski palców są również elementem zapisanym w nowych dowodach osobistych, które obowiązują od marca 2019 roku. Popularność tej cechy biometrycznej pokazują również prognozy dotyczące zysków, jakie wygeneruje rynek sensorów umożliwiających pobieranie odcisków palców. Jedną z takich prognoz przedstawiono na rysunku 3[4]. Rysunek ten przedstawia wartość (rok 2019) oraz prognozowaną wartość (lata 2020-2024) rynku urządzeń pobierających odciski palców na całym świecie. Okazuje się, że w 2024 roku zysk ten ma wynieść ponad 7 miliardów dolarów amerykańskich.

[4] https://www.marketsandmarkets.com/Market-Reports/fingerprint-sensors-market-169519533.html

Rozwój kolejnej cechy biometrycznej, twarzy, był zupełnie inny. Mimo iż ludzie rozpoznają się nawzajem właśnie przez spojrzenie na twarz, na automatyczny system rozpoznawania osób na podstawie tej części ciała trzeba było czekać aż do 1973 roku. System ten został zaproponowany przez Takeo Kanade w jego pracy doktorskiej. Jednym z kroków milowych w rozwoju rozpoznawania twarzy była metoda opracowana i opisana w [78] przez duet badaczy Viola i Jones. Ich algorytm wykrywania twarzy jest nadal bardzo skuteczny w operacjach czasu rzeczywistego, jednak wciąż trwają prace nad poprawą jego działania w przypadku, gdy twarz na obrazie jest ustawiona nieco bokiem lub niektóre jej części są niewidoczne. Na rozwój tej cechy biometrycznej wpłynął również postęp technologiczny, który pozwolił na tworzenie coraz to lepszych kamer służących do rejestrowania obrazu twarzy. Obecnie spotykane kamery cyfrowe są porównywalne nawet do ludzkiego oka w zakresie ilości klatek, jakości i rozdzielczości widzenia. Wizerunek twarzy również jest zbierany w procesie wyrabiania paszportu na terenie Polski. W czerwcu 2019 roku na największym polskim lotnisku, Lotnisku im. Fryderyka Chopina w Warszawie zostały zainstalowane bramki automatyczne (ABC - ang. *Automated Border Control*), które umożliwiają samodzielne przejście kontroli paszportowej dla pasażerów odlatujących i przybywających z krajów spoza strefy Schengen.

Inną cechą biometryczną jest tęczówka oka. Chociaż jest to organ bardzo niewielki, może zostać wykorzystany do rozróżnienia osób. Tęczówka posiada bowiem strukturę skomplikowaną, losową i różną dla każdej osoby. Pierwszy patent na użycie tej cechy biometrycznej do rozpoznawania osób został przyznany w 1985 roku. Jedną z przeszkód w rozwoju tej cechy był brak odpowiednich urządzeń do pobierania próbek. Pierwsze kamery opracowane w latach 90 XX w. były mało poręczne, drogie i wymagały współpracy osoby, od której pobierało się próbkę. Jednak raz z rozwojem techniki zwiększała się popularność rozpoznawania osób na podstawie wzoru tęczówki. Jedną z kluczowych implementacji takiego systemu biometrycznego jest ten stosowany w Zjednoczonych Emiratach Arabskich od 2001 roku, w którym sprawdzane są wszystkie osoby przekraczające granice kraju.

W kolejnych latach zaczęto tworzyć kolejne automatyczne systemy biometryczne bazujące na głosie, twarzy, własnoręcznym podpisie, geometrii dłoni czy źrenicy oka. Szeroka lista aktualnie stosowanych cech biometrycznych została przedstawiona na rysunku 4. Oczywiście istnieje również wiele cech biometrycznych, które nie zostały ujęte na tym wykazie. Wśród nich można wymienić profil twarzy, którego wykorzystanie opisano w [49]. Z widocznych na rysunku cech największą popularność zyskały opisane wcześniej: odciski palców, twarz oraz tęczówka oka. Zdecydowaną przewagą odcisków palców i twarzy jako cechy biometrycznej jest również dostępność wielu baz danych (m.in. bazy danych kierowców czy imigrantów tworzone przez organizacje rządowe wielu krajów na



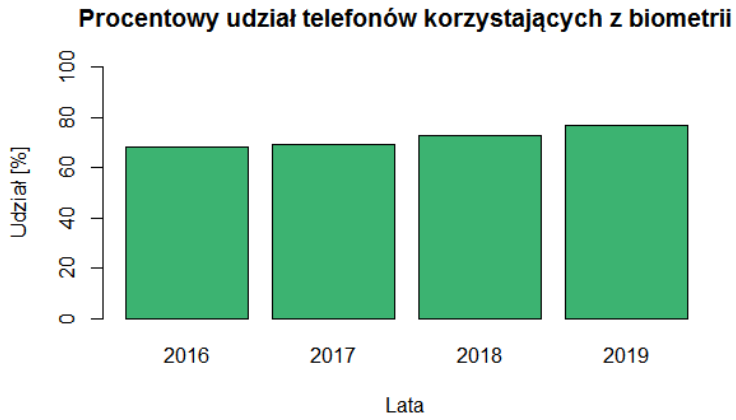
Rysunek 4. Podział cech biometrycznych [72]

świecie), na których można realizować badania, a także rozwijać istniejące już systemy.

2.2. Biometria mobilna

W XXI wieku w krajach rozwiniętych liczba aktywnych telefonów komórkowych przekroczyła już liczbę mieszkańców [59]. Dzieje się tak, ponieważ spora część społeczeństwa posiada więcej niż jeden telefon komórkowy. Dynamiczny rozwój technologii i wzrost popularności urządzeń przenośnych spowodował migrację wielu systemów, w tym biometrii, do scenariusza mobilnego. Mimo że obecnie wykorzystywane telefony posiadają moce obliczeniowe przekraczające możliwości dawnych komputerów osobistych, nadal nie są w stanie przeprowadzić identyfikacji użytkownika na podstawie olbrzymich baz danych (szeroko wykorzystywanej w dochodzeniach kryminalnych). Są jednak w stanie przeprowadzić weryfikację użytkownika za pomocą jego cech biometrycznych i właśnie takie systemy są najczęściej implementowane przy użyciu urządzeń przenośnych.

Cechy, których używają systemy mobilne, są znacznie bardziej ograniczone. Obecnie komercyjnie korzysta się jedynie z rozpoznawania odcisków palców,

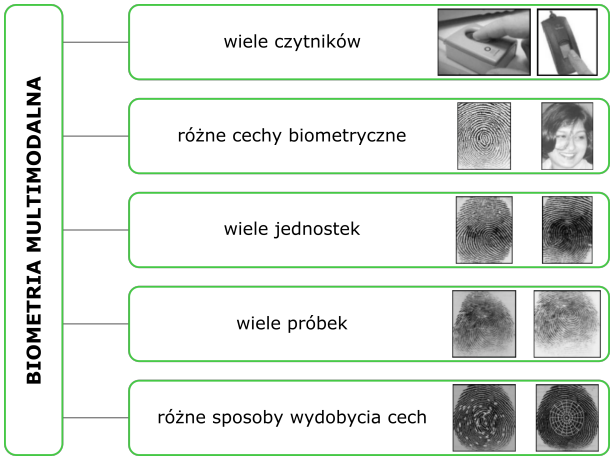


Rysunek 5. Procentowy udział telefonów korzystających z biometrii spośród wszystkich dostępnych modeli

twarzy oraz tęczówki oka. Rozpoznawanie twarzy zostało po raz pierwszy zaimplementowane w systemie Android 4.0, który ujrzał światło dzienne w październiku 2011 roku. Niestety ten sposób odblokowania telefonu był dość niedopracowany. Wystarczyło bowiem przed aparatem telefonu umieścić zdjęcie użytkownika i system udzielał dostępu do chronionych danych. Kolejną cechą komercyjnie zastosowaną w telefonach komórkowych są odciski palców. Do ich wprowadzenia niezbędne było umieszczenie miniaturowego skanera linii papilarnych, który znalazł sobie miejsce z przodu, z boku lub z tyłu telefonu komórkowego. Rozwiązanie to zostało wprowadzone w 2011 roku w modelu Motorola Atrix, a później w iPhone 5. Najnowsze systemy (np. iPhone X) wykorzystują weryfikację na podstawie tęczówki oka poprzez analizę obrazu widocznego w świetle podczerwonym. Niestety jak podają liczne źródła internetowe, wszystkie systemy analizujące odciski palców, jak i analizujące wzór tęczówki oka zostały oszukane i złamane przez hakerów w około pół roku od daty premiery. Najczęściej atak polega na podaniu do sensora lub kamery sztucznie wyprodukowanej próbki, na podstawie której system podejmuje decyzję o pozytywnej autoryzacji.

Biometria mobilna z roku na rok staje się coraz bardziej popularna. Wykres przedstawiony na rysunku 5[5] przedstawia, jaki procent ogólnej liczby telefonów stanowiły te, które umożliwiają biometryczną autoryzację. Widać na nim tendencję wzrostową. W roku 2016 68% telefonów korzystało z biometrii, a w 2019 roku było to już 77%.

[5] www.zdnet.com/pictures/2019s-tech-security-and-authentication-trends/12/?fbclid=IwAR3PTVGTJxnswLxmM0l30pizfyLDeZRiuFUXlgqbxjeZbbFUGr35ngFyaMQ



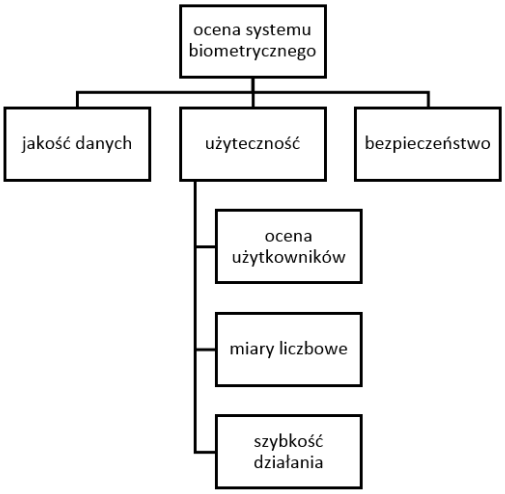
Rysunek 6. Różne sposoby łączenia modalności biometrycznych [61]

2.3. Biometria multimodalna

Chociaż, jak pokazano we wcześniejszych rozdziałach, biometria zyskuje coraz większą popularność, nie jest pozbawiona wad. Dla systemów korzystających z tylko jednej cechy wymienia się następujące [61, 67]:

- szum pojawiający się w pobranych próbkach – szumem takim w systemach rozpoznających osoby na podstawie odcisków palców może być blizna w wykorzystywanym rejonie, a w systemie rozpoznającym twarze szum może powodować niewystarczające oświetlenie;
- wariacje wewnątrz klas – spowodowane głównie przez nieodpowiednią interakcję z czytnikiem próbki;
- podobieństwa między klasami – w przypadku dużej ilości próbek w bazie różnice pomiędzy identyfikowanymi osobami mogą być bardzo niewielkie;
- brak uniwersalności – wykorzystywana cecha może nie być możliwa do pobrania od jakiegoś podzbioru osób;
- ataki wykorzystujące fałszywą próbkę – możliwe jest stworzenie sztucznej próbki (np. gumowego palca), który pozytywnie przejdzie proces identyfikacji.

Wady te doprowadziły do stworzenia systemów biometrii multimodalnej. Ta jednak jest bardzo rozbudowana, gdyż jak zostało to przedstawione na rysunku 6, można duplikować różne elementy systemu (np. cechę biometryczną czy ilość pobieranych próbek). Podział biometrycznych systemów multimodalnych prezentuje się następująco:



Rysunek 7. Sposoby oceny systemu biometrycznego [23]

1. Multimodalność polegająca na zwielokrotnieniu liczby wykorzystywanych urządzeń do pobrania próbek – przykładem może być użycie optycznych i pojemnościowych skanerów linii papilarnych;
2. Multimodalność polegająca na użyciu różnych śladów biometrycznych – mogą to być systemy wykorzystujące jednocześnie twarz i odcisk palca, a nawet system wykorzystujące jednocześnie trzy ślady;
3. Multimodalność polegająca na użyciu różnych jednostek reprezentujących jeden ślad biometryczny – są to systemy korzystające jednocześnie z odcisków dwóch palców lub z obrazów wewnętrznych części obu dłoni;
4. Multimodalność polegająca na zwielokrotnieniu liczby próbek pobieranych od identyfikowanej osoby – użycie wielu próbek pozwala na stworzenie bardziej dokładnego obrazu próbki;
5. Multimodalność polegająca na łączeniu wielu cech – mogą to być systemy korzystające jednocześnie z cech charakterystycznych bazujących na teksturze i kolorze.

2.4. Ocena systemów biometrycznych

Aby system biometryczny działał jak najlepiej, dokonuje się oceny jego parametrów. Parametry, które powinny podlegać ocenie, zostały przedstawione na rysunku 7 [23].

Pierwszym z nich jest jakość zebranych danych. Dane o dobrej jakości pozytywnie wpływają na proces podejmowania decyzji. Z kolei dane z dużym dodatkiem szumów mogą, mimo zastosowania odpowiednich metod przetwarzania wstępnego, negatywnie wpływać na działanie systemu. Przykładowa ocena zebranych próbek została przedstawiona w [69], natomiast w [85] zaprezentowano wpływ ostrości próbek na działanie całego systemu biometrycznego.

Innym, równie ważnym elementem podlegającym ocenie, jest użyteczność. Może ona zostać określona m.in. przez użytkowników, którzy decydują, jak dobrze, bądź jak źle korzysta się z danego systemu. Z pewnością będą zwracać uwagę na jakość zastosowanego czytnika, na szybkość jego działania oraz na fakt ewentualnej konieczności ponownego pobrania próbki. Przykładowa ocena zaimplementowanego w rzeczywistości systemu biometrycznego przez jego użytkowników została przedstawiona w [20].

Jako że ocena użytkowników jest dość trudna do zebrania (konieczność tworzenia ankiety oraz zebrania reprezentatywnej grupy respondentów), wprowadzono miary liczbowe, które odpowiadają na pytanie, jak dobrze działa system biometryczny. Do oceny systemów weryfikacji wykorzystywane są m.in. miary FAR i FRR. FAR (ang. *False Acceptance Rate*) to prawdopodobieństwo z jakim system udzieli nieupoważnionemu użytkownikowi dostępu do chronionych zasobów i jest określone równaniem 1. FRR (ang. *False Rejection Rate*) zaś jest prawdopodobieństwem z jakim system odmówi dostępu użytkownikowi, który jest uprawniony od uzyskania dostępu do chronionych zasobów i wyraża się równaniem 2.

$$FAR = \frac{FN}{FN + TN} \tag{1}$$

gdzie:

FN - (ang. *False Negatives*) liczba próbek, które powinny być zakwalifikowane negatywnie, ale zostały zakwalifikowane pozytywnie, czyli otrzymały dostęp do chronionych zasobów, mimo iż nie posiadały ku temu uprawnień;
TN - (ang. *True Negatives*) liczba próbek, które powinny być zakwalifikowane negatywnie i tak zostały zakwalifikowane, czyli nie posiadały uprawnień i poprawnie nie otrzymały dostępu do zasobów.

$$FRR = \frac{FP}{FP + TP} \tag{2}$$

gdzie:

TP - (ang. *True Positives*) liczba próbek, które powinny zostać zakwalifikowane pozytywnie i tak zostały zakwalifikowane, czyli poprawnie uzyskały dostęp;

FP - (ang. *False Positives*) liczba próbek, które powinny być zakwalifikowane pozytywnie, ale zostały zakwalifikowane negatywnie, czyli nie otrzymały dostępu mimo posiadania uprawnień.

W pracach naukowych dotyczących biometrii zwykle miary te dążą do jednej wartości, a w przypadku gdy miary te są sobie równe, mówić można o EER (ang. *Equal Error Rate*), która wyraża równą wielkość błędu i wynosi tyle, ile błędy FAR i FRR. W systemach rzeczywistych minimalizuje się jeden z błędów, w zależności od typu systemu i miejsca jego implementacji. Inną stosowaną miarą jest dokładność (ang. *accuracy*), która może zostać wyrażona równaniem 3. Wskazuje ona na procentowy udział poprawnych odpowiedzi wśród wszystkich przeprowadzonych weryfikacji.

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \cdot 100\% \tag{3}$$

Oprócz dokładności stosuje się również miary swoistości (ang. *selectivity*, TNR) i czułości (ang. *sensitivity*, TPR), które zostały określone odpowiednio wzorami 5 oraz 4. Wraz z miarą czułości (zwaną również *recall*) zazwyczaj prezentuje się miarę precyzji (ang. *precision*), którą można wyrazić równaniem 6.

$$TNR = \frac{TN}{TN + FP} \tag{4}$$

$$recall = TPR = \frac{TP}{TP + FN} \tag{5}$$

$$precision = \frac{TP}{TP + FP} \tag{6}$$

Precyzję i czułość systemu można też przedstawić za pomocą miary $F1_{score}$, korzystając z zależności przedstawionej równaniem 7. Im wyższa wartość tej miary, tym lepsze działanie systemu (dla optymalnego systemu $F1_{score} = 1$).

$$F1_{score} = 2 \cdot \frac{precision \cdot recall}{precision + recall} \tag{7}$$

W przypadku niezbalansowanego zestawu testowego (przeważająca ilość próbek pozytywnych lub negatywnych) można zastosować dokładność zbalansowaną, którą wyraża się równaniem 8.

$$Acc_B = \frac{TNR + TNR}{2} \tag{8}$$

Aby w sposób wizualny ocenić działanie systemu biometrycznego stosuje się m.in. wykres ROC (ang. *Receiver Operating Characteristic*), który jest zależnością pomiędzy miarą TPR i wynikiem odejmowania $1-TNR$. Jest on szczególnie przydatny w przypadku testowania danego rozwiązania z różnymi parametrami - im bliżej osi OX i OY znajdzie się wykres, tym wyższą gwarantuje skuteczność.

W literaturze podczas analizy działania systemu biometrycznego spotyka się również wykresy histogramów Autentyczny/Fałszywy, które noszą angielską nazwę *Genuine/Impostor Histogram*. Przedstawiają one prawdopodobieństwo (oś OY) z jakim próbka zostanie zakwalifikowana jako autentyczna lub fałszywa w zależności od wyniku (np. wartości progu na osi OX).

Natomiast w systemach identyfikacji ocenia się parametr CCR (ang. *Correct Classification Rate*), który określa stopień poprawnej identyfikacji. Innym istotnym parametrem może być czas potrzebny na wykonanie wszystkich obliczeń w systemie biometrycznym. System identyfikacji osób współpracujący z dużą bazą danych z pewnością będzie dawał odpowiedź w znacznie dłuższym czasie. Z drugiej strony jednak w systemach weryfikacji użytkownicy będą wymagali jak najkrótszego czasu działania, najlepiej w czasie rzeczywistym.

2.5. Wybrane zastosowania systemów biometrycznych

Biometria ma obecnie wiele zastosowań. Z pewnością dalszy jej rozwój sprawi, że lista ta zostanie jeszcze wydłużona:

- Dochodzenia kryminalne – pierwsze i najbardziej podstawowe wykorzystanie biometrii; przestępca, który zostawia pewne ślady na miejscu zbrodni, może zostać odnaleziony przez ich odpowiednią klasyfikację.
- Kontrola paszportowa – paszporty biometryczne, o których już wspomniano wcześniej, są wprowadzane do coraz większej ilości państw, dzięki czemu mamy dostęp do informacji kto, kiedy i gdzie przekracza granicę bez żmudnego przepisywania danych, a także do informacji o tym, czy paszport jest oryginalny i czy na pewno nie został skradziony.
- Dostęp do chronionych zasobów – jedno z nowszych zastosowań, które pojawiło się wraz z rozwojem techniki i miniaturyzacją urządzeń pobierających próbki; chronionym zasobem może być na przykład siłownia, na teren której poprzez weryfikację cechy biometrycznej mogą wejść jedynie zarejestrowani wcześniej użytkownicy. W roku 2019 południowokoreański koncern samochodowy Hyundai zaproponował również odblokowanie i uruchomienie pojazdu za pomocą odcisku palca.
- Rozwiązania mobilne – zastosowanie które pojawiło się wraz z rozwojem urządzeń przenośnych takich jak telefony czy tablety; cecha biometryczna pozwala na zalogowanie się do całego urządzenia lub do wybranej aplikacji.

– Bankowość – biometria w bankowości pozwala na zabezpieczenie środków zgromadzonych na koncie przed dostępem osób niepowołanych; przykładami mogą być mobilne aplikacje bankowe, ale również centra komunikacji z klientem, które oprócz standardowych metod weryfikacji stosują rozpoznawanie głosu, na świecie są również dostępne bankomaty, które weryfikują użytkownika na podstawie różnych cech biometrycznych. Do biometrycznej bankowości można zaliczyć też karty przechowujące wzorzec odcisku palca, które od 2018 roku są testowane przez Mastercard i Visę.
– Ochrona zdrowia – dane biometryczne takie jak zapis EKG może zostać wykorzystany do identyfikacji osób, ale również do postawienia odpowiedniej diagnozy i wprowadzenia właściwego leczenia, można tu również wymienić systemu stałego monitorowania niektórych parametrów, które w przypadku otrzymania nieoczekiwanych wyników natychmiast informują odpowiedni ośrodek zdrowia.
– Rejestracja czasu i obecności – biometria może być wykorzystana również w systemach działających w dużych firmach czy fabrykach; zamiast tradycyjnego podpisania karty obecności lub wczytania identyfikatora można zweryfikować tożsamość na podstawie cech biometrycznych; systemy takie z powodzeniem są stosowane m.in. w Kenii.
– Systemy wielozadaniowe – wśród zastosowań biometrii nie można pominąć indyjskiego systemu Aadhaar. Jest to system, który pojawił się już w 2009 roku i choć do tej pory budzi pewne wątpliwości, szczególnie w zakresie bezpieczeństwa danych oraz praw człowieka, korzysta z niego już prawie 1,3 mld osób. Aadhaar zbiera dane biometryczne oraz demograficzne rezydentów Indii - nie potwierdza więc obywatelstwa. Jest wykorzystywany do spraw urzędowych, w bankowości, do podpisu elektronicznego, a nawet podczas wyborów. Zebrane na potrzeby tego systemu dane (odciski 10 palców, skany obu tęczówek oraz zdjęcie twarzy) tworzą największą bazę danych biometrycznych na świecie.

2.6. Prawne aspekty biometrii

W maju 2018 roku zostało wprowadzenie rozporządzenie Parlamentu Europejskiego, które znane jest szerzej pod nazwą RODO - Ogólne rozporządzenie o ochronie danych [71]. Przyjęcie tego dokumentu miało niebagatelny wpływ na nowe systemy biometryczne oraz proces ich tworzenia, ponieważ dane biometryczne zostały uznane za „specjalną kategorię danych osobowych”. W opracowaniu [62] podkreślono następujące wymagania:

– Osoba może zdecydować, którą część swoich danych udostępni (którą cechę biometryczną).

– Osoba powinna zadeklarować świadomą zgodę na przetwarzanie danych.
– Osoba musi być poinformowana, kto zbiera dane, kto jest ich administratorem, jaki jest cel zbierania danych oraz do jakiego procesu zostaną użyte. Powinno się również określić czas przechowywania danych oraz ewentualne sposoby ich udostępniania podmiotom trzecim.
– Osoba może odmówić podania danych osobowych, a także wycofać zgodę na ich przetwarzanie w dowolnym momencie.

Ważnym elementem jest również anonimizacja zebranych danych biometrycznych. Oznacza to, że zebrane dane nie mogą zostać powiązane z żadną konkretną osobą, np. jej imieniem czy nazwiskiem. Dlatego podczas tworzenia baz danych biometrycznych, użytkownicy otrzymują numery. Dodatkowo podczas udostępniania takiej bazy innym ośrodkom badawczym, można pokusić się o zmiany numerów przydzielonych użytkownikom.

Zanim wprowadzono RODO, opublikowano dokument ISO/IEC FCD 19792 [58], który prezentuje listę potencjalnych zagrożeń dla systemów biometrycznych. Standard ten odnosi się również do spraw związanych z prywatnością danych biometrycznych. Jednym z najbardziej istotnych zagrożeń dla systemu biometrycznego jest utrata próbki, która może powodować dla ofiary straty finansowe i społeczne. Jest to atak na jej prywatność. Dlatego w dzisiejszym cyfrowym świecie ochrona próbki biometrycznej jest tak ważna, szczególnie jeśli weźmie się pod uwagę ograniczoną liczbę znanych, skutecznych i stosowanych cech biometrycznych. Warto też wspomnieć o normie PN:ISO 19092 [57], w której skupiono się na wykorzystaniu różnych modalności biometrycznych w celu zapewnienia bezpieczeństwa systemów bankowych.

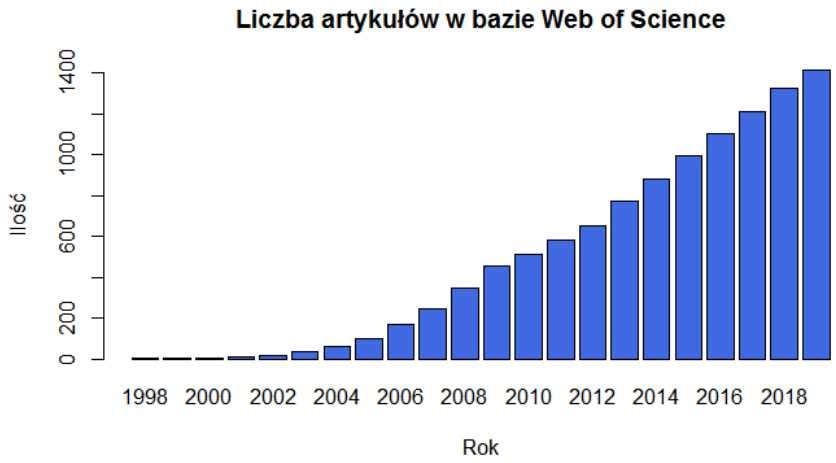
3. Przegląd literatury

Historia badań nad systemami wykorzystującymi obrazy wewnętrznych części dłoni jako cechę biometryczną nie jest tak długa, jak historia użycia odcisków palców czy wizerunku twarzy. Pierwsze doniesienia pochodzące z bazy Web of Science pochodzą z ostatniej dekady XX wieku, a rosnącą popularność odcisków wewnętrznych części dłoni przedstawiono na rysunku 8. Widać na nim, że do końca roku 2019 opublikowano nieco ponad 1400 artykułów. Dla porównania można dodać, że w tym samym okresie czasu opublikowano ponad 20 tysięcy artykułów traktujących o odciskach palców (stan na luty 2020). Można jednak przyjąć, że intensywne badania nad wykorzystaniem obrazu dłoni do identyfikacji osób są prowadzone od blisko 20 lat.

W tym rozdziale przedstawiono przegląd literatury dotyczącej obrazów dłoni jako cechy biometrycznej, składający się na aktualny stan wiedzy. W pierwszej części rozdziału przedstawiono obraz wewnętrznej części dłoni jako cechę biometryczną wraz z jej anatomicznym opisem. Następnie dokonano krytycznej analizy dotychczasowych osiągnięć naukowych dotyczących obrazu dłoni jako cechy biometrycznej. Biorąc pod uwagę liczbę artykułów, zdecydowano się podzielić ten rozdział na mniejsze sekcje dotyczące kolejnych kroków przetwarzania: akwizycji obrazu, przetwarzania wstępnego, wydobycia cech i klasyfikacji. Rozdział kończy się podsumowaniem, w którym Autorka podkreśla najbardziej obiecujące kierunki rozwoju obrazu dłoni jako cechy biometrycznej.

3.1. Obraz dłoni jako cecha biometryczna

Wybór odpowiedniej cechy biometrycznej zależy od różnych czynników. Ich porównanie w zakresie podstawowych wymagań stawianych systemom biometrycznym, zostało przedstawione w tabeli 1. Obserwując zaprezentowane dane, można stwierdzić, nie istnieje jedna idealna cecha biometryczna, która okazałaby się złotym środkiem dla każdego z projektowanych systemów. Wybór tej cechy zawsze zależy od jego specyfiki i konkretnej implementacji. Obrazy wewnętrznych części dłoni dobrze wypadają w zaprezentowanym porównaniu. Wśród ich niewątpliwych zalet zwykle wymienia się następujące:



Rysunek 8. Ilość artykułów z podziałem na lata publikacji w bazie Web of Science, które zawierają w tytule hasło „*palmprint*" [opracowanie własne z lutego 2020]

- są unikatowe – są formowane między 3 a 5 miesiącem ciąży i są różne nawet w przypadku bliźniąt [21];
- mają bogatą strukturę – umożliwia ona znalezienie wielu punktów kluczowych, mogących pomóc w poprawnej identyfikacji [18, 37], wielkość wewnętrznej części dłoni oraz ilość szczegółów pozwalają na zastosowanie w sytuacjach, kiedy dłoń jest częściowo brudna lub powierzchnia skóry jest zniszczona (u osób starszych lub pracowników fizycznych) [28];
- są niezmienne – podczas rozwoju człowieka wzór widoczny na wewnętrznej części dłoni pozostaje bez zmian (za wyjątkiem zmiany wielkości dłoni) [36];
- można je łatwo pobrać – dłonie nie są zakrywane w większości kultur i religii świata (jako wyjątek można wymienić grupę Muzułmanek, które noszą tzw. pełną burkę, zasłaniającą całe ciało od stóp do głów), ponadto nie jest konieczne dotykanie żadnych skanerów;
- charakteryzuje je niewielkie zniekształcenie w przypadku zamykania i otwierania dłoni [42];
- są łatwe w pozycjonowaniu poprzez wyszukanie nasady kciuka oraz innych palców.

Najważniejszymi elementami w strukturze obrazów wewnętrznych części dłoni są bruzdy i fałdy. Rysunek 9 przedstawia główne linie, które są widoczne w tej cesze biometrycznej. Fachowa literatura medyczna udostępnia bardziej

Tabela 1. Charakterystyka wybranych cech biometrycznych [38, 63]

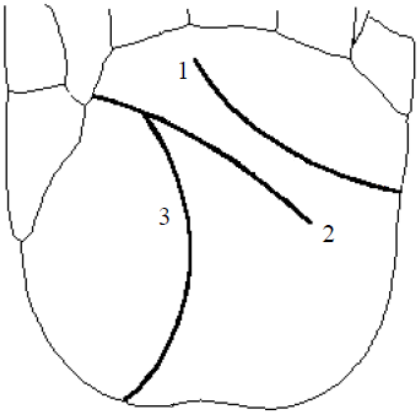
CECHA	UNIWERSAL-NOŚĆ	ODMIEN-NOŚĆ	ŁATWOŚĆ AKWIZYCJI	TRWAŁOŚĆ
DNA	wysoka	wysoka	niska	wysoka
obraz ucha	średnia	średnia	średnia	wysoka
obraz twarzy	wysoka	niska	wysoka	średnia
termiczny obraz twarzy	wysoka	wysoka	wysoka	niska
wzór żył dłoni	średnia	wysoka	wysoka	średnia
odciski palców	średnia	wysoka	wysoka	średnia
chód	niska	niska	wysoka	niska
geometria dłoni	średnia	średnia	wysoka	średnia
tęczówka oka	wysoka	wysoka	średnia	wysoka
obraz wewnętrznej części dłoni	**średnia**	**wysoka**	**średnia**	**wysoka**
siatkówka oka	wysoka	wysoka	niska	średnia
podpis odręczny	średnia	niska	wysoka	niska
głos	średnia	niska	średnia	niska

anatomiczny opis tej części ciała [8]. W porównaniu do grzbietu dłoni, jej wewnętrzna strona charakteryzuje się stosunkowo grubą skórą, nieprzesuwalną i silnie złączoną z podłożem. Podczas zgięcia tworzą się fałdy ograniczone bruzdami, które podczas prostowania dłoni, wygładzają się. Bruzdy na dłoni to tzw. linie chiromantów, którzy korzystając ze zmiennego ich przebiegu, starają się przewidzieć ludzkie losy. Trzema najważniejszymi bruzdami są:

1. bruzda dalsza zgięcia (łac. *linea flexoria distalis*, linia serca) - zaczyna się między palcem wskazującym a palcem środkowym, biegnie nieco powyżej stawów śródręczno-paliczkowych trzech ostatnich palców do brzegu łokciowego ręki;
2. bruzda bliższa zgięcia (łac. *linea flexoria proximalis*, linia głowy) - rozpoczyna się powyżej opuszki dotykowej nasady palca wskazującego i biegnie skośnie ku górze i kłębowi palca małego. Czasami te dwie bruzdy zlewają się w jedną, tworząc tzw. bruzdę małpią;
3. bruzda przeciwstawna kciuka (łac. *linea opponens pollicis*, linia życia) - obejmuje kłąb kciuka.

3.2. Akwizycja obrazu dłoni

Pobranie obrazu do systemu jest pierwszym krokiem przetwarzania. Zwykle w badaniach korzysta się z popularnych i ogólnie dostępnych baz obrazów. Ich użycie sprawia, że prezentowane wyniki są bardziej miarodajne i łatwiejsze do porównania z innymi badaniami, które także korzystały z wybranej bazy danych. Bazom poświęcono oddzielny podrozdział (5.2), a w dalszej części tej sekcji

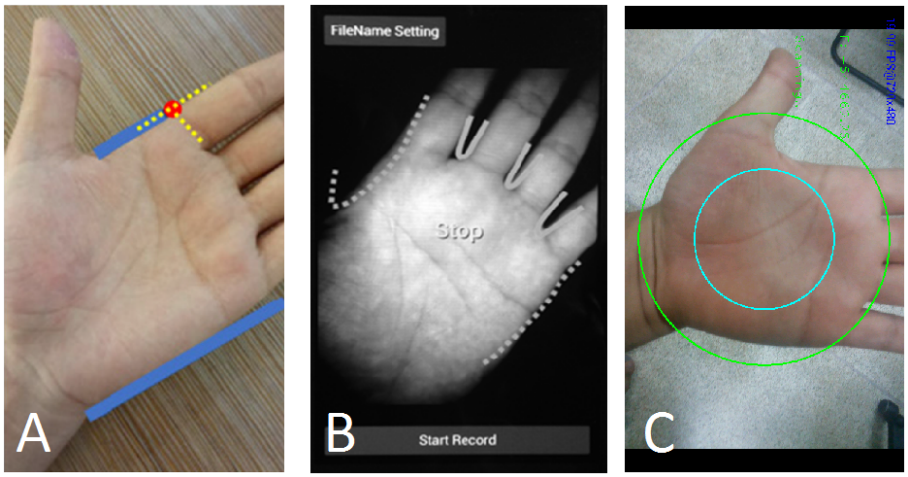


Rysunek 9. Główne linie obrazu wewnętrznej strony dłoni: 1 – linia serca, 2 – linia głowy, 3 – linia życia [65]

przedstawiono artykuły, w których z różnych względów autorzy zdecydowali się samodzielnie pobierać próbki do systemu.

Akwizycja wydaje się szczególnie istotna w przypadku scenariusza mobilnego. Kim w swoim artykule [43] jako jedną z zalet korzystania z odcisków wewnętrznych części dłoni, wymienia możliwość korzystania z wbudowanego czytnika, jakim w telefonie komórkowym jest kamera cyfrowa. Ocenia również liczne implementacje systemów korzystających z tej cechy biometrycznej jako bardzo dobrze działające i osiągające obiecujące rezultaty, jednak funkcjonujące w specyficznym, bardzo mocno nadzorowanym środowisku. Jako przykład takiego nadzoru wymienia konieczność konkretnego ustawienia dłoni podczas pobierania próbki. Natomiast za największe wyzwania stojące przed biometrią obrazów dłoni w ujęciu mobilnym uznaje brak kontroli nad pozycją dłoni, jej oświetleniem oraz różnorodne tło. Na szczególną uwagę zasługuje sposób zaprojektowania graficznego interfejsu użytkownika. Widać na nim kształt, do którego powinna zostać dopasowana dłoń. Ważniejsze linie (między palcami) są reprezentowane liniami ciągłymi, a mniej istotne (dookoła dłoni) liniami kropkowanymi. Wzięto również pod uwagę komfort użytkownika przez obrót całego kształtu o 45°. Podczas pobierania próbki zastosowano również algorytm sprawdzania koloru dłoni. Wykorzystuje on przestrzeń barw $YCbCr$ i na podstawie prostych obliczeń matematycznych (m.in. odległości Euklidesa) decyduje, czy w zaznaczonym fragmencie znajduje się dłoń, czy nie.

Inny przykład graficznego asystenta pomagającego użytkownikowi w odpowiednim umiejscowieniu dłoni przedstawiono w [51]. W prezentowanej tam metodzie wykorzystuje się dwie linie oraz jeden punkt, do których użytkownik musi



Rysunek 10. Przykłady graficznych asystentów A: Leng et al. [51], B: Kim et al. [43] oraz C: Tiwari et al. [70]

dopasować położenie swojej dłoni na podglądzie widocznym na ekranie urządzenia mobilnego. Następnie zaproponowano etap walidacji, czyli sprawdzenia czy dłoń została poprawnie umiejscowiona. W tym celu analizowane są długości przerw między palcami oraz ich odległość od siebie. Dopiero kiedy próbka przejdzie pozytywnie walidację, następują kolejne kroki przetwarzania.

Kolejny przykład graficznego asystenta dla użytkownika można poznać w [70]. Tu z kolei zaproponowano wykorzystanie dwóch okręgów. Wewnętrzny zawiera ROI, zaś zewnętrzny powinien otaczać dłoń i przecinać dolne punkty przestrzeni między palcami. W prezentowanym podejściu użytkownik został zwolniony nawet z konieczności zrobienia zdjęcia. Algorytm wykonuje serię ujęć, a następnie na podstawie kilku parametrów ocenia ich przydatność dla weryfikacji i właśnie najlepszą próbkę przekazuje do kolejnych kroków metody. Na rysunku 10 przedstawiono opisane wcześniej systemy wspomagające poprawne ułożenie dłoni.

3.3. Przetwarzanie wstępne obrazu

Krok przetwarzania wstępnego może wydawać się mniej istotnym niż wydobycie cech czy klasyfikacja, która sprawia, że na końcu działania algorytmu otrzymujemy decyzję o pozytywnej lub negatywnej autoryzacji użytkownika. Należy jednak pamiętać, że podczas przetwarzania wstępnego zmniejszany jest analizowany obszar (wyznaczenie ROI) oraz następuje poprawa jakości obrazu. Krok ten i pewne usprawnienia wprowadzone do metod autoryzacji na tym etapie mogą

znacząco wpłynąć na skuteczność podejmowania decyzji. Może się również okazać, że wybór zbyt skomplikowanej i złożonej obliczeniowo metody przetwarzania wstępnego bardzo zwolni działanie całego systemu.

Autorzy [41] podkreślili etap normalizacji jako kluczowy dla skutecznej weryfikacji. Jak przekonują, normalizacja zmniejsza wariancję jasności pikseli w najbliższym otoczeniu, co jest szczególnie istotne przy niejednorodnym oświetleniu lub cieniach widocznych na obrazie ROI. Ponadto zastosowali też filtr Gaussa, aby pozbyć się niechcianych detali.

Artykuł [85] pokazuje wpływ ostrości próbki na skuteczność weryfikacji. Autorzy w swojej pracy zdecydowali się sprawdzić, czy prawdziwym jest stwierdzenie, iż im ostrzejszy wzór linii na obrazie dłoni, tym skuteczniej można zweryfikować tożsamość osoby. Z przedstawionych badań wynika, że stwierdzenie to jest nieprawdziwe, chociaż nadmierne rozmycie również nie jest pożądanym efektem. Dlatego wprowadzono miarę ostrości krawędzi (ang. *Edge Acutance Value*, EAV), na podstawie której można wybrać taki stopień rozmycia ROI, aby skuteczność działania algorytmu była jak największa.

Z kolei w [4] przedstawiono dedykowany sposób segmentacji dłoni od dalszego planu, co jest szczególnie istotne dla zastosowań w scenariuszu mobilnym. W proponowanej metodzie wykorzystano przestrzeń barw CIELab, która uważana jest za przestrzeń doskonale odzwierciedlającą postrzeganie oka ludzkiego.

W [2] natomiast skorzystano z metody sztucznej inteligencji już na etapie przetwarzania wstępnego. W prezentowanym algorytmie CNN (ang. *Convolutional Neural Network*) została wykorzystana do określenia, o jaki kąt została obrócona dłoń i o jaki kąt należy obrócić obraz, aby wydobyć odpowiedni obraz ROI.

Artykuł [52] opisuje, że rozpoznawanie osób na podstawie dłoni może być przydatne podczas śledztw, w których dowodami są nagrania wideo. W takich okolicznościach bardzo często widoczne są dłonie sprawcy, jednak są one zniekształcone - zgięte, przechylone. W celu „wyprostowania" dłoni zastosowano sieć neuronową o nazwie VGG-16, a dopiero po otrzymaniu właściwego ROI przeprowadzono wydobycie cech i klasyfikację.

W [87] zaproponowano własny detektor, który wykrywał przestrzenie między palcami. Na podstawie jego wskazań wyznaczano obszar zainteresowań. Proces uczenia był bardzo żmudny, bo polegał na ręcznym przydzieleniu etykiet.

Należy jednak pamiętać, że zasadniczą rolą przetwarzania wstępnego jest podkreślenie tych elementów, które będą przydatne podczas kolejnych etapów weryfikacji. Dlatego też w wielu pracach wykorzystuje się rozmycie ukrywające niechciane szczegóły, czy operacje morfologiczne, jak przedstawiono w [26].

3.4. Wydobycie cech

Jednym z pierwszych dostępnych artykułów traktujących o rozpoznawaniu osób na podstawie obrazu dłoni jest publikacja autorstwa Junichi Funady i in. [27], w której autorzy stosują dokładnie te same techniki, które są używane podczas analizy odcisków palców. Autorzy przedstawili system ścieniający obraz linii papilarnych dłoni i wykrywający tzw. minucje. Są to punkty charakterystyczne linii papilarnych (np. początek, zakończenie, oczko, haczyk) opisane dokładnie w książce [30].

Bardzo wcześnie zaczęto również stosować filtr Gabora. Może on być implementowany w systemach korzystających z różnych cech biometrycznych do wydobycia cech tekstury [66], a także do oceny żywotności próbki [81]. Sposób jego działania można przedstawić za pomocą równania 9.

$$\begin{gathered} G(x, y, \Theta, u, \sigma) = \\ = \frac{1}{2\pi\sigma} exp\Big\{ \frac{-x^2}{2\sigma^2} + \frac{-y^2}{2\sigma^2} \Big\} exp\{2\pi i(ux\cos\Theta + uy\sin\Theta)\} \end{gathered} \tag{9}$$

gdzie:

x, y – współrzędne względem osi OX i OY;
$i = \sqrt{-1}$;
u – częstotliwość sinusoidy;
Θ – kierunek funkcji;
σ – odchylenie standardowe.

Podejście to zostało przeniesione do systemów korzystających z obrazów dłoni w 2002 roku [44] i w latach kolejnych [84]. W obu tych artykułach podkreślony został fakt popularności tego filtru i łatwości jego wykorzystania. Wskazano również, że to analiza tekstury powinna być kierunkiem rozwoju obrazów dłoni jako cechy biometrycznej, a nie np. analiza samych linii głównych. Te bowiem mogą być bardzo podobne do siebie dla dwóch zupełnie innych osób. Autorzy w swoich pracach używają różnych wartości parametrów filtru, w pierwszym przypadku są to: $u = 0,1833$, $\Theta = \pi/4$, $\sigma = 2,8090$, natomiast w drugim $u = 0,0916$, $\Theta = \pi/4$, $\sigma = 5,6179$. W [88] również użyto filtru Gabora. W tym przypadku jednak zdecydowano się wydobywać cechy z większego niż standardowe (o wielkości 3×3) sąsiedztwa. Także w przypadku artykułu [25] wykorzystano filtr Gabora. W tej jednak pracy zdecydowano połączyć go z lokalnym deskryptorem, jakim jest metoda Lokalnych Wzorców Binarnych (ang. *Local Binary Patterns*, LBP). Natomiast w [77] połączono filtr Gabora z techniką PCA (ang. *Principal Line Analysis*).

Kolejną grupę artykułów dotyczących analizy tekstury są te, które korzystają z transformat i przekształceń. W [32, 33] zaprezentowano wykorzystanie dyskretnej transformaty falkowej (ang. *Discrete Wavelet Transform*, DWT) do wydobycia

cech z obrazu dłoni. Wymieniono również zalety DWT w stosunku do innych popularnych transformat: transformaty cosinusowej czy transformaty Fouriera. Pokazano również, że próbki dwóch osób mogą się różnić na dwóch poziomach: linii głównych oraz linii pobocznych. Gdy analizuje się cały obraz holistycznie, nie można rozróżnić dwóch obrazów dłoni, na których linie główne mają podobny kształt. W związku z tym zaproponowano wykonanie DWT nie na całym obrazie, ale na blokach zawierających jego części. W ten sposób analizie poddaje się fragmenty linii głównych, ale przede wszystkim ułożenie linii pobocznych.

Inne podejście zaproponowano w [60], gdzie do wydobycia cech użyto transformaty Hough. Jej cechą charakterystyczną są szczyty (jaśniejsze miejsca w macierzy wyjściowej) w miejscach, gdzie w obrazie źródłowym znajduje się najwięcej linii prostych. Do wektora cech wprowadzono w czasie eksperymentów 1, 2 lub 3 najjaśniejsze punkty z macierzy wyjściowej. Eksperyment korzystający z 3 punktów charakterystycznych jednocześnie gwarantował najbardziej skuteczną identyfikację.

W [11] przedstawiono wykorzystanie transformaty ślimakowej do wydobycia cech z obrazu dłoni. Zaprezentowane w artykule obliczenia stanowią matematyczny dowód na to, że ta metoda jest odporna na zmianę jasności obrazu, a także na mogące się pojawić na obrazie szumy.

Autorzy [80] wykorzystali miarę energii tekstury. Głównym elementem tego podejścia była operacja splotu macierzy - obraz wejściowy ROI został spleciony z maską. Odpowiednie maski podkreślały istnienie linii pionowych, poziomych oraz pochylonych o 45°i 135°. Co ważne operacja ta była wykonywana globalnie (dla całego obrazu) oraz lokalnie (dla 64 mniejszych, nieprzecinających się bloków), a następnie jej wyniki włączono do jednowymiarowego wektora cech. System jednak został tak zoptymalizowany, że najpierw wykorzystywano cechy globalne i dopiero w przypadku gdy były one wystarczająco podobne, analizowano cechy lokalne.

W [17] skupiono się na cechach koloru wzbogaconych cechami tekstury. Zaproponowano połączenie dwóch metod: metodę PCA (ang. *Principal Component Analysis*), która po pewnej modyfikacji wykonywała znacznie mniej operacji, co z kolei zmniejszało czas działania, oraz metodę HOG (ang. *Historgam of Oriented Gradients*). Do wykonania badań została użyta baza zawierająca 252 obrazy. Okazało się, że proponowana fuzja pozwoliła na osiągnięcie wyższej skuteczności niż obie metody zastosowane oddzielnie.

Oprócz informacji zawartych w obrazie wewnętrznej strony dłoni, często stosuje się cechy geometryczne. Takie podejście zaprezentowano w [14], w którym to podejściu obliczano powierzchnie różnych części dłoni, np. poszczególnych palców czy powierzchnię między charakterystycznymi punktami (końcówka palca, podstawa palca). W kolejnych artykułach [15, 45] zaprezentowano fuzję

cech geometrycznych i teksturowych. Następnie wykrywano dwa obszary zainteresowań: jeden kwadratowy od wydobycia cech teksturowych i jeden w kształcie wielokąta do wydobycia cech geometrycznych. Wierzchołkami tego wielokąta były punkty charakterystyczne takie jak punkty między poszczególnymi palcami czy punkty w przestrzeniach między palcami. Kształt dłoni był przechowywany w postaci 15-elementowego wektora. Zawierał on siedem współrzędnych punktów względem osi X, siedem współrzędnych punktów względem osi Y oraz współczynnik prostokątności dłoni definiowany jako stosunek długości środkowego palca do szerokości dłoni.

W [65] zaproponowano system identyfikacji korzystający z geometrii linii papilarnych dłoni. Jako cech wytypowanych do porównania autorzy używają linii zawartych w obrazach oraz punktów znajdujących się na ich końcach. Dla każdej linii porównywane są współrzędne początku, końca, nachylenie między punktami, przecięcie linii z osią współrzędnych oraz długość linii obliczana przez wykorzystanie odległości Euklidesa.

Autorzy [73] oraz [76] użyli algorytmu SIFT (ang. *Scale-Invariant Feature Transform*) na etapie wyodrębniania cech. Algorytm ten jest z powodzeniem wykorzystywany w wielu zastosowaniach przetwarzania obrazów. Jego główną ideą jest znalezienie punktów kluczowych w obrazie, a następnie porównanie tych punktów z zestawem punktów kluczowych innego obrazu.

Inne podejście zaprezentowano w [12], w którym to artykule wykorzystuje się zmarszczki widoczne na obrazie dłoni w celu uzyskania informacji o tożsamości osoby. Zmarszczka została określona jako podłużny, wąski element obrazu, który charakteryzuje się dużym odchyleniem standardowym w stosunku do obszarów tła i małym odchyleniem w stosunku do obszarów należących do zmarszczki. System ten jednak nie korzystał z rzeczywistych próbek, ale z wydruków przedstawiających wewnętrzne części dłoni.

W kolejnym artykule [47] zaprezentowano hybrydowe podejście do wydobywania cech, w którym analizowano jednocześnie cechy kształtu i tekstury. Skupiono się również na etapie łączenia cech, gdzie porównano SVM, sieci neuronowe i klasyfikatory będące drzewami decyzyjnymi. Do wydobycia cech teksturowych wykorzystano popularną dyskretną transformację cosinusową (ang. *Discrete Cosine Transform*, DCT). Niewątpliwą jej zaletą jest to, że spora część otrzymanych w jej wyniku współczynników jest bliska zeru i może zostać pominięta w dalszym działaniu. W tym podejściu natomiast jako cechę całego obrazu przyjmuje się odchylenie standardowe istotnych (różnych od zera) współczynników otrzymanych w wyniku zastosowania DCT. Oprócz cechy teksturowej w wektorze cech znajdują się też te geometryczne opisane dokładniej w [24]:

- *perimeter* – obwód dłoni;
- *solidity* - stosunek pikseli wewnątrz obiektu do pikseli wewnątrz wielokąta opisanego na obiekcie;

– *extent* - stosunek powierzchni obiektu do powierzchni opisanego prostokąta;
– *eccentricity* - opisuje stopnień rozciągnięcia dłoni (jeśli obiekt jest rozciągnięty, ma dużą wartość tego parametru (linia ma $eccentricity = 1$), obiekt okrągły ma małą wartość tego parametru (koło ma $eccentricity = 0$);
– odległości x, y punktu środkowego dłoni mierzone od granic obiektu;
– *convex area* - powierzchnia wielokąta opisanego na dłoni;
– 4 długości palców;
– 8 szerokości palców mierzonych na przegubach;
– szerokość dłoni;
– długość całej dłoni;
– długość dłoni do wysokości nasady palców;
– powierzchnia dłoni.

Wszystkie te cechy są przechowywane we wspólnym, 24-elementowym wektorze i wykorzystane do identyfikacji.

Ciekawym podejściem do analizy obrazów dłoni jest użycie operacji statystycznych. W takich przypadkach ROI jest traktowana jako macierz liczb. W [1] wykorzystano entropię Shannona obliczoną odpowiednio dla kolejnych bloków obrazu o rozmiarach 3×3, 5×5, 7×7 oraz 9×9.

Z kolei w [54, 55] wykorzystano teorię fraktali. Autorzy zaproponowali obliczanie wielkości fraktali dla poszczególnych części obrazu ROI, co pozwala na ocenę stopnia różnorodności i przerywania tekstury. Natomiast w [56] wykorzystano macierz zbieżności poziomów szarości (ang. *Grey Level Cooccurrence Matrix*), która wskazuje na prawdopodobieństwo wystąpienia takiego samego poziomu szarości dla specyficznej pary pikseli.

Kolejny artykuł [16] był dedykowany rozwiązaniom mobilnym. Zaproponowano w nim nowe podejście do wydobycia cech, które gwarantowało dużą szybkość i skuteczność działania przy wykorzystaniu niewielkiej ilości zasobów obliczeniowych. W badaniu użyto bazy danych składającej się z 250 obrazów. Identyfikacja była oparta na cechach analogicznych do falek Haar'a (algorytm Viola-Jones stosowany do rozpoznawania twarzy), jednak w tym przypadku poszczególnym fragmentom przypisano wartości -1, 0 lub 1 tworząc tym samym maskę reprezentującą obraz ROI. W [18] przedstawiono rozwinięcie tej metody, a także skuteczną fuzję z inną cechą biometryczną, kostkami palców dłoni.

Artykuł [13] przedstawia podejście wykorzystujące algorytm SAX (ang. *Symbolic Aggregate approXimation*) na etapie wyodrębniania cech, który to pozwala na kwantyzację wartości jasności obrazu i przedstawienie ROI w postaci ciągu liter. W tym przypadku nie przeprowadzano kwantyzacji na poziomie bitowym, ale w większych blokach. W każdym z bloków obliczona została średnia i to ona została poddana kwantyzacji na wybranej ilości poziomów (w tym przypadku 4). Wykorzystanie algorytmu SAX powoduje więc „przetłumaczenie" obrazu na kod znaków, co sprawia, że zwiększa się bezpieczeństwo przechowywanej próbki.

3.5. Klasyfikacja cech

Najbardziej ogólnie można stwierdzić, że metody klasyfikacji w systemach rozpoznawania osób na podstawie obrazów dłoni można podzielić na dwie grupy. Pierwsza to miary odległości, a drugą stanowią metody uczenia maszynowego, w tym sieci neuronowe.

Mogłoby się wydawać, że proste miary odległości będą mało skuteczne w przypadku rozpoznawania tak skomplikowanych i bogatych w cechy obrazów, jakimi są obrazy wewnętrznej części dłoni. Jednak są one stosowane w wielu znanych z literatury metodach. W [46] i [53] użyto odległości Hamminga. Z kolei w [43] do klasyfikacji wykorzystano odległość chi-kwadrat. Dużą popularnością cieszy się również odległość Euklidesa, którą zastosowano na przykład w [79, 82]. Kolejne algorytmy do klasyfikacji używają odległości Manhattan [3] lub odległości kątowej [22]. Te mniej skomplikowane miary są bardzo często implementowane w urządzeniach o mniejszej mocy obliczeniowej, a więc również w urządzeniach mobilnych.

Drugą grupę stanową metody, które przed zastosowaniem należy nauczyć przy pomocy zbioru próbek uczących. Wśród nich wymienia się m.in. SVM (ang. *Support Vector Machine*) zastosowane w [68, 86], algorytm kNN (ang. *k-Nearest Neigbours*) użyty w [83, 75] czy algorytm *Random Forest* wykorzystany w [56]. W tej grupie należy również wymienić wszystkie sieci neuronowe, które wraz z rozwojem sztucznej inteligencji coraz częściej są implementowane w wielu zastosowaniach. Wykorzystanie sieci RFN (ang. *Rectified Factor Networks*) pokazano w [50], w [29, 2] wykorzystano sieć CNN (ang. *Convolutional Neural Network*), w [89] przedstawiono implementację opartą o DDCN (ang. *Discriminative Deep Convolutional Network*), natomiast w [64] zaprezentowane zostało działanie sieci DHN (ang. *Deep Hashing Network*).

3.6. Podsumowanie aktualnego stanu wiedzy

Podejścia opisane we wcześniejszych sekcjach przedstawiono częściowo również w tabeli 2, dzieląc publikacje w zależności od scenariusza, jakiego dotyczą. Pierwsza część tabeli dotyczy rozwiązań dedykowanych komputerom osobistym, druga wyłącznie rozwiązaniom mobilnym. W podsumowaniu aktualnego stanu wiedzy zdecydowanie pomagają artykuły przeglądowe, które traktują o biometrycznej weryfikacji osób na podstawie obrazu dłoni. Jednym z takich wartościowych artykułów jest praca [90], w której autorzy pokusili się o podsumowanie dotychczasowych osiągnięć w tej dziedzinie ze szczególnym uwzględnieniem ostatnich 10 lat. Autorzy potwierdzają, że wykorzystanie obrazu dłoni jest obiecującym podejściem do weryfikacji tożsamości i powinno być kontynuowane

podczas dalszych badań. Jest to rozwiązanie bezpieczne, stabilne, jednak nadal pozostawia wielkie pole do popisu dla naukowców. Część badań prowadzi się w kierunku poprawy metod przetwarzania wstępnego (wyznaczenie ROI, ale też problemy związane z segmentacją tła), inne w kierunku wyznaczenia nowych cech z tekstury, koloru lub geometrii linii papilarnych dłoni. Odrębną część badań stanowią te, które odnoszą się do etapu klasyfikacji, nierzadko z użyciem metod uczenia maszynowego. Podobne wnioski wysnuli autorzy [74], którzy dodatkowo podkreślili nowy i coraz bardziej potrzebny trend, jakim jest wykorzystanie urządzeń o mniejszej mocy obliczeniowej do prowadzenia weryfikacji osób. W ten sposób zaznaczyli, że rozwój systemów mobilnych identyfikacji opartych o obrazy dłoni jest jak najbardziej zasadne i wartościowe.

W tym rozdziale został przedstawiony przekrój metod stosowanych w identyfikacji osób na podstawie obrazów dłoni. Najbardziej popularne rozwiązania to wykorzystanie cech tekstury, koloru i kształtu. Bardzo często stosuje się również rozwiązania hybrydowe, które łączą ze sobą wyżej wymienione rodzaje cech. System taki można już zakwalifikować do biometrii multimodalnej - jest to modalność na poziomie analizowanych cech. Biometria multimodalna ma wiele zalet, które zostały już wcześniej omówione (rozdział 2.3.) Coraz większą uwagę poświęca się również podejściom kodującym ROI obrazu dłoni w postaci ciągu znaków. Za wykorzystaniem kodu przemawia również konieczność zapewnienia bezpieczeństwa próbki biometrycznej. Jeśli zostanie ona przechowana w postaci ciągu znaków, nie będzie można odtworzyć samego wzorca, ani nie będzie trzeba go przechowywać.

Dzięki przedstawionej w rozdziale analizie, podczas tworzenia własnych rozwiązań Autorka postanowiła skupić się głównie na wykorzystaniu cech teksturowych. Zgodnie jednak z obecnymi trendami, część proponowanych metod wykorzystuje cechy hybrydowe, metody statystyczne oraz kodowanie.

Tabela 2. Porównanie wybranych metod state-of-the-art

Publikacja	Scenariusz	Baza danych	Przetwarzanie wstępne	Ekstrakcja cech	Klasyfikacja	Skuteczność
Zhang et al. [84]	PC	PolyU	rozmycie Gaussa	filtr Gabora	odległość Hamminga	EER = 0,6%
Imitaz et al. [32]	PC	PolyU, IITD	korekcja jasności	2D-DWT	suma najmniejszych kwadratów	do 99%
Ray et al. [60]	PC	PolyU	operator Sobel progowanie	transformata Hough	odległość Manhattan	powyżej 90%
El-Tarhouni et al. [25]	PC	PolyU	progowanie	LBP filtr Gabora	kNN	do 98%
Mokni et al. [56]	PC	PolyU IITD CASIA	Steerable filter progowanie	cechy oparte na fraktalach	Random Forest	98%
Tabejamaat et al. [66]	PC	PolyU	rozmycie Gaussa	filtr Gabora	odległość kątowa	do 99%
Dubey et al. [22]	PC	PolyU, IITD	rozmycie Gaussa	kod oparty na banku odpowiedzi filtru Gabora	odległość kątowa	99%
Kumar [46]	PC	CASIA	normalizacja	DWT	odległość Hamminga	EER=1,17%
Ahmadi et al. [2]	PC	THUPALMLAB	CNN	transformata Hough	własna miara podobieństwa MMC-matching algorithm	EER=0,04%
Matkowski et al. [52]	PC	CASIA, IITD	CNN	FERnet	SVM, kNN Softmax	do 99%
Choraś et al. [18]	mobilny	własna baza	weryfikacja koloru dłoni	PCA	odległość Euklidesa	EER=1,7%
Moco et al. [53]	mobilny	IT dataset	binaryzacja Otsu normalizacja koloru	OLOF - Orthogonal Line Ordinal Features	odległość Hamminga	FRR=9,27% FAR=0,03%
Kim et al. [43]	mobilny	własna baza	konwersja do przestrzeni YCbCr	filtr Gabora	odległość chi-kwadrat	EER=2,88%
Fang [26]	mobilny	własna baza	progowanie operacja ścieniania	LEM - Line Edge Map	odległość Hamminga	EER=4,5%
Ungureanu et al. [73]	mobilny	własna baza	LBP	SIFT	kNN	90%
Tiwari et al. [70]	mobilny	własna baza	normalizacja ocena jakości próbki	SIFT, ORB	własna miara podobieństwa	EER=5,55%
Leng et al. [51]	mobilny	własna baza	weryfikacja znalezienia dłoni na obrazie	filtr Gabora	odległość Hamminga	EER powyżej 2%
Zhang et al. [87]	mobilny	własna baza	własny detektor D	SiameseMobileNetwork	własny klasyfikator C	90%

4. Własne propozycje metod rozpoznawania osób

W tym rozdziale przedstawiono proponowane przez Autorkę algorytmy i metody, które mogą zostać zaimplementowane w biometrycznym systemie rozpoznawania użytkowników przy pomocy obrazu wewnętrznej części dłoni na urządzeniach mobilnych. Po opracowaniu poszczególnych metod przeprowadzono eksperymenty. Protokół ich prowadzenia został opisany w kolejnym rozdziale, zaś w następnym przedstawiono otrzymane wyniki.

4.1. Propozycja algorytmu wyznaczania rejonu zainteresowań

Krok wstępnego przetwarzania obrazu jest niezwykle ważny w całym systemie rozpoznawania wzorców. Jednym z głównych zadań tego kroku jest wydobycie ROI (ang. *Region of Interest*). Wyznaczenie mniejszego obszaru poprawia czas działania systemu (brak konieczności analizy całego obrazu).

Poszczególne kroki algorytmu zostały przedstawione na rysunku 11. Rysunek obrazuje wykorzystanie jednego algorytmu dla dwóch różnych baz obrazów, lewa część dotyczy bazy IITD, prawa z kolei bazy PolyU. Dane wejściowe stanowi obraz wewnętrznej części dłoni. Pierwszym krokiem algorytmu jest operacja progowania. Dzięki temu, że tło jest bardzo ciemne w próbkach obu baz, wykorzystano binaryzację z progiem równym 90. Dzięki temu wszystkie piksele o jasności większej niż 90 zostały zaznaczone kolorem białym. Biały obszar natomiast został uznany za pierwszy plan, czyli dłoń. Kolejnym etapem była morfologiczna operacja zamknięcia. W ten sposób pozbyto się niechcianych nieciągłości. Następnie wyznaczono kontury na obrazie binarnym, a najdłuższy kontur został uznany za obrys dookoła dłoni i zaznaczony zielonym kolorem na rysunku. Na podstawie stworzonego konturu wyznaczone są punkty w przestrzeniach między palcami wskazującym i środkowym (punkt A) oraz serdecznym i małym (punkt B). Punkty oznaczono kolorem niebieskim na rysunku. Następnie została poprowadzona linia prosta między punktami A i B. Obraz został obrócony w taki sposób, aby stworzona linia była pionowa (dla bazy PolyU) lub pozioma (baza

IITD). Kolejnym krokiem jest wyznaczenie kwadratu o zadanym boku w ustalonej odległości od linii (kolor czerwony na obrazku). Ostatnim krokiem algorytmu było wycięcie zaznaczonego obszaru jako ROI (E). Wielkość tego obszaru można modyfikować, jednak w większości badań ROI stanowił obraz o rozmiarze 128×128.

4.2. Propozycja metody opartej na histogramie gradientów

Po dokonaniu analizy bieżącej literatury, Autorka postanowiła sprawdzić, czy i jak wpłynie na biometryczną rozpoznawanie osób zmiana jednego z etapów analizy obrazu. Jako krok do zmodyfikowania zostało wybrane przetwarzanie wstępne obrazów dłoni. Aby jednak przeprowadzić takie testy, należało stworzyć pierwszy system biometrycznego rozpoznawania osób. System ten wydobycia cech używał metody HOG (ang. *Histogram of Oriented Gradients*), a do klasyfikacji cech wykorzystywał odległość Euklidesa wyrażaną równaniem 11. Metoda HOG to popularna metoda analizy obrazu oraz zapisu wideo. Wykorzystuje ona podział obrazu na bloki, a następnie w każdym bloku analizuje gradient koloru. Obliczone zostają wielkość oraz kierunek gradientu i to właśnie one zostają włączone do wektora cech. Poszczególne etapy działania tego algorytmu zostały przedstawione na rysunku 12. Do porównania działania algorytmów przetwarzania wstępnego wytypowane zostały cztery metody, które w przeglądzie literatury pojawiały się bardzo często:

- rozmycie Gaussa, którego działanie opisuje równanie 10;
- filtr medianowy, który przypisuje poszczególnym pikselom wartość równą medianie z wybranego sąsiedztwa;
- filtr bilateralny, którego cechą charakterystyczną jest bardzo dobre zachowywanie krawędzi;
- wyostrzenie, które zostało zrealizowane przez odjęcie obrazu rozmytego filtrem Gaussa od obrazu źródłowego.

Przykładowe wyniki działań wszystkich czterech metod zawiera rysunek 13.

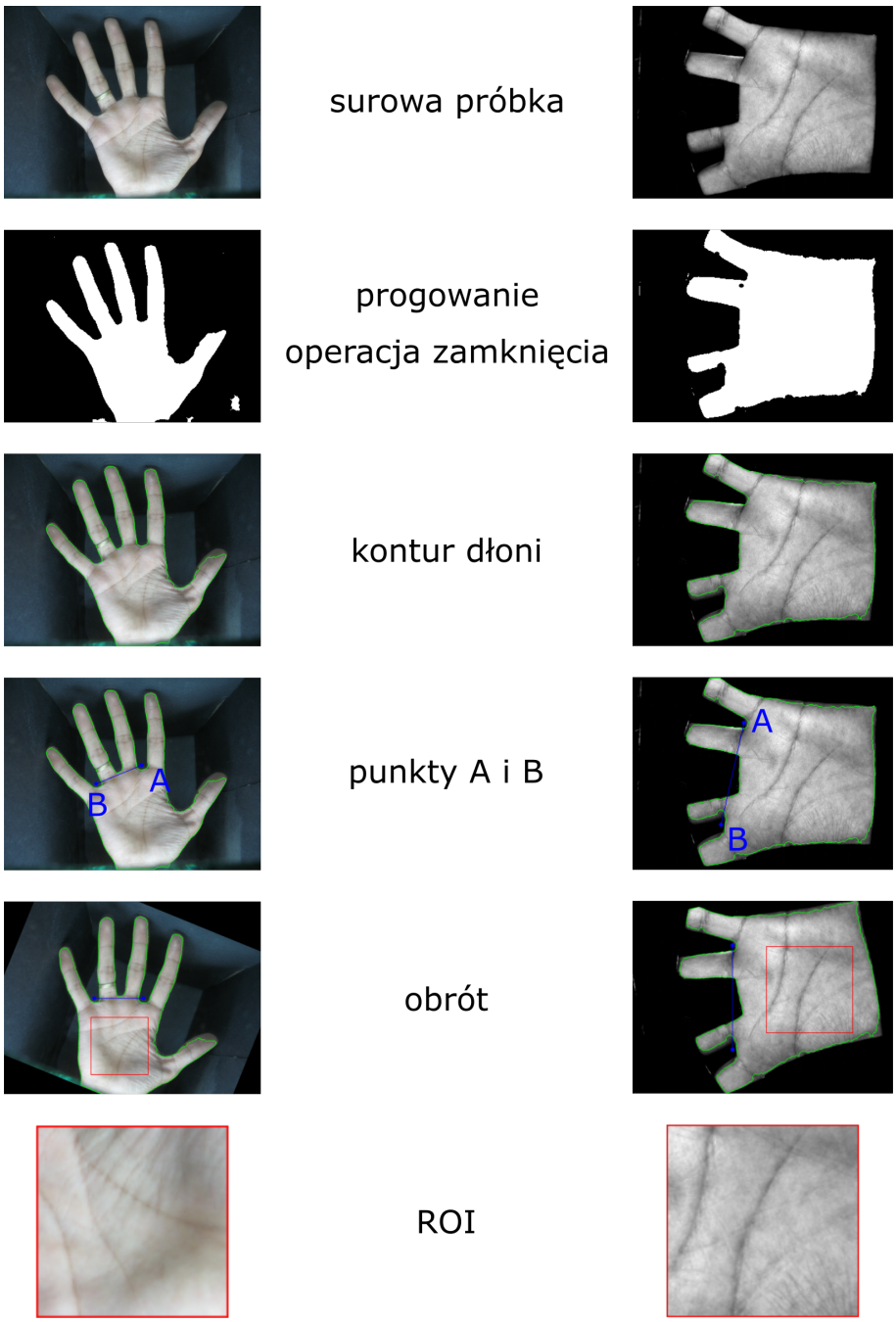
$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{\frac{-x^2+y^2}{2\sigma^2}} \tag{10}$$

gdzie:

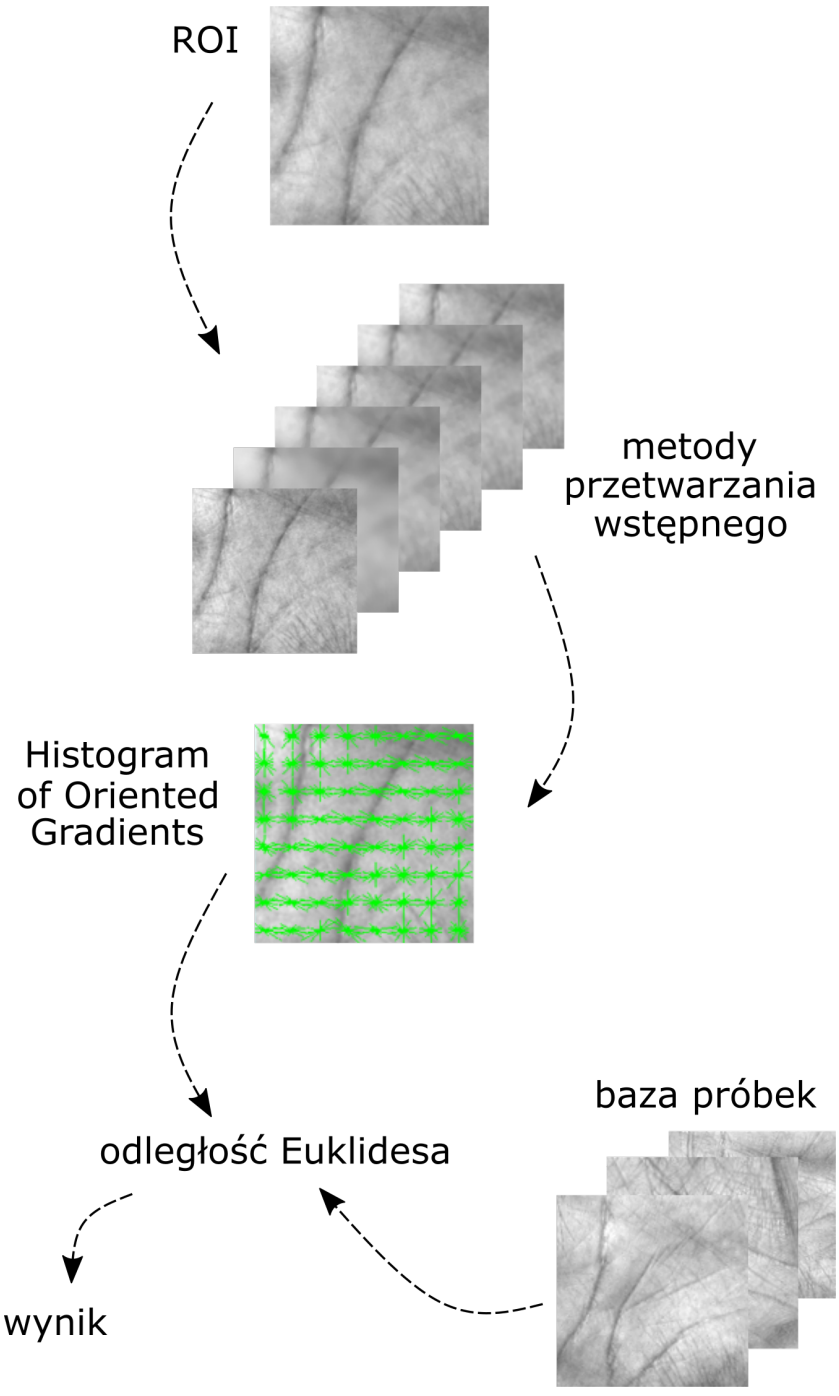
x, y – współrzędne punktu względem osi X i Y;
σ – odchylenie standardowe.

$$d(p, q) = \sqrt{(p_x - q_x)^2 + (p_y - q_y)^2} \tag{11}$$

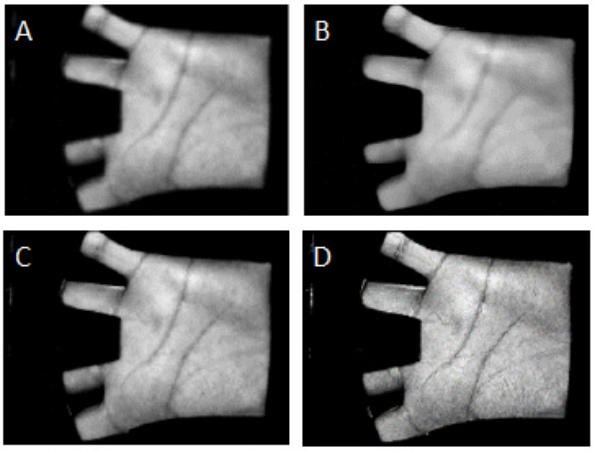
gdzie:



Rysunek 11. Kolejne kroki algorytmu wydobycia ROI (bazy PolyU oraz IITD) [opracowanie własne]



Rysunek 12. Kolejne kroki przetwarzania [opracowanie własne]



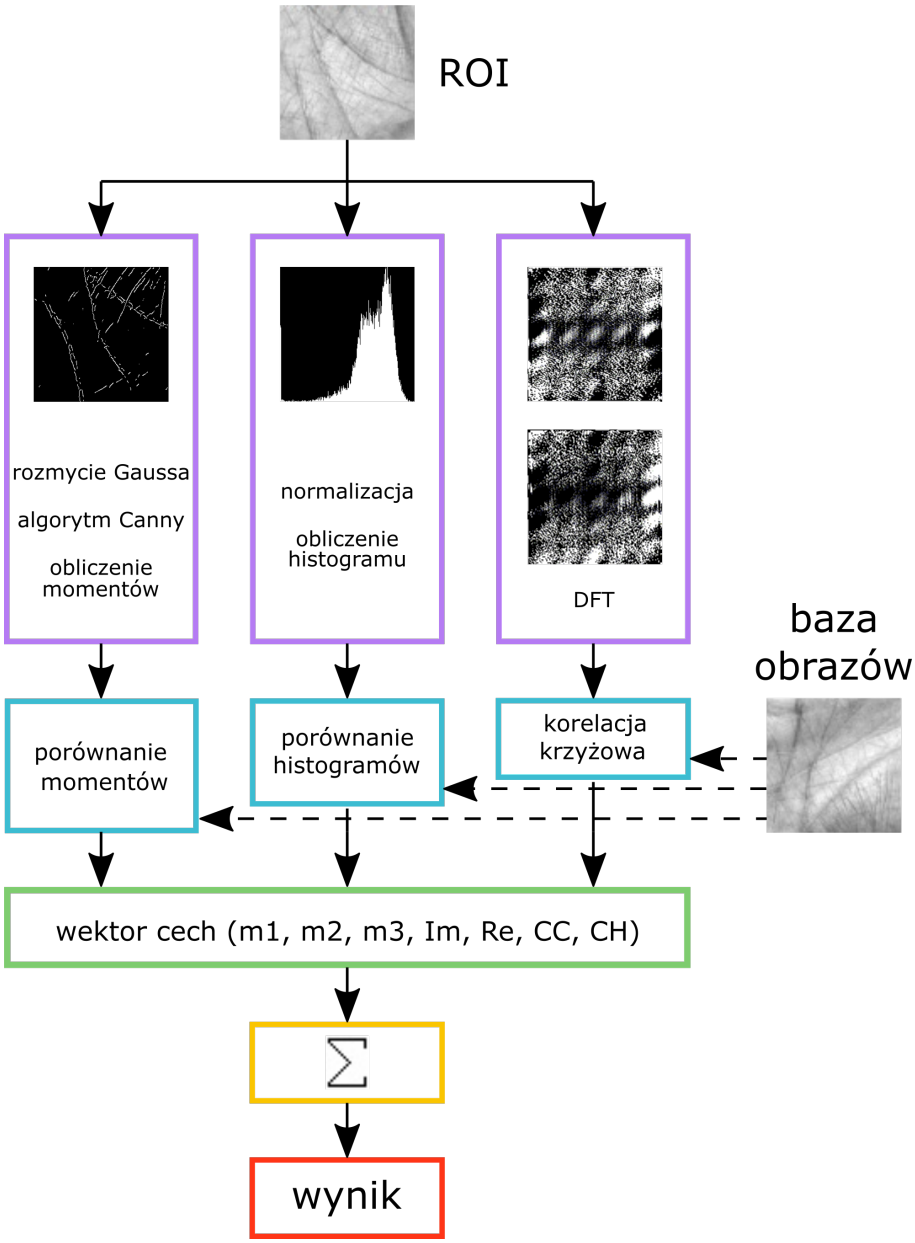
Rysunek 13. Obrazy z bazy PolyU wstępnie przetworzone porównywanymi metodami (A: rozmycie Gaussa, B: filtr medianowy, C: filtr bilateralny, D: wyostrzenie) [opracowanie własne]

p – punkt z wektora cech analizowanego obrazu (p_x – współrzędna osi X, p_y – współrzędna osi Y);
q – punkt z wektora cech obrazu z bazy danych (q_x – współrzędna osi X, q_y – współrzędna osi Y);

4.3. Propozycja metody hybrydowej Color-Texture

W kolejnej metodzie, która została nazwana metodą hybrydową Color-Texture (CT), wykorzystano fuzję cech, która miała zapewnić podwyższoną skuteczność działania systemu oraz jego większą uniwersalność. Do fuzji wybrano cechy koloru oraz tekstury. Schemat przetwarzania w systemie został przedstawiony na rysunku 14. Proponowany system korzysta z wcześniej opisanego algorytmu wyznaczania ROI. Wykorzystano tu trzy rodzaje cech, do każdego z nich wybrano również inne metody przetwarzania wstępnego. Etap przetwarzania wstępnego na rysunku14 został zaznaczony kolorem fioletowym. Pierwszą grupą są cechy tekstury, w tym przypadku momenty (ang. *raw moments*). Przed ich obliczeniem obraz został wygładzony filtrem Gaussa, a następnie został użyty algorytm Canny do wyznaczania krawędzi. Dopiero posiadając zestaw krawędzi, można obliczyć momenty, korzystając ze wzoru opisanego równaniem 12.

$$M_{ji} = \sum_x \sum_y I(x,y) x^i y^j \tag{12}$$



Rysunek 14. Kolejne kroki przetwarzania w proponowanym algorytmie [opracowanie własne]

gdzie:

x, y – współrzędne punktu względem osi X i Y;
i, j – numery momentu;
I – jasność piksela.

W proponowanej metodzie wykorzystane są trzy cechy oparte na momentach i są to: powierzchnia (M_{00}) oraz współrzędne x i y punktu środka masy ($\overline{x}$, $\overline{y}$), wyrażane odpowiednio przez równanie 13 oraz równanie 14.

$$\overline{x} = \frac{M_{10}}{M_{00}} \tag{13}$$

$$\overline{y} = \frac{M_{01}}{M_{00}} \tag{14}$$

Jednak wyniki przedstawionych równań nie są bezpośrednio włączane do wektora cech. Za pomocą tych samych równań oblicza się momenty także dla obrazu bazowego (wprowadzonego do systemu w fazie uczenia, zweryfikowanego jako pozytywny). Natomiast do wektora cech trafiają stosunki wartości momentów obliczonych dla obrazu weryfikowanego oraz bazowego zgodnie z równaniami 15-17. Etap porównania momentów może już zostać zaliczony do etapu wydobycia cech, który został oznaczony na rysunku 14 kolorem niebieskim.

$$m_1 = \begin{array}{ll} A_1/A_2 & \text{dla } A_2 > A_1 \\ A_2/A_1 & \text{przeciwnie} \end{array} \tag{15}$$

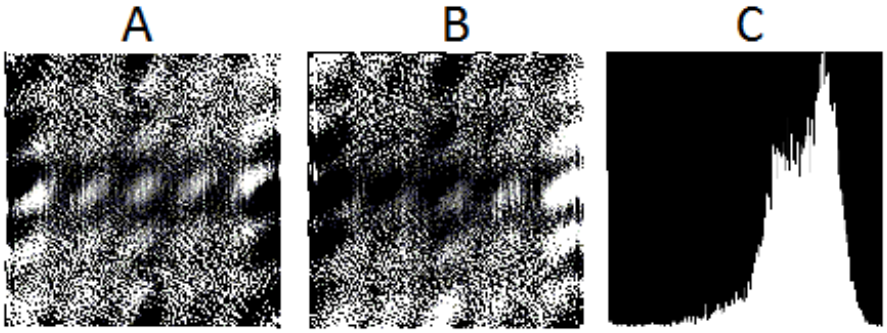
$$m_2 = \begin{array}{ll} X_1/X_2 & \text{dla } X_2 > X_1 \\ X_2/X_1 & \text{przeciwnie} \end{array} \tag{16}$$

$$m_3 = \begin{array}{ll} Y_1/Y_2 & \text{dla } Y_2 > Y_1 \\ Y_2/Y_1 & \text{przeciwnie} \end{array} \tag{17}$$

gdzie:

A_1, A_2 – momenty M_{00} (powierzchnia) dla obrazu weryfikowanego oraz bazowego;
X_1, X_2 – wartości $\overline{x}$ (współrzędna x punktu środka masy) dla obrazu weryfikowanego oraz bazowego;
Y_1, Y_2 – wartości $\overline{y}$ (współrzędna y punktu środka masy) dla obrazu weryfikowanego oraz bazowego.

Kolejna cecha jest zależna od koloru obrazu. Aby ją wyznaczyć, zostaje obliczony histogram. Zanim jednak do tego dojdzie, należy przeprowadzić normalizację obrazu, dzięki której obraz będzie wykorzystywał cały dostępny zakres kolorów (dla obrazu w skali szarości będzie to $< 0, 255 >$). Dwa histogramy



Rysunek 15. Przykładowe obrazy powstałe w wyniku działania DFT (część rzeczywista: A, część urojona: B) oraz obliczony histogram (C) [opracowanie własne]

(pochodzący z obrazu testowego i bazowego) zostają następnie porównane. Przykładowy obraz histogramu został przedstawiony w części C rysunku 15.

Ostatnie cechy pochodzą z produktów Dyskretnej Transformaty Fouriera (ang. *Discrete Fourier Transform, DFT*) i również są cechami tekstury. W wyniku DFT otrzymuje się dwa obrazy: rzeczywisty (Re) i urojony (Im), których przykłady można zobaczyć na rysunku 15 w częściach A i B. Dla obu tych obrazów oraz dla niezmienionego ROI zostaje obliczona znormalizowana korelacja krzyżowa, którą wyraża równanie 18. Jest ona czasem nazywana miarą podobieństwa obrazów.

$$C_{NORM} = \frac{\sum_{ij}(Img_A(i,j) \cdot Img_B(i,j))}{\sqrt{\sum_{ij} Img_A(i,j)^2 \cdot \sum_{ij} Img_B(i,j)^2}} \tag{18}$$

gdzie:

- Img_A, Img_B - obraz testowy i obraz bazowy;
- i, j - współrzędne względem osi X oraz Y.

Dla obrazów o tej samej wielkości korelacja krzyżowa daje wynik będący liczbą zmiennoprzecinkową. Liczba ta wynosi 1 dla obrazów identycznych oraz zbliża się do 0 proporcjonalnie do zmniejszającego się podobieństwa obrazów.

W ten sposób otrzymany został wektor liczb, na podstawie którego następuje klasyfikacja. Został oznaczony na rysunku 14 kolorem zielonym. Wektor ten to $[m1, m2, m3, Im, Re, CC, CH]$, gdzie $m1, m2, m3$ - współczynniki podobieństwa momentów (powierzchnia oraz współrzędne x, y punktu środka masy), Im, Re, CC - wyniki korelacji krzyżowej dla części urojonych, rzeczywistych oraz niezmienionego ROI oraz CH - współczynnik podobieństwa histogramów. W ostatnim kroku wykonywana jest suma (kolor żółty na rysunku 14) wszystkich

tych liczb i w zależności od ustalonego empirycznie progu podejmuje się decyzję (kolor czerwony na rysunku 14) o pozytywnej bądź negatywnej weryfikacji.

4.4. Propozycja metody hybrydowej Geometric-Texture

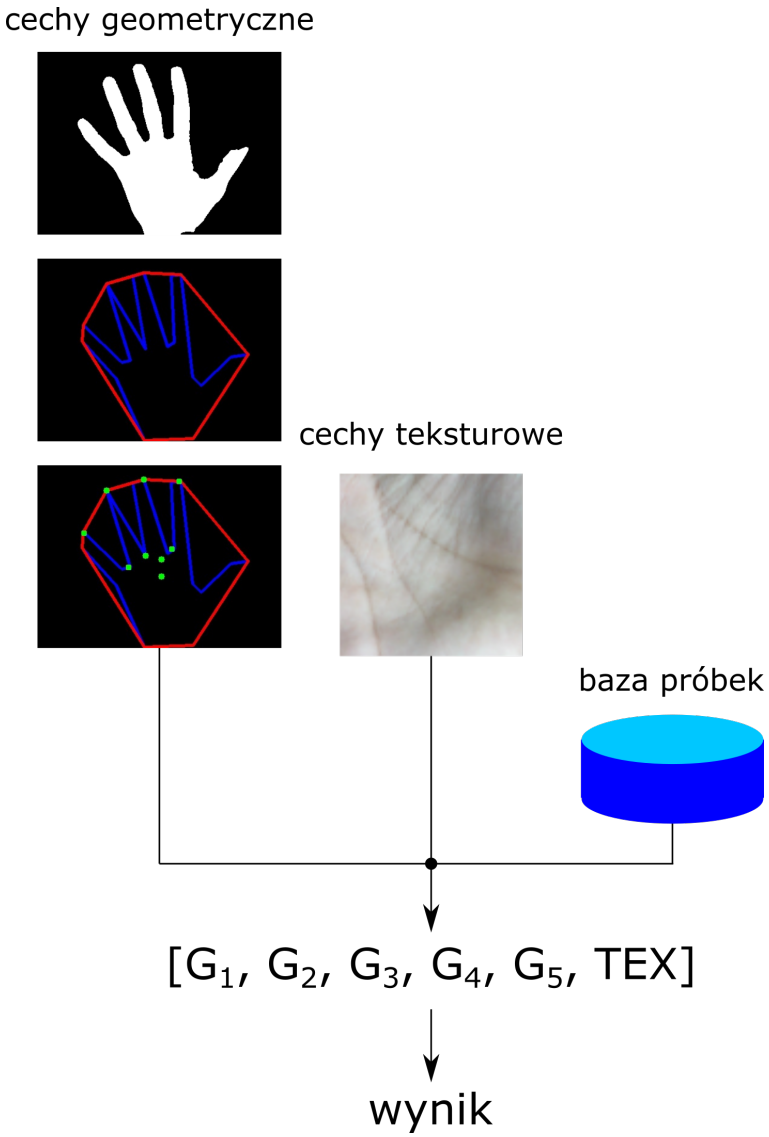
Następna proponowana metoda zyskała nazwę hybrydowej Geometric-Texture (GT), ponieważ do niej wybrano zarówno cechy teksturowe jak i cechy geometryczne. Kolejne kroki przetwarzania wykorzystane w proponowanej metodzie zostały przedstawione na rysunku 16.

W tej metodzie rozbudowano krok przetwarzania wstępnego. Przede wszystkim zawiera on etap wydobycia ROI zgodny z wcześniej przedstawionym algorytmem. Obszar ROI jest wykorzystany w kolejnych krokach do analizy tekstury. Jednak w metodzie GT na etapie wstępnego przetwarzania po wyznaczeniu obrysu dłoni (kolor niebieski na rysunku) następuje przygotowanie do wydobycia cech geometrycznych. W tym celu została wyznaczona łamana dookoła obrysu dłoni (kolor czerwony na rysunku). Następnie obliczone zostały punkty charakterystyczne, które są użyte do stworzenia cech geometrycznych (zaznaczone kolorem zielonym na rysunku). Zbiór punktów charakterystycznych stanowią:

0. czubek małego palca;
1. przestrzeń między palcami małym i serdecznym;
2. czubek palca serdecznego;
3. przestrzeń między palcami serdecznym i środkowym;
4. czubek środkowego palca;
5. przestrzeń między palcami środkowym i wskazującym;
6. czubek palca wskazującego;
7. środek masy konturu;
8. środek masy łamanej opisanej na konturze.

Należy zwrócić uwagę na to, że długości poszczególnych odcinków mogą się zmieniać np. w przypadku zmiany odległości od kamery. Dlatego zamiast długości zaproponowano wykorzystanie stosunków długości. Cechy geometryczne wykorzystywane w systemie zostały przedstawione równaniem 19. Użyta w tym równaniu funkcja *dist(A,B)* to nic innego jak odległość Euklidesa między punktami A i B. Cechy geometryczne są obliczane dla obrazu testowego oraz dla obrazu z bazy.

$$\begin{bmatrix} G_1 \\ G_2 \\ G_3 \\ G_4 \\ G_5 \end{bmatrix} = \begin{bmatrix} dist(0,1)/dist(1,5) \\ dist(2,3)/dist(1,5) \\ dist(4,5)/dist(1,5) \\ dist(5,6)/dist(1,5) \\ dist(7,8)/dist(1,5) \end{bmatrix} \tag{19}$$



Rysunek 16. Schemat przetwarzania próbek w metodzie GT [opracowanie własne]

W metodzie oprócz cech geometrycznych zostały również użyte cechy tekstury. W tym przypadku zdecydowano się skorzystać z korelacji: $CCOEFF, CCORR$ oraz $SQDIFF$, których sposób obliczania przedstawiają równania 20, 23 and 24. W ten sposób otrzymano wektor 6 cech, z których każda miała wartość należącą do przedziału $< 0,1 >$. Wszystkie cechy zostały zsumowane, a następnie na podstawie eksperymentalnie ustalonej wartości progowej, zakwalifikowane jako pozytywne lub negatywne.

Na dalszych etapach pracy nad metodą GT rozszerzony został wektor cech. Do wektora włączono bowiem jednocześnie wyniki trzech korelacji lub zwielokrotniono wynik wybranej metody analizy tekstury. Celem takiego działania było lepsze zbalansowanie metody, gdyż w podstawowej wersji metoda zależała głównie od pięciu cech geometrycznych.

$$TM_{CCOEFF} = \frac{\sum_{x,y}(T'(x,y) \cdot I'(x,y))}{\sqrt{\sum_{x,y} T'(x,y)^2 \cdot \sum_{x,y} I'(x,y)^2}} \tag{20}$$

gdzie:

$$T'(x,y) = T(x,y) - \frac{1}{w \cdot h} \sum_{i,j} T(i,j) \tag{21}$$

$$I'(x,y) = I(x,y) - \frac{1}{w \cdot h} \sum_{i,j} I(i,j) \tag{22}$$

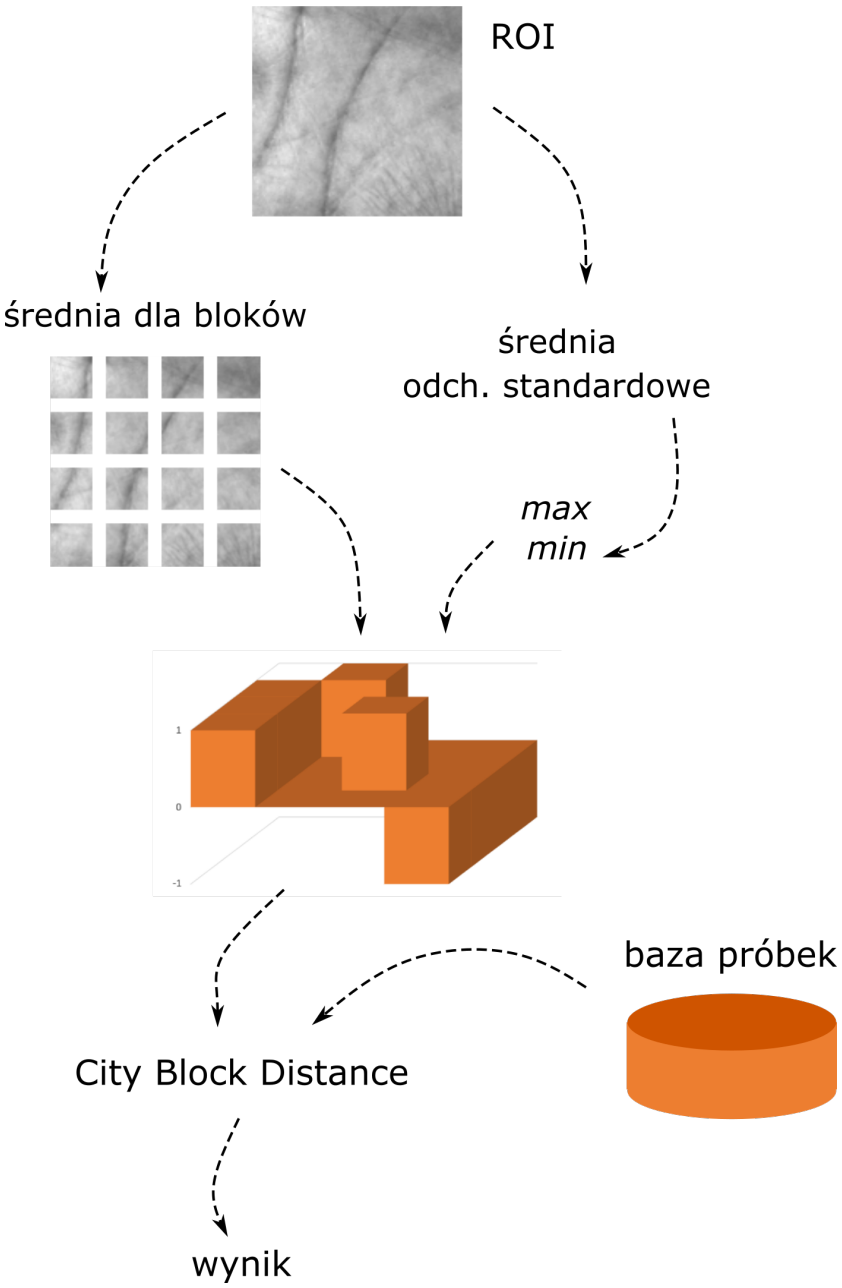
$$TM_{CCORR} = \frac{\sum_{x,y}(T(x,y) \cdot I(x,y))}{\sqrt{\sum_{x,y} T(x,y)^2 \cdot \sum_{x,y} I(x,y)^2}} \tag{23}$$

$$TM_{SQDIFF} = 1 - \frac{\sum_{x,y}(T(x,y) - I(x,y))^2}{\sqrt{\sum_{x,y} T(x,y)^2 \cdot \sum_{x,y} I(x,y)^2}} \tag{24}$$

4.5. Propozycja metody 3-wartościowej maski

Zgodnie z wnioskami wyciągniętymi z przeglądu literatury, postanowiono w kolejnej metodzie zastosować podział całego ROI na mniejsze bloki. Taki jest właśnie główny zamysł metody 3-wartościowej maski, a schemat działania całego systemu przedstawiono na rysunku 17.

Po wyznaczeniu rejonu zainteresowań, podzielono go na mniejsze, nienakładające się kwadratowe bloki. W metodzie 3-wartościowej maski zdecydowano się użyć 16 kwadratowych bloków o równej długości boku. Następnie dla każdego



Rysunek 17. Ogólny schemat działania metody 3-wartościowej maski [opracowanie własne]

z nich obliczana jest średnia arytmetyczna jasności pikseli. Liczona jest również średnia arytmetyczna ($\overline{x}$) i odchylenie standardowe (δ) dla całego obrazu, korzystając ze wzorów 25 i 26. Wprowadzono również dwie miary, które zostały wyrażone równaniami 28 oraz 27. Następnie dla każdego bloku przydziela się wartość maski w zależności od średniej wartości w danym bloku oraz średniej i odchylenia standardowego całego obrazu, w sposób taki jak zostało to przedstawione wzorem 29.

$$\overline{x} = \frac{\sum_{i=1}^{N} x_i}{N} \tag{25}$$

gdzie:

x_i – jasność i-tego piksela;
i – numer kolejnego piksela;
N – całkowita liczba pikseli w obrazie.

$$\delta = \sqrt{\frac{\sum_{i=1}^{N} (x_i - \overline{x})^2}{N}} \tag{26}$$

gdzie:

x_i – jasność i-tego piksela;
$\overline{x}$ – średnia wartość jasności;
i – numer kolejnego piksela;
N – całkowita liczba pikseli w obrazie.

$$min = \overline{x} - \frac{\delta}{2} \tag{27}$$

gdzie:

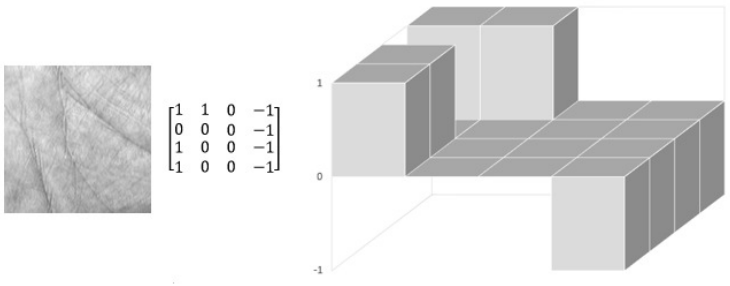
$\overline{x}$ – średnia wartość jasności;
δ – odchylenie standardowe jasności.

$$max = \overline{x} + \frac{\delta}{2} \tag{28}$$

gdzie:

$\overline{x}$ – średnia wartość jasności;
δ – odchylenie standardowe jasności.

$$vec[a] = \begin{cases} -1 & \text{dla } \overline{x_a} \leq min \\ 0 & \text{dla } min < \overline{x_a} \leq max \\ 1 & \text{dla } \overline{x_a} > max \end{cases} \tag{29}$$



Rysunek 18. Przedstawienie ROI za pomocą obrazu, macierzy oraz wykresu [opracowanie własne]

gdzie:

vec[a] – kolejny element wektora cech o numerze a;
$\overline{x_a}$ – średnia w a-tym bloku;
min, max – opisane powyżej.

Otrzymane w ten sposób wartości zostają włączone do wektora cech. Wektor ten ma zaledwie 16 elementów, więc stanowi zwartą reprezentację obrazu ROI charakterystycznego dla każdego z użytkowników. Rysunek 18 zawiera możliwe reprezentacje tego samej próbki - ROI, macierz liczb oraz wykres.

W przypadku prezentowanego podejścia zdecydowano użyć się metod uczenia maszynowego oraz sprawdzić, czy pozwolą one na uzyskanie lepszych rezultatów niż miary odległości. Oprócz samej skuteczności, istotny był również czas uczenia oraz czas predykcji dla każdej z wybranych metod. Do klasyfikacji wytypowano dwie metody uczenia maszynowego: SVM (ang. *Support Vector Machine*) oraz drzewo decyzyjne (*decision tree*, DT). SVM jest metodą bardzo często implementowaną do rozpoznawania obrazów. W przypadku wykorzystania jedynie dwóch klas, klasyfikator na podstawie danych testowych tworzy hiperpłaszczyznę, która oddziela próbki z tych klas. W tym przypadku zastosowano typ RBF *Radial Basis Function*. Drzewo decyzyjne natomiast jest przykładem drzewa binarnego, które minimalizuje sumę odległości pomiędzy wektorem testowym a wcześniej dostarczonymi do drzewa danymi uczącymi. Jako metodę do porównania wybrano odległość Manhattan (in. *City Block Distance*), którą oblicza się korzystając z równania 30.

$$d_m(x, y) = \sum_{k=1}^{n} |x_k - y_k| \tag{30}$$

gdzie:

x, y – porównywane wektory;
k – numer elementu w wektorach;
n – ilość elementów w wektorach.

Jako że metoda 3-wartościowej maski korzysta z uczenia maszynowego, należało przeprowadzić proces uczenia. W tym celu wytypowano zestaw 12 próbek uczących, z których połowa była pozytywna, a połowa negatywna. Próbki negatywne pochodziły od innych, losowo wybranych użytkowników i zostały później wykluczone z fazy testów. Dla każdej z próbek uczących został obliczony wektor cech, które w przypadku metod uczenia maszynowego (*SVM* oraz *DT*) następnie zostały dostarczone do klasyfikatora. W przypadku wykorzystania odległości Manhattan, został obliczony wektor średni dla próbek pozytywnych. W dalszych krokach obliczono odległość Manhattan każdego wektora pozytywnego i negatywnego oraz średnią tych odległości. Średnia ta stała się progiem - w przypadku gdy analizowany wektor znajdzie się w odległości bliższej niż ten próg, próbka mu odpowiadająca zostanie zakwalifikowana jako autentyczna. W przeciwnym wypadku zostania sklasyfikowana jako fałszywa.

4.6. Propozycja metody kodu binarnego

Kolejnej proponowanej metodzie nadano nazwę metody kodu binarnego, ponieważ jej głównym założeniem jest przedstawienie ROI za pomocą wektora zer i jedynek. W pracy Haralicka [31] zaprezentowano zestaw 14 cech teksturowych. Były to cechy opisujące statystycznie analizowaną teksturę. Pierwotnie były one wykorzystane do analizy obrazów satelitarnych i do identyfikacji obiektów widocznych na zdjęciach wykonanych z powietrza. Cechy te korzystają z macierzy GLCM (ang. *Grey Level Co-occurence Matrix*). Określa ona relacje pikseli o poszczególnych tonach jasności w analizowanym obrazie (tutaj: ROI). Macierz ta jednak nie doczekała się swojej jednoznacznej nazwy w języku polskim. Bywa nazywana macierzą zdarzeń, przejść, koincydencji lub histogramem drugiego rzędu. Dlatego w dalszej części pracy będzie nazywana po prostu macierzą GLCM. Omawiana i wykorzystana w metodzie kodu binarnego macierz jest macierzą kwadratową. Jej rozmiar określa ilość poziomów szarości (tutaj: 256×256). Poszczególne elementy macierzy określają, ile razy piksel o zadanej jasności sąsiaduje z pikselem o jasności referencyjnej. Przykładowo więc rząd 10. macierzy zawiera liczbę występowania obok siebie pikseli o jasności 10 i kolejno pikseli o jasnościach: 0, 1, 2, ..., 255.

Z zestawu 14 cech proponowanych przez Haralicka do metody kodu binarnego wybrane zostały dwie cechy: Haralick Sum Average (*HSAvg*) oraz Haralick Sum

Variance (*HSVar*). Miary te są określone równaniem 31 oraz 32. Obie miary zostały obliczone dla całego ROI oraz każdego z 16 bloków, na które go podzielono. Każdy z bloków był kwadratem i nie nakładał się na sąsiednie bloki.

$$HSAvg = \sum_{i=2}^{2N_g} i \cdot p_{x+y}(i) \tag{31}$$

$$HSVar = \sum_{i=2}^{2N_g} (i - HSEnt)^2 \cdot p_{x+y}(i) \tag{32}$$

gdzie:

N_g – ilość poziomów szarości (przyjęto $Ng = 255$);
$p(i,j)$ – element macierzy GLCM;
$p_{x+y}(i) = \sum_{i=1}^{N_g} \sum_{j=1}^{N_g} p(i,j)$ - suma wartości $p(i,j)$;
$HSEnt = \sum_{i=2}^{2N_g} p_{x+y}(i) \cdot \log \{p_{x+y}(i)\}$ – miara entropii również określona w pracy [31].

Następnym elementem algorytmu jest stworzenie kodu binarnego w zależności od obliczonych wartości. Każdy kolejny element wektora cech otrzymuje wartości zgodnie z równaniem 33 dla bitów nieparzystych i zgodnie z równaniem 34 dla parzystych. Na etapie klasyfikacji wykorzystano odległość Manhattan (in. *City Block Distance*) i w zależności od empirycznie ustalonego progu próbka była kwalifikowana jako autentyczna lub fałszywa.

$$vec[a] = \begin{cases} 0 & \text{jeżeli } HSAvg_{local} \leq HSAvg_{global} \\ 1 & \text{jeżeli } HSAvg_{local} > HSAvg_{global} \end{cases} \tag{33}$$

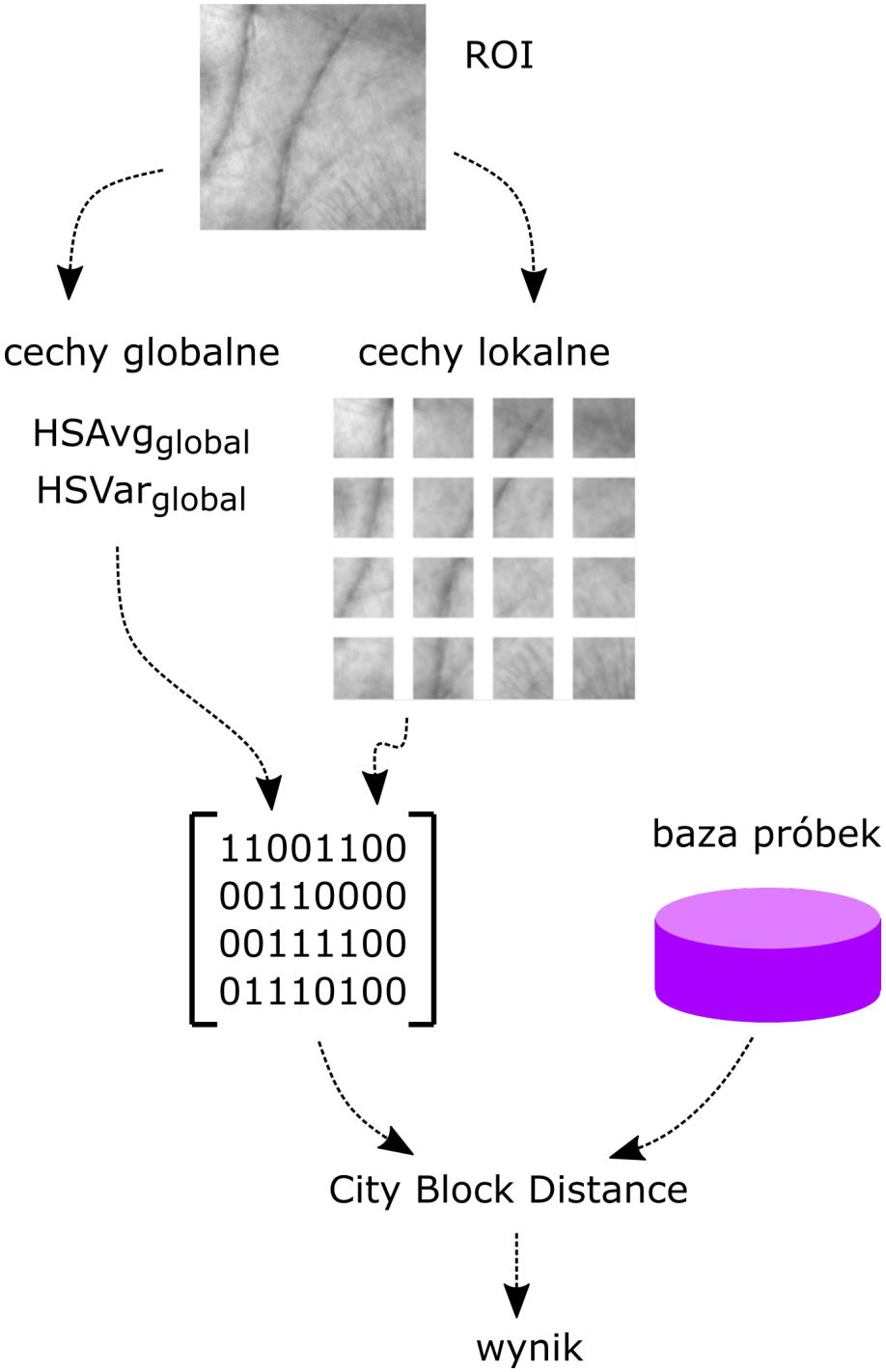
gdzie:

$HSAvg_{local}$ - średnia wartość obliczona dla bloku o numerze a;
$HSAvg_{global}$ - średnia wartość obliczona dla całego obrazu ROI.

$$vec[a] = \begin{cases} 0 & \text{jeżeli } HSVar_{local} \leq HSVar_{global} \\ 1 & \text{jeżeli } HSVar_{local} > HSVar_{global} \end{cases} \tag{34}$$

gdzie:

$HSVar_{local}$ - wartość wariancji obliczona dla bloku o numerze a;
$HSVar_{global}$ - wartość wariancji obliczona dla całego obrazu ROI.



Rysunek 19. Ogólny schemat przetwarzania [opracowanie własne]

4.7. Propozycja metody energii tekstury

Kolejna metoda również zawiera podział obrazu ROI na mniejsze części. Schemat całej proponowanej metody przedstawiono na rysunku 21. Wykorzystano w niej cechy tekstury zaproponowane w [48]. We wspomnianej pracy autor opisał pięć różnych wektorów. Kiedy dwa z tych wektorów zostaną ze sobą pomnożone, tworzy się macierz, która następnie jest użyta do przeprowadzenia operacji splotu z obrazem bazowym, dzięki czemu można podkreślić specyficzne cechy tekstury, np. kropki, grzbiety czy krawędzie. Do podkreślenia cech obrazu dłoni wytypowano dwa wektory, które noszą nazwy L5 oraz S5. Wektory oraz wyniki ich mnożenia zostały przedstawione równaniami 35 - 38. Wyniki mnożenia, co oczywiste z matematycznego punktu widzenia, są różne. Zdecydowano o użyciu obu wyników, a więc macierzy LS i SL, w operacjach splotu z ROI wydobytym z próbki. Następnie dodano macierze wynikowe operacji splotu do siebie. Wyniki kolejnych kroków przetwarzania obrazu przedstawiono na rysunku 20.

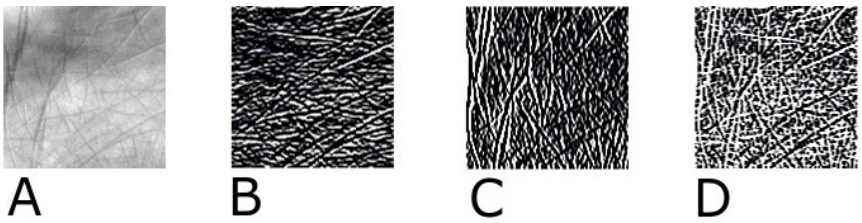
$$L5 = [1, 4, 6, 4, 1] \tag{35}$$

$$S5 = [-1, 0, 2, 0, -1] \tag{36}$$

$$kernel_{LS} = \begin{bmatrix} -1, & 0, & 2, & 0, & -1 \\ -4, & 0, & 8, & 0, & -4 \\ -6, & 0, & 12, & 0, & -6 \\ -4, & 0, & 8, & 0, & -4 \\ -1, & 0, & 2, & 0, & -1 \end{bmatrix} \tag{37}$$

$$kernel_{SL} = \begin{bmatrix} -1, & -4, & -6, & -4, & -1 \\ 0, & 0, & 0, & 0, & 0 \\ 2, & 8, & 12, & 8, & 2 \\ 0, & 0, & 0, & 0, & 0 \\ -1, & -4, & -6, & -4, & -1 \end{bmatrix} \tag{38}$$

Wynikowy obraz poddano kolejnej operacji, mianowicie wyznaczono miarę energii tekstury (ang. *texture energy measure*, TEM). Jest to miara, którą oblicza się przez dodanie wartości bezwzględnych jasności piksela w najbliższym sąsiedztwie, zgodnie z równaniem 39. W metodzie zastosowano sąsiedztwo o wielkości 15×15. To z kolei oznacza, że dla wielkości ROI $120px \times 120px$ miara TEM jest obliczana 64 razy. Ponadto wprowadzono drugą miarę - TEM_{avg}, która jest średnią arytmetyczną wszystkich 64 wartości TEM z całego obrazu. Aby stworzyć wektor cech, porównano kolejne wartości TEM z wartością TEM_{avg} zgodnie ze wzorem 40. W ten sposób został stworzony wektor cech.



Rysunek 20. Kolejne kroki przetwarzania: A: ROI, B: ROI po splocie z LS, C: ROI po splocie z SL, D: suma powstałych obrazów [opracowanie własne]

$$TEM = \sum_{i=1}^{m} \sum_{j=1}^{n} |C(i,j)| \tag{39}$$

gdzie:

$C(i,j)$ – jasność piksela;
i, j – współrzędne względem osi X i Y;
$m \times n$ – wielkość sąsiedztwa.

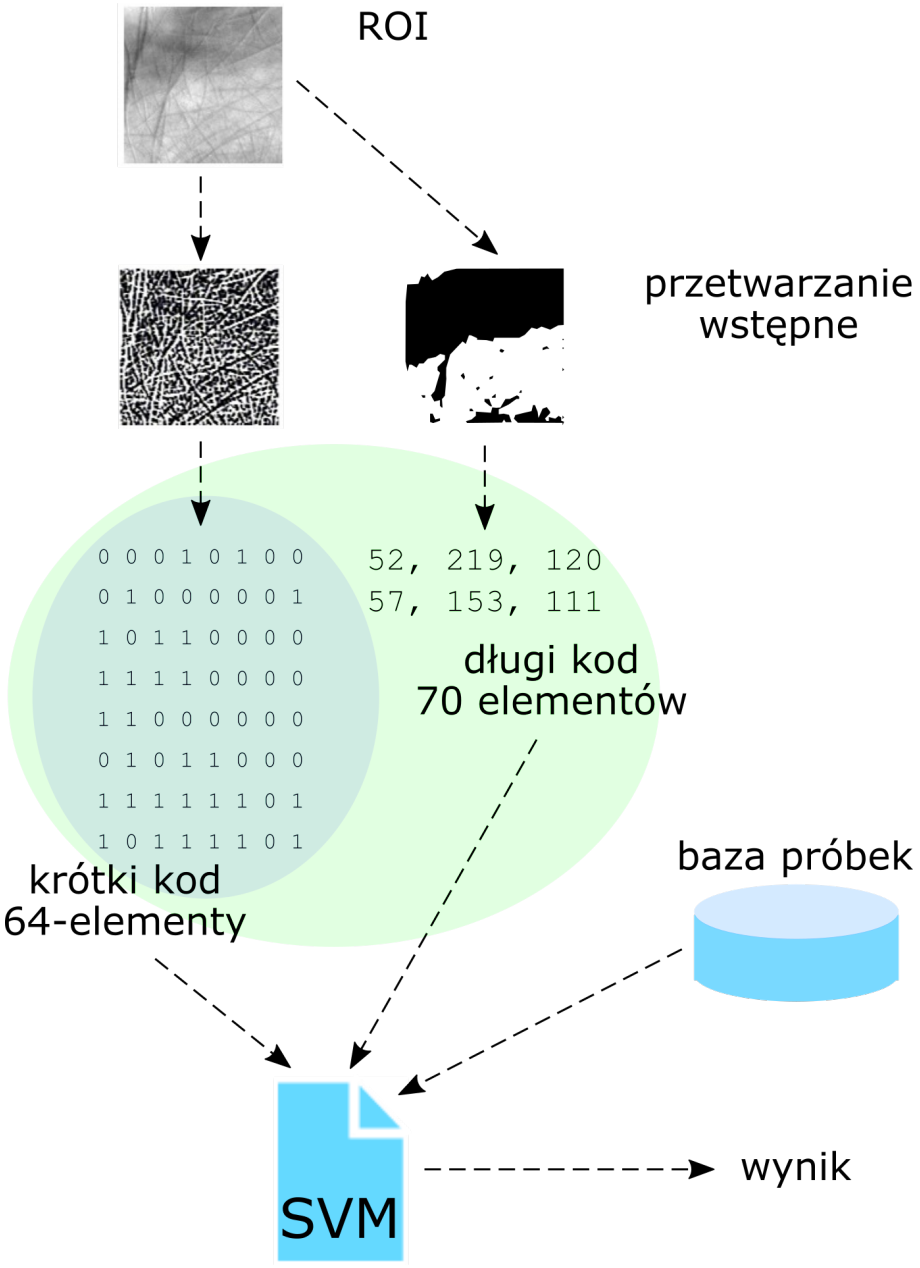
$$vec[a] = \begin{cases} 0 & \text{jeśli } TEM[a] < TEM_{avg} \\ 1 & \text{jeśli } TEM[a] \geq TEM_{avg} \end{cases} \tag{40}$$

gdzie:

$vec[a]$ – a-ty element wektora cech;
$TEM[a]$ – energia tekstury w rejonie a;
TEM_{avg} – średnia wartość energii tekstury w obrazie.

W pierwszych testach tej metody okazało się jednak, że skuteczność systemu nie jest wystarczająca. Wobec tego szukano sposobu na zwiększenie skuteczności przy niewielkim skomplikowaniu metody. Wszak miało to być rozwiązanie mobilne. Do metody wytypowano więc sześć dodatkowych cech. Długości przebiegów (ang. *runlength*) pozwalają uzyskać informację o teksturze analizowanego obrazu. Długie przebiegi świadczą o tym, że tekstura jest gładka. Z drugiej strony liczne krótkie przebiegi mogą sugerować, że obraz ma skomplikowaną i niejednorodną teksturę. Długość przebiegu oblicza się dla obrazów binarnych i jest to nic innego jak liczba kolejnych pikseli w jednym kolorze (białe lub czarne). Do wektora cech wprowadzono sześć cech pochodzących z obliczania długości przebiegów. Były to, analizowane dwukrotnie bo horyzontalnie i wertykalnie, następujące liczby:

1. liczba przebiegów o długości nieprzekraczającej 3;



Rysunek 21. Schemat przetwarzania zaproponowany w metodzie energii tekstury [opracowanie własne]

2. liczba przebiegów o długości większej niż 60;
3. długość najdłuższego przebiegu w obrazie.

W ten sposób został wyznaczony wektor 70 liczb, który stał się podstawą do rozpoznawania tożsamości na podstawie obrazu dłoni. Jako metodę klasyfikacji wybrano ponownie SVM. Wybór ten był podyktowany bardzo dobrymi wynikami tego sposobu klasyfikacji dla poprzednich metod.

4.8. Podsumowanie

W tym rozdziale przedstawiono założenia teoretyczne wszystkich metod opracowanych przez autorkę. Przedstawione systemy różnią się zarówno sposobami wydobycia cech, jak i metodami klasyfikacji. Różnią się również długością wektora cech. Zestawienie wszystkich metod zostało przedstawione w tabeli 3.

Tabela 3. Podsumowanie opracowanych metod

NAZWA	PRZETW. WSTĘPNE	WYDOBYCIE CECH	DŁ. WEKT.	KLASYFIKACJA
Metoda oparta na HOG	filtr Gaussa filtr medianowy filtr bilateralny wyostrzenie	HOG	2490	odległość Euklidesa
Metoda hybrydowa CT	filtr Gaussa algorytm Canny norm. histogramu DFT	momenty zwykłe korelacja krzyżowa	8	odległość Euklidesa
Metoda hybrydowa GT	progowanie	odległości między punktami, korelacja krzyżowa	6	odległość Euklidesa
Metoda maski 3-wartościowej	filtr Gaussa	średnia jasność pikseli w blokach	do 36	SVM, DT odległość Manhattan
Metoda kodu binarnego	macierz GLCM	średnia HSAvg, średnia HSVar	32	odległość Manhattan
Metoda energii tekstury	operacja splotu, progowanie	długość przebiegu, energia tekstury	70	SVM

5. Opracowanie stanowiska i planu badawczego

5.1. Stanowisko badawcze

5.1.1. Urządzenia testowe

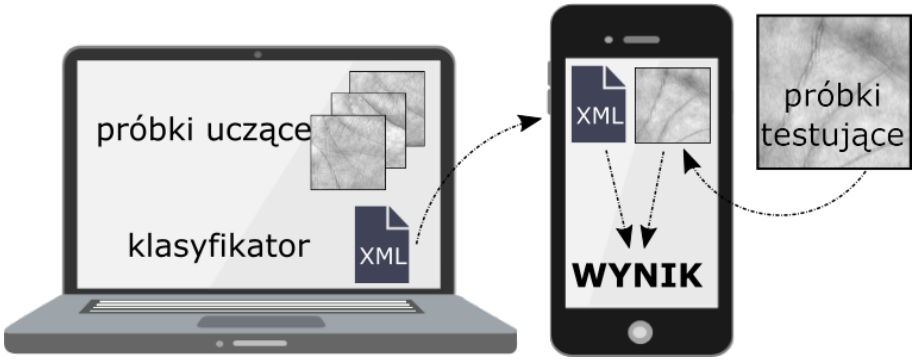
Z uwagi na tematykę rozprawy doktorskiej przed przystąpieniem do badań, należało stworzyć stanowisko badawcze, do którego zakupiono urządzenia przenośne, na których można by było przeprowadzić badania. Zakup części urządzeń został sfinansowany ze środków MNiSW w ramach uczelnianych projektów dla młodych naukowców BSM 81/2017 i BN 43/2019, których kierownikiem była Autorka. Tabela 4 zawiera szczegóły specyfikacji wykorzystanych urządzeń. Innym elementem stanowiska badawczego, a także urządzeniem na którym realizowano sporą część badań był komputer osobisty o następujących parametrach: procesor Intel Core i5420U, 4×1, 7GB, 4GB RAM. Jedną z metod przetestowano również na komputerze Raspberry Pi 2.

5.1.2. Protokół badań

Większość eksperymentów przeprowadzono zgodnie ze schematem przedstawionym na rysunku 22. Z racji ograniczonych zasobów dostępnych na urządzeniach mobilnych pierwsza implementacja zawsze była wykonana na komputerze osobistym. Również proces uczenia w każdym z przypadków był przeprowadzony na komputerze. Następnie klasyfikator (w przypadku metod uczenia maszynowego) lub wartość progu (dla mniej skomplikowanych miar) były przekazywana do urządzeń mobilnych – na rysunku zostało to przedstawione w postaci pliku XML. W dalszej części były prowadzone eksperymenty z wykorzystaniem urządzeń mobilnych, które prowadziły przetwarzanie wstępne próbki, wydobycie

Tabela 4. Specyfikacja urządzeń mobilnych wykorzystanych w prezentowanych badaniach

Urządzenie	System operacyjny	Procesor	RAM
Samsung A5 2017	Android 8.0 Oreo	8×1.90GHz	3GB
Xiaomi Mi6	Android 8.0 Oreo	8×2.45GHz	4GB
Huawei P10 Lite	Android 7.0 Nougat	8×2.10GHz	3GB
Samsung Galaxy S5	Android 6.0 Marshmallow	4×2.50GHz	2GB



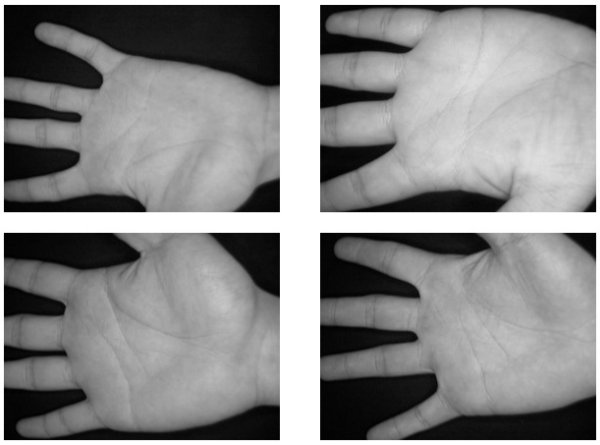
Rysunek 22. Schemat przeprowadzania eksperymentów [opracowanie własne]

cech oraz klasyfikację. Cały proces dla pojedynczej próbki kończył się wynikiem: autentyczny lub fałszywy. Eksperymenty przeprowadzono z wykorzystaniem różnych baz danych, którym poświęcono kolejny podrozdział pracy. Podczas badań zasadniczo obserwowano dwa parametry. Pierwszym była skuteczność działania rozumiana jako ilość poprawnie zweryfikowanych próbek. Drugim parametrem był czas przetwarzania jednej próbki przez konkretne urządzenie mobilne.

Podczas badania skuteczności i czasu działania poszczególnych podejść, zwykle korzystano z metody 3-krotnej walidacji. Polega ona na trzykrotnym różnym podziale zestawu próbek na uczące i testowe, a następnie uśrednieniu otrzymanych wyników. Wykorzystanie 3-krotnej walidacji pozwala stwierdzić, że otrzymane rezultaty nie zależą od danych uczących.

5.2. Dostępne bazy obrazów dłoni

Jednym z czynników, który musi być wzięty pod uwagę podczas wyboru analizowanej cechy biometrycznej, jest dostępność baz danych, na których można przeprowadzić badania, a także przetestować cały zaprojektowany system. Dla każdej z cech biometrycznych dostępne są różne bazy danych. Mogą się one różnić sposobem pobierania próbek, ilością próbek, a także ilością osób od których pobrano próbki. Różnią się też popularnością. Oczywistym wydaje się fakt, iż przeprowadzanie badań na bardzo popularnej i wykorzystywanej na całym świecie bazie danych, będzie dawało bardziej obiektywne wyniki niż wykonanie tych samych badań na małej i stworzonej prywatnie bazie danych, z której nikt wcześniej nie korzystał. Istnieją również bazy dedykowane biometrii multimodalnej, w których można znaleźć próbki przedstawiające dwie cechy biometryczne dla każdej z osób.



Rysunek 23. Przykłady obrazów z bazy CASIA [5]

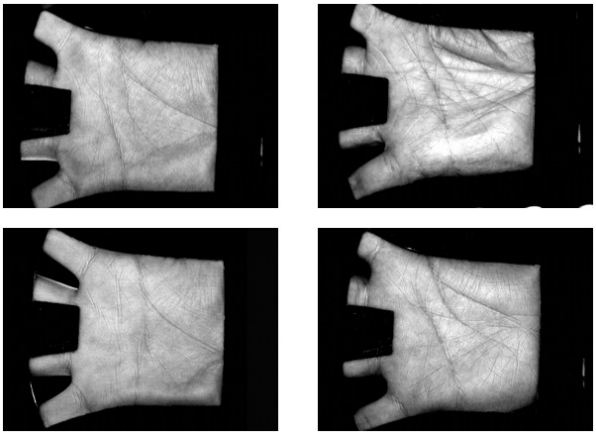
Do badania systemów weryfikacji i identyfikacji na podstawie obrazów wewnętrznych części dłoni wykorzystywane są zazwyczaj trzy, popularne na całym świecie bazy danych: CASIA, PolyU oraz IITD. Zostały one opisane w dalszej części tego rozdziału. Niestety żadna z opisanych baz danych nie jest dedykowana dla scenariusza mobilnego. Dlatego podczas przygotowań do napisania tej rozprawy doktorskiej, przygotowano koncepcję nowej, mobilnej bazy danych.

5.2.1. CASIA

Baza ta została stworzona i jest nadzorowana przez Chińską Akademię Nauk [5]. Jest udostępniona dla osób, które prowadzą badania oraz dla celów edukacyjnych. Zawiera 5502 obrazy przedstawiające obrazy wewnętrznych części dłoni 312 osób. Obrazy były pobierane za pomocą urządzenia zaprojektowanego przez twórców bazy. Przedstawiają one zarówno prawą, jak i lewą rękę. Przykładowe obrazy z bazy CASIA zostały przestawione na rysunku 23.

5.2.2. PolyU

Baza danych PolyU została stworzona przez naukowców z Chin i Hong-Kongu [7]. Obrazy również do tej bazy były pobierane za pomocą specjalnie do tego zaprojektowanego urządzenia, które zostało opisane w [84]. W bazie można znaleźć 7752 obrazy w formacie BMP, które są próbkami pobranymi od 389 osób. Dla każdej z nich pobrano około 10 próbek w pierwszej sesji oraz 10 w kolejnej, która nastąpiła 2 miesiące później. Baza danych jest udostępniona dla celów naukowych po wcześniejszym zalogowaniu. Przykłady próbek pobranych z tej bazy zostały przedstawione na rysunku 24.



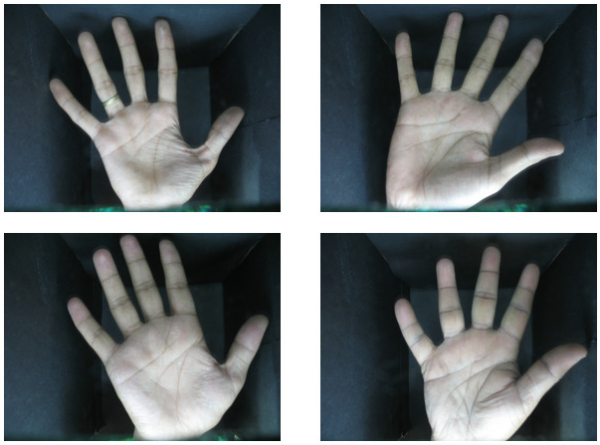
Rysunek 24. Przykłady obrazów z bazy PolyU [7]

5.2.3. IITD

Baza danych IIT Delhi zawiera obrazy wewnętrznych części dłoni pobrane od studentów i personelu instytutu IIT Delhi w Indiach [6]. Została stworzona na przełomie lat 2006 i 2007. Obrazy były pobierane w dość specyficznych warunkach – w zamkniętym pomieszczeniu z dobrym oświetleniem ustawionym dookoła kamery. Aktualnie dostępna baza danych zawiera próbki pobrane od 235 użytkowników w grupie wiekowej 12-57 lat, wszystkie obrazy zostały zapisane w formacie bitmap (*.bmp) i są kolorowe. Dla każdej osób można znaleźć po siedem zdjęć prawej i lewej ręki w różnych pozycjach względem kamery. Przykłady próbek z bazy IITD zostały przedstawione na rysunku 25.

5.3. Koncepcja bazy do eksperymentów

W związku z wykazanym w opisie aktualnego stanu wiedzy brakiem dużej, powszechnie dostępnej i relewantnej bazy danych, Autorka przygotowała wstępną koncepcję biometrycznej bazy danych zawierającej zdjęcia obrazów dłoni wykonane za pomocą telefonów komórkowych. Koncepcja zawiera kilka kluczowych elementów. Pierwszym z nich było urządzenie, którym była pobierana próbka – w ten sposób zgromadzone dane nie są zależne od specyficznego urządzenia. Pozwala to też założyć, że zaprojektowany system będzie skutecznie funkcjonował również z innymi urządzeniami. Ponadto na zdjęciach mają zostać przedstawione obie dłonie – użytkownik powinien mieć wybór, której ręki będzie używał do weryfikacji. Osobom leworęcznym jest znacznie łatwiej zrobić zdjęcie swojej prawej ręce, w lewej trzymając telefon komórkowy. Dodatkowo posiadanie zdjęć



Rysunek 25. Przykłady obrazów z bazy IITD [6]

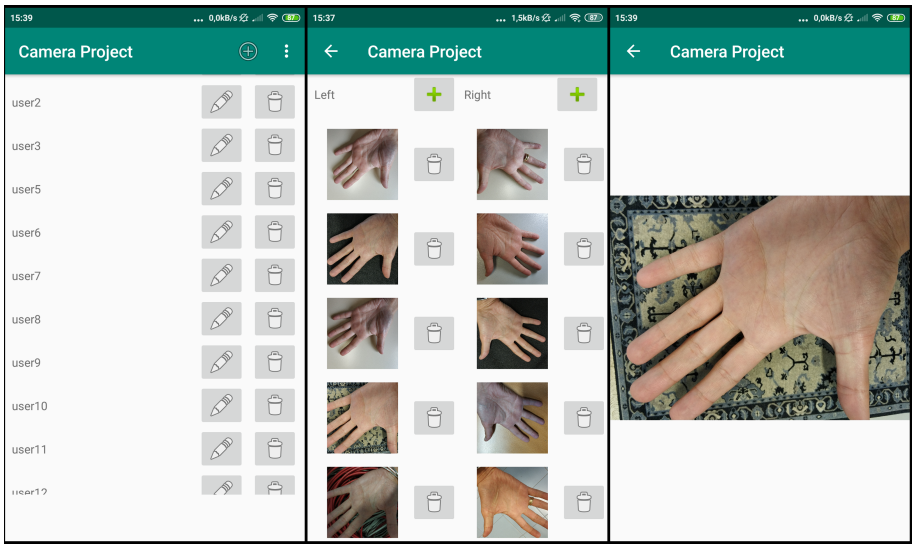
obu dłoni pozwala na stworzenie systemu bimodalnego, w którym analizie zostanie poddana zarówno prawa jak i lewa ręka użytkownika. Ostatnim z założeń jest tło. Różnorodne tło zbliża tworzony system do rzeczywistego oraz zwiększa użyteczność bazy danych. Ciężko bowiem wyobrazić sobie konieczność szukania jednorodnego tła do zrobienia zdjęcia w procesie weryfikacji.

5.3.1. Aplikacja do zbierania próbek

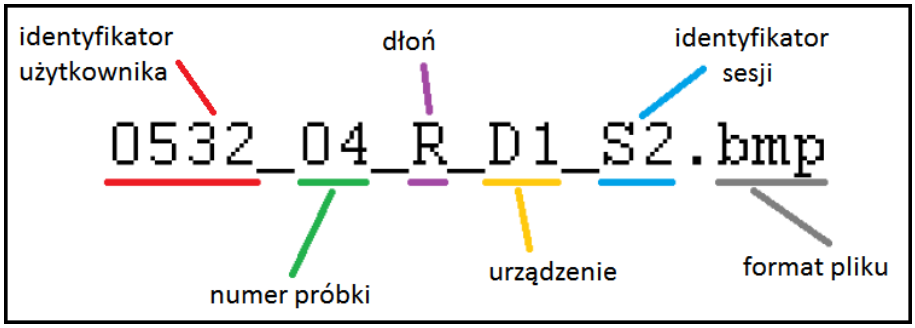
Aby umożliwić zbieranie próbek biometrycznych (w tym przypadku zdjęć dłoni), zdecydowano się stworzyć autorską aplikację mobilną na system Android. Celem aplikacji jest sprawienie, że proces pobierania zdjęć będzie możliwie jak najbardziej komfortowy i intuicyjny dla użytkownika. Rysunek 26 przedstawia podstawowe funkcjonalności stworzonego oprogramowania. Tuż po uruchomieniu aplikacji można przejrzeć listę użytkowników, którzy zdecydowali się przekazać dane biometryczne do bazy. Po wybraniu konkretnego użytkownika można przejrzeć zdjęcia jego dłoni, zarządzać nimi oraz dodawać nowe zdjęcia obu dłoni. Umożliwia też podgląd wykonanego zdjęcia. Przed pobraniem próbki należy określić takie zmienne jak numer sesji oraz rodzaj tła (jasne, ciemne, złożone).

Zmienne określające konkretną próbkę powinny zostać zapisane w niepowtarzalnej nazwie pliku korzystając z formatu widocznego na rysunku 27. Nazwa ta zawiera:

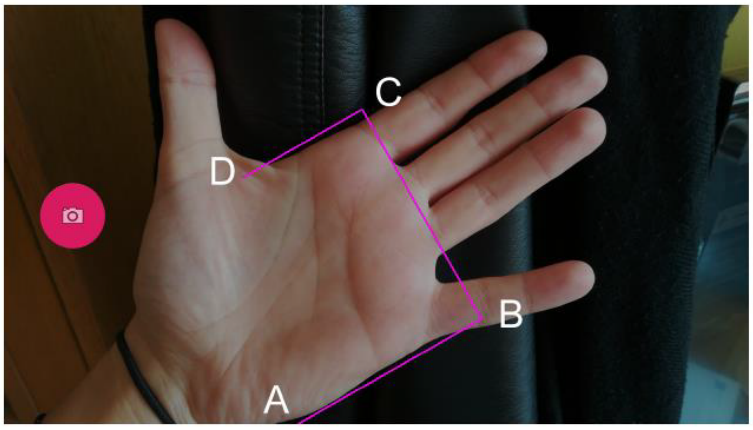
- niepowtarzalny identyfikator osoby (użytkownika),
- numer pobranej próbki,
- identyfikator tła (D - ciemne, L - jasne and C - złożone),



Rysunek 26. Widok interfejsu użytkownika stworzonej aplikacji: (od lewej) lista użytkowników, pobrane próbki dla jednego użytkownika, podgląd próbki [opracowanie własne]



Rysunek 27. Proponowany szablon nazw plików w bazie [opracowanie własne]



Rysunek 28. Widok graficznego asystenta użytkownika [opracowanie własne]

– oznaczenie R lub L w zależności od tego, czy na zdjęciu jest przedstawiona prawa czy lewa ręka,
– identyfikator urządzenia (D1 - Samsung A5, D2 - Huawei, D3 - Xiaomi, D4 - Samsung S5, D5 - inne urządzenie),
– numer sesji.

Oprogramowanie zostało przygotowane z myślą o telefonach komórkowych wyposażonych w system operacyjny Android i zostało przetestowane na czterech urządzeniach: Samsung Galaxy A5 2017, Xiaomi Mi6, Huawei P10 Lite oraz Samsung Galaxy S5.

Aby jednak ustalić jednolite położenie dłoni na zapisywanym obrazie, zdecydowano się na wprowadzenie graficznego asystenta użytkownika, który przedstawia rysunek 28. Widać na nim również punkty charakterystyczne, które zostały opisane równaniami 41 dla zdjęć lewej dłoni oraz równaniami 42 dla prawej. Punkty zostały wybrane w taki sposób, aby umożliwić obsługę oprogramowania tylko jedną ręką. Wzięto również pod uwagę komfort użytkownika i dlatego dłoń na zdjęciu jest nachylona pod kątem zbliżonym do 30°.

$$\begin{aligned} A &= (x, m) \\ B &= \left(\frac{3x}{4}, \frac{y}{3}\right) \\ C &= \left(\frac{x}{4}, \frac{y}{2}\right) \\ D &= \left(n, \frac{2y}{3}\right) \end{aligned} \tag{41}$$

$$
\begin{aligned}
A &= (x, y - m) \\
B &= \left(\frac{3x}{4}, y - \frac{y}{3}\right) \\
C &= \left(\frac{x}{4}, y - \frac{y}{2}\right) \\
D &= \left(n, y - \frac{2y}{3}\right)
\end{aligned}
\tag{42}
$$

gdzie:

x, y – współrzędne punktów względem osi OX i OY;
m, n – miary określone równaniami 43 i 44.

$$
n = \left(\frac{y}{6} + \frac{3x^2}{4y}\right) \cdot \frac{y}{3x} \tag{43}
$$

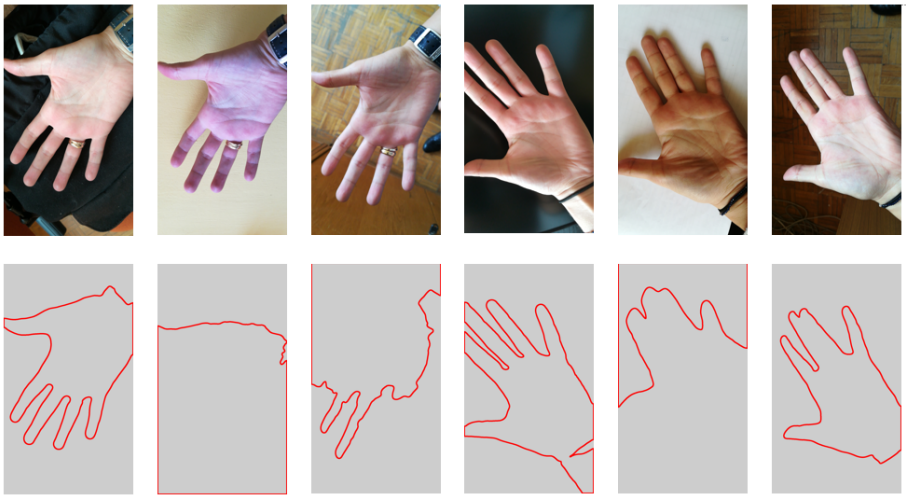
$$
m = \frac{3x^2}{y} + \frac{y}{3} - \frac{9x^2}{4y} \tag{44}
$$

5.3.2. Drugi algorytm wydobycia ROI

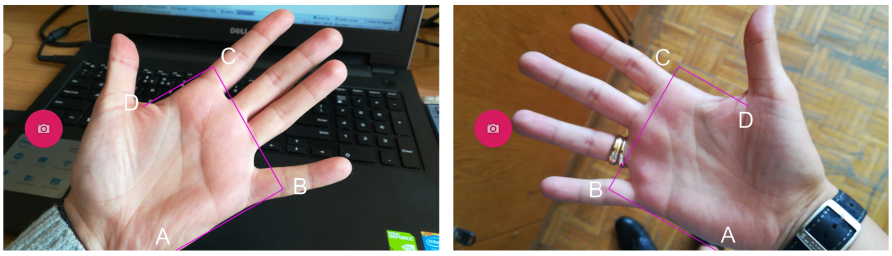
Drugi algorytm został stworzony do proponowanej w rozprawie bazy danych. Drugi algorytm trzeba było opracować gdyż pierwszy nie sprawdzał się dla próbek z tłem innym niż ciemne. Najwięcej problemów sprawiał etap wyznaczenia konturu dookoła dłoni, który jest niezbędny do poprawnego wyznaczenia punktów w przestrzeniach między palcami, obrotu obrazu, a w efekcie wyznaczenia ROI. Na rysunku 29 przedstawiono próby segmentacji dłoni od tła przeprowadzone z wykorzystaniem obrazów z nowej bazy. Widać na nim, że segmentacja jest szczególnie trudna w przypadku jasnego i złożonego (zawierającego różne kolory) tła.

Ponieważ aplikacja mobilna do zbierania próbek do bazy danych została wyposażona w graficzny asystent położenia dłoni, postanowiono skorzystać z niego podczas wydobycia ROI. Widok ekranu aplikacji zbierającej próbki przedstawiono na rysunku 30. Widać na nim, że ROI znajduje się wewnątrz figury o wierzchołkach oznaczonych literami A-D. Obszar zawierający najwięcej użytecznych informacji jest jednak obrócony, w tym celu należy dokonać obrotu całego obrazu względem punktu C o 30°dla lewej ręki przeciwnie do wskazówek zegara, a dla prawej zgodnie do wskazówek. Następnie w zadanej odległości od punktu C wyznaczono rejon zainteresowań.

Algorytm jednak powinien być przygotowany do pracy w warunkach niekontrolowanych przez operatora, stąd wprowadzono dodatkową walidację. W tym



Rysunek 29. Przykłady segmentacji dla próbek pobranych za pomocą telefonów komórkowych [opracowanie własne]



Rysunek 30. Zrzut ekranu aplikacji wraz z graficznym asystentem położenia dłoni [opracowanie własne]

celu po wydobyciu ROI następuje sprawdzenie, czy na pewno zawiera ono zdjęcie skóry. Weryfikacja ta jest pozytywna, kiedy co najmniej 95% pikseli spełnia nierówności 45.

$$\begin{gathered} R > 95; G > 40; B > 20 \\ max(R,G,B) - min(R,G,B) > 15 \\ |R - G| > 15; R > B; R > G \end{gathered} \tag{45}$$

gdzie:

R – intensywność składowej czerwonej piksela;
G – intensywność składowej zielonej piksela;
B – intensywność składowej niebieskiej piksela.

6. Wyniki przeprowadzonych eksperymentów

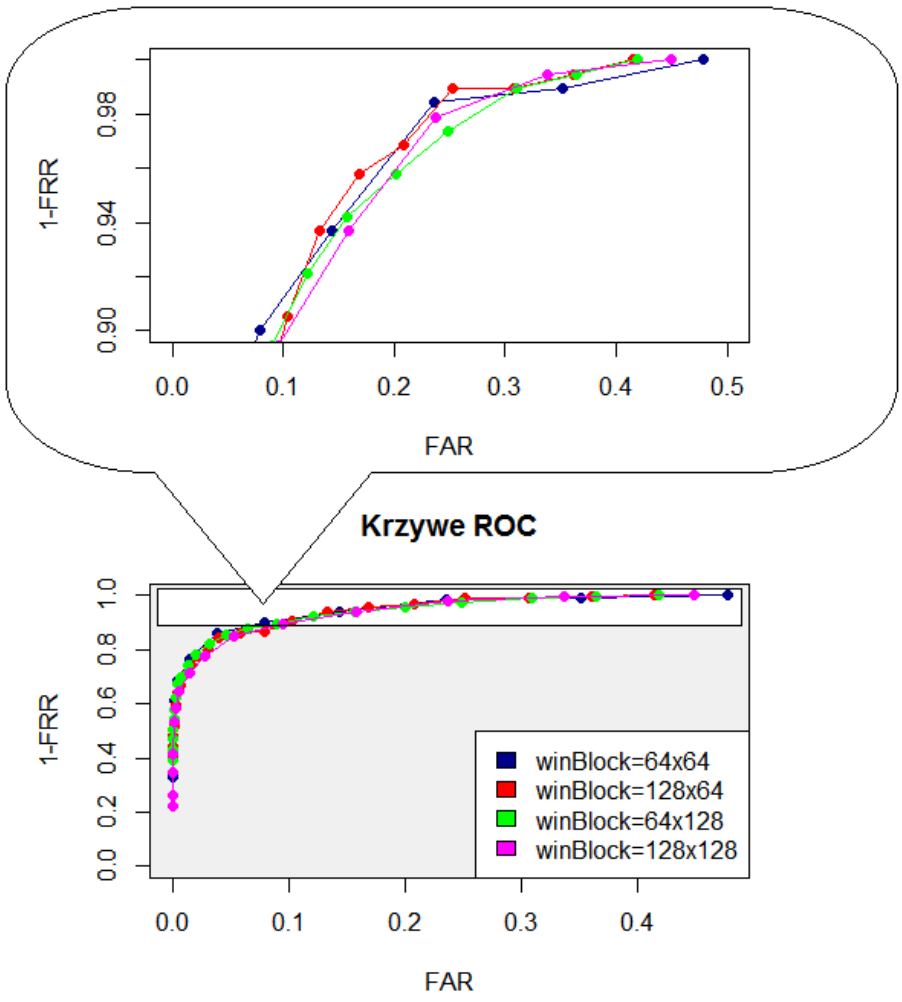
6.1. Badanie metody opartej na histogramie gradientów

6.1.1. Badanie metod przetwarzania wstępnego obrazów

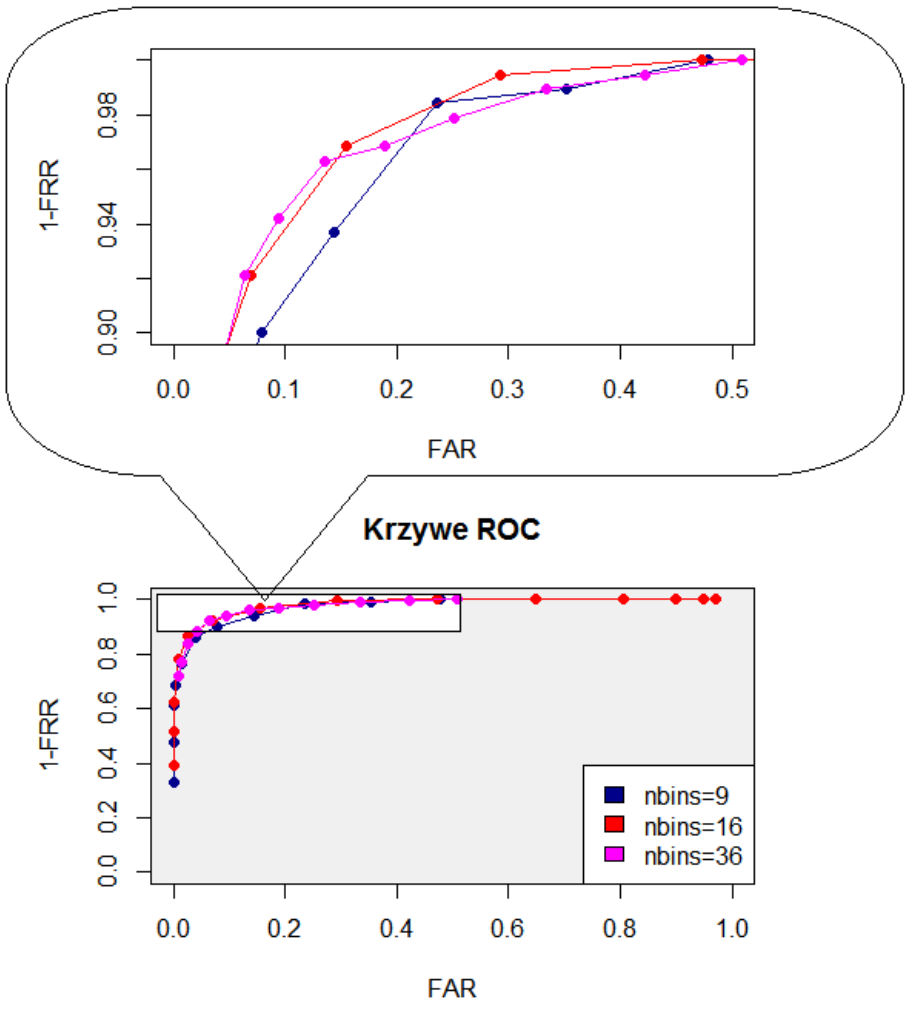
Jednym z pierwszych przeprowadzonych eksperymentów było badanie metod przetwarzania wstępnego. Badania te potwierdziły przypuszczenie, że zmiana metody przetwarzania wstępnego może znacznie poprawić skuteczność rozpoznawania osób.

Pierwszą część eksperymentów poświęcono dostosowaniu parametrów metody HOG. W tym celu na początku wybrano wielkość okna. Przetestowano cztery rozmiary okna: $64px \times 64px$, $128px \times 64px$, $64px \times 128px$ oraz $128px \times 128px$. Wyniki tych testów przedstawiono na rysunku 31. Na rysunku widać, że wszystkie cztery konfiguracje gwarantowały podobną skuteczność. Kiedy jednak porównano czas działania, okazało się, że użycie okna o rozmiarze $128px \times 128px$ pozwalało osiągnąć najkrótszy czas. Testy przeprowadzono również, aby wybrać wartość parametru *nbins*. Wartość tego parametru określa, w ilu kierunkach jest obliczany gradient. Wyniki testów przedstawiono na rysunku 32. Widać na nim, że skuteczność rośnie wraz ze wzrostem wartości parametru *nbins*. Jednocześnie jednak zaobserwowano wydłużenie czasu działania rozpoznawania. Dostosowano również wielkość komórki (ang. *cellSize*) oraz wielkość bloku (ang. *blockSize*). Ostatecznie zdecydowano się wykorzystać metodę HOG o następujących parametrach: $winSize = 128 \times 128$, $nbins = 16$, $cellSize = 8 \times 8$ oraz $blockSize = 8 \times 8$.

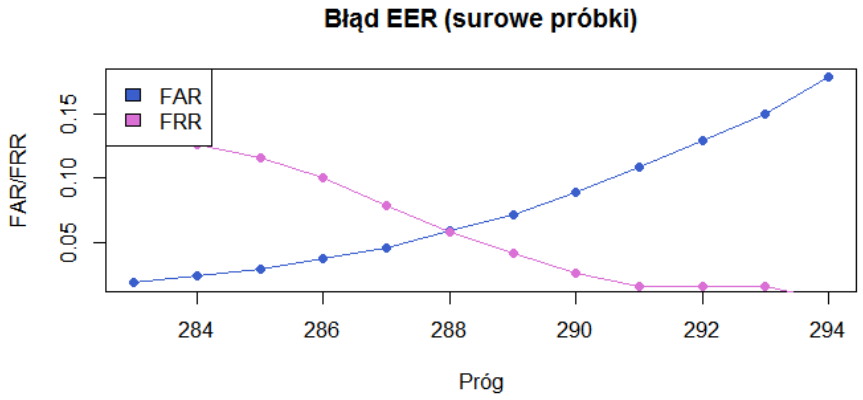
W przypadku biometrycznego systemu rozpoznawania osób polegającym na wykorzystaniu metody HOG i odległości Euklidesa przy braku metod przetwarzania wstępnego, które poprawiają wygląd próbki, otrzymano skuteczność działania na poziomie 94,0%. Z kolei przy użyciu różnych metod przetwarzania wstępnego, osiągnięto skuteczność na poziomie od 93,3% do 97,1%, co dokładniej zaprezentowano w tabeli 5. Wyniki eksperymentów przedstawiono również w postaci wykresów błędów FAR i FRR na rysunku 33 (próbki bez przetwarzania wstępnego) oraz rysunku 34 dla każdej z przebadanych metod wstępnego przetwarzania obrazu. Na tych wykresach widać zależność obu błędów od ustalonego progu. W miejscu przecięcia się wykresów wyznaczony jest błąd EER. Nieco zaskakującym może okazać się pogorszenie skuteczności dla wyostrzonej próbki.



Rysunek 31. Krzywe ROC dla różnych rozmiarów okna w metodzie HOG



Rysunek 32. Krzywe ROC dla różnych wartości parametru *nbins*



Rysunek 33. Wykres błędu EER dla surowych próbek [opracowanie własne]

Podczas implementacji na telefonach komórkowych porównano czasy działania wymienionych metod wstępnego przetwarzania. W tabeli 6 przedstawiono czasy wykonywania analizy jednej próbki z wyszczególnieniem czasu przetwarzania dla poszczególnych metod przetwarzania wstępnego: filtru Gaussa o wielkości 3×3 oraz 5×5, filtru medianowego o wielkości 3 oraz 5, filtru bilateralnego i wyostrzania.

Tabela 5. Wyniki skuteczności dla różnych metod przetwarzania wstępnego

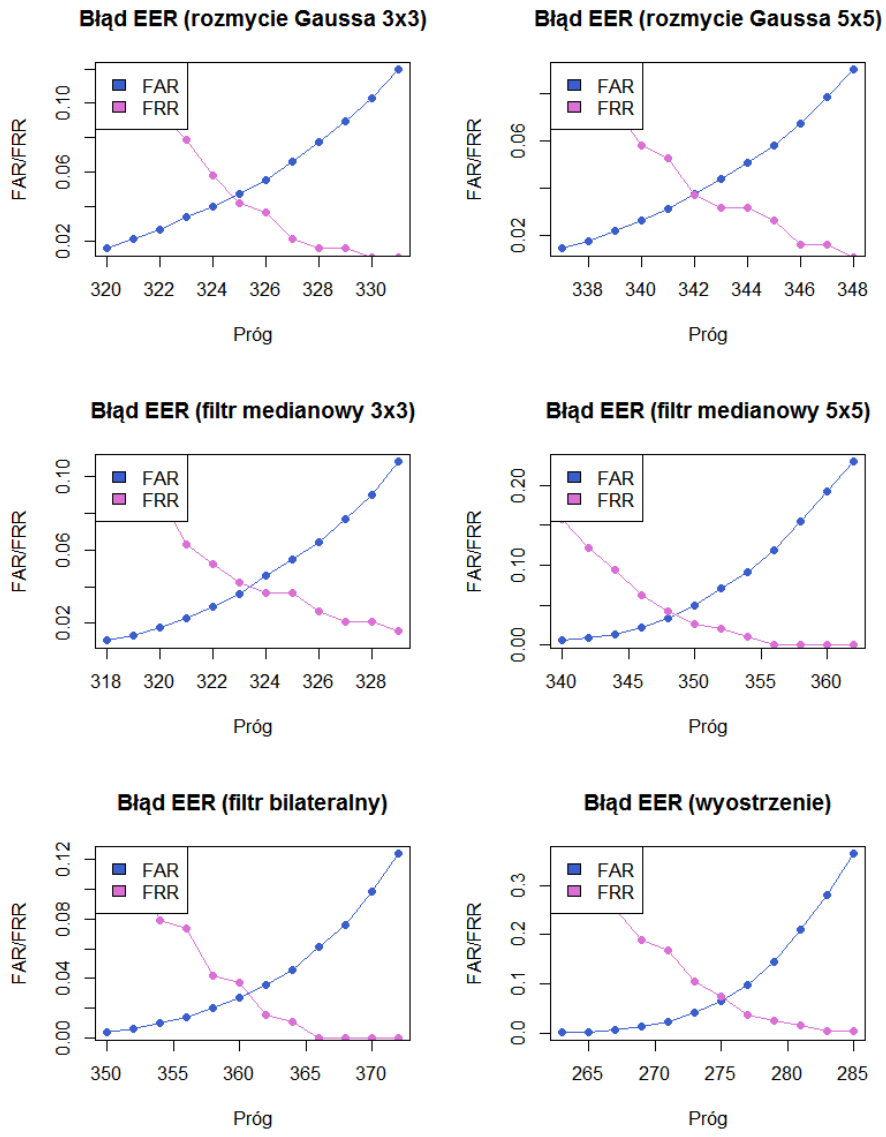
Metoda przetwarzania wstępnego	Skuteczność
surowe próbki	94,0%
filtr Gaussa o wielkości 3×3	95,1%
filtr Gaussa o wielkości 5×5	96,1%
filtr medianowy o wielkości 3×3	96,2%
filtr medianowy o wielkości 5×5	95,8%
filtr bilateralny	**97,1%**
wyostrzenie	93,3%

6.1.2. Badanie metody opartej na HOG na urządzeniu Raspberry Pi 2

Kolejnym eksperymentem była implementacja i testowanie wcześniej sprawdzanego systemu na komputerze Raspberry Pi 2. Można do niego podłączyć dowolną kamerę internetową przez złącze USB oraz korzystać z wielu bibliotek, w tym z biblioteki do przetwarzania obrazu, dźwięku i nagrań wideo, jaką jest biblioteka OpenCV. Stworzone urządzenie służące do weryfikacji zostało przedstawione na rysunku 35. W obudowie wydrukowanej techniką druku 3D zostało ukryte urządzenie Raspberry Pi 2, dwie podłączone do niego kolorowe diody, przycisk oraz kamera internetowa Logitech C130. Chociaż podczas badań metod

Tabela 6. Porównanie czasów działania dla poszczególnych urządzeń mobilnych

Xiaomi Mi6							
Próba	**Filtr Gaussa** 3×3	**Filtr Gaussa** 5×5	**Filtr medianowy 3**	**Filtr medianowy 5**	**Filtr bilateralny**	**Wyostrzenie**	**Eks. cech + klasyfikacja**
Podzbiór 1	9,91 ms	9,26 ms	9,13 ms	11,12 ms	32,59 ms	11,06 ms	7,50 ms
Podzbiór 2	9,71 ms	9,26 ms	9,10 ms	11,51 ms	34,37 ms	11,47 ms	6,79 ms
Podzbiór 3	9,40 ms	8,85 ms	8,94 ms	10,79 ms	32,31 ms	10,35 ms	6,75 ms
Średnia	9,67 ms	9,13 ms	9,06 ms	11,14 ms	33,09 ms	10,96 ms	7,01 ms
Huawei P10 Lite							
Próba	**Filtr Gaussa** 3×3	**Filtr Gaussa** 5×5	**Filtr medianowy 3**	**Filtr medianowy 5**	**Filtr bilateralny**	**Wyostrzenie**	**Eks. cech + klasyfikacja**
Podzbiór 1	10,52 ms	11,07 ms	10,11 ms	12,92 ms	35,81 ms	11,98 ms	7,21 ms
Podzbiór 2	11,23 ms	10,88 ms	10,96 ms	13,07 ms	34,98 ms	12,62 ms	8,11 ms
Podzbiór 3	10,87 ms	10,91 ms	9,91 ms	13,18 ms	34,92 ms	12,78 ms	7,43 ms
Średnia	10,87 ms	10,95 ms	10,33 ms	13,06 ms	35,24 ms	12,46 ms	7,58 ms
Samsung Galaxy A5 2017							
Próba	**Filtr Gaussa** 3×3	**Filtr Gaussa** 5×5	**Filtr medianowy 3**	**Filtr medianowy 5**	**Filtr bilateralny**	**Wyostrzenie**	**Eks. cech + klasyfikacja**
Podzbiór 1	12,50 ms	12,15 ms	12,35 ms	14,61 ms	37,80 ms	13,88 ms	7,41 ms
Podzbiór 2	12,10 ms	11,96 ms	11,69 ms	14,00 ms	36,36 ms	13,20 ms	6,54 ms
Podzbiór 3	12,35 ms	12,09 ms	11,89 ms	14,28 ms	37,13 ms	13,45 ms	6,58 ms
Średnia	12,32 ms	12,07 ms	11,98 ms	14,30 ms	37,10 ms	13,51 ms	6,84 ms
Samsung Galaxy S5							
Próba	**Filtr Gaussa** 3×3	**Filtr Gaussa** 5×5	**Filtr medianowy 3**	**Filtr medianowy 5**	**Filtr bilateralny**	**Wyostrzenie**	**Eks. cech + klasyfikacja**
Podzbiór 1	12,85 ms	12,18 ms	11,67 ms	15,42 ms	42,88 ms	14,40 ms	13,90 ms
Podzbiór 2	12,05 ms	11,83 ms	10,90 ms	14,05 ms	38,92 ms	14,03 ms	11,13 ms
Podzbiór 3	12,45 ms	12,30 ms	11,42 ms	14,33 ms	38,98 ms	14,70 ms	11,97 ms
Średnia	12,45 ms	12,11 ms	11,33 ms	14,60 ms	40,26 ms	14,38 ms	12,33 ms



Rysunek 34. Wykresy błędu EER dla pozostałych testowanych metod przetwarzania [opracowanie własne]

Rysunek 35. Urządzenie do weryfikacji użytkowników [opracowanie własne]

przetwarzania wstępnego najwyższą skuteczność gwarantował filtr bilateralny, do tego systemu wybrano filtr medianowy o wielkości 5. Wybór ten był podyktowany znacznie krótszym czasem działania przy tylko nieznacznie mniejszej skuteczności. W ramach testów wykonanych zostało 30 eksperymentów. Do urządzenia wprowadzono zestawy uczące składające się z 3 pozytywnych próbek zrobionych kamerą internetową Logitech C130 oraz 7 negatywnych pochodzących z bazy PolyU, do których były porównywane kolejne zdjęcia dłoni. Dla każdego z eksperymentów wyliczono skuteczność rozpoznawania korzystając ze wzoru 3. Otrzymano wyniki w granicach od 85% do 94%.

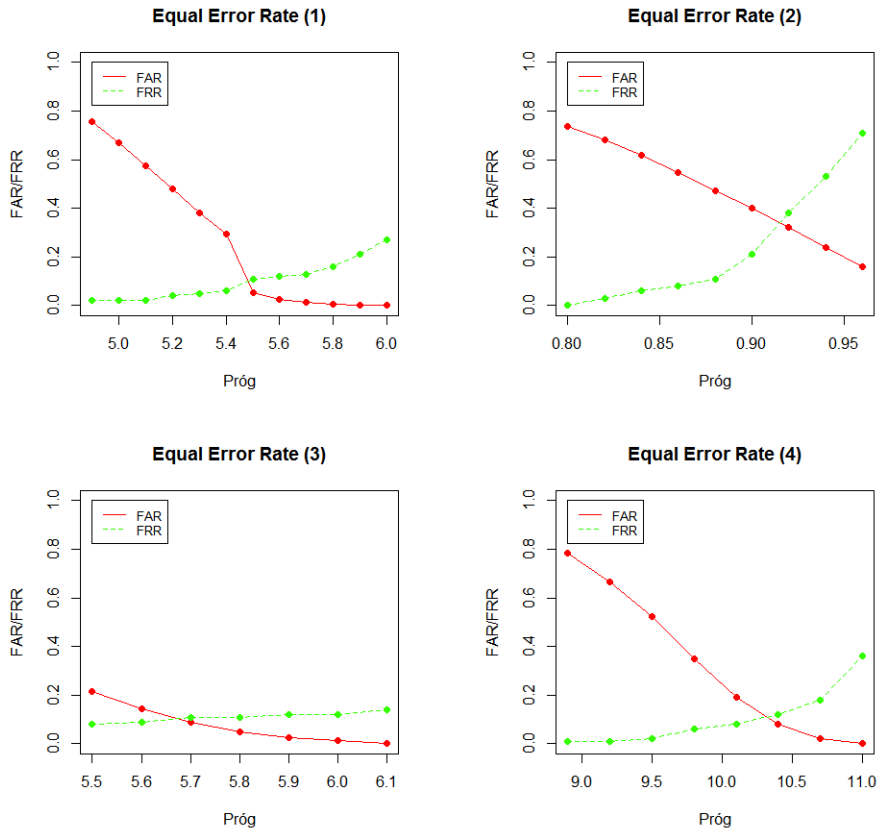
6.2. Badania metody hybrydowej Color-Texture

Aby sprawdzić skuteczność metody hybrydowej CT, przeprowadzono kilka eksperymentów. Miały one na celu zweryfikowanie, czy zaproponowana fuzja jest skuteczna, a także opracowanie parametrów, które gwarantują najbardziej obiecujące rezultaty. W pierwszej części sprawdzono skuteczność rozpoznawania za pomocą metody hybrydowej CT, jednak oddzielnie dla cech koloru i dla cech tekstury. Do eksperymentów wykorzystano bazę PolyU.

Tabela 7. Wyniki skuteczności dla różnych zestawów cech

Rodzaj cech	**Skuteczność**
6 cech tekstury	94,4%
1 cecha koloru	67,7%
6 cech tekstury oraz 1 cecha koloru 5×5	91,0%
6 cech tekstury oraz zwielokrotniona cecha koloru	92,0%

Otrzymane wyniki zaprezentowano w tabeli 7. Ponadto przedstawiono je w postaci wykresów błędów FAR i FRR na rysunku 36. Część 1 tego rysunku



Rysunek 36. Wyniki FAR i FRR dla badania metody hybrydowej CT: 1) cechy tekstury, 2) cechy koloru, 3) 6 cech tekstury + 1 cecha koloru oraz 4) 6 cech tekstury + 1 cecha koloru zwielokrotniona sześciokrotnie [opracowanie własne]

dotyczy wykorzystania tylko cech tekstury, część 2 wyłącznie cechy koloru. Części 3 i 4 przedstawiają wykresy EER dla kolejno: fuzji opartej na sześciu cechach tekstury i jednej koloru oraz fuzji opartej na sześciu cechach tekstury i jednej koloru zwielokrotnionej sześć razy. Z badań wynika, że zaprezentowany sposób nie poprawił w spodziewany sposób skuteczności działania całego systemu. Dla systemu wykorzystującego jedynie cechy tekstury uzyskano najwyższą skuteczność. Natomiast dodanie do wektora cech wartości wyliczonych na podstawie histogramu (cecha koloru) nieznacznie pogorszyło działanie całego systemu (z $94,4\%$ na odpowiednio $91,0\%$ oraz $92,0\%$). Prawdopodobnie jednak system oparty na dwóch rodzajach cech (analizowana tekstura oraz kolor obrazu) jest bardziej uniwersalny.

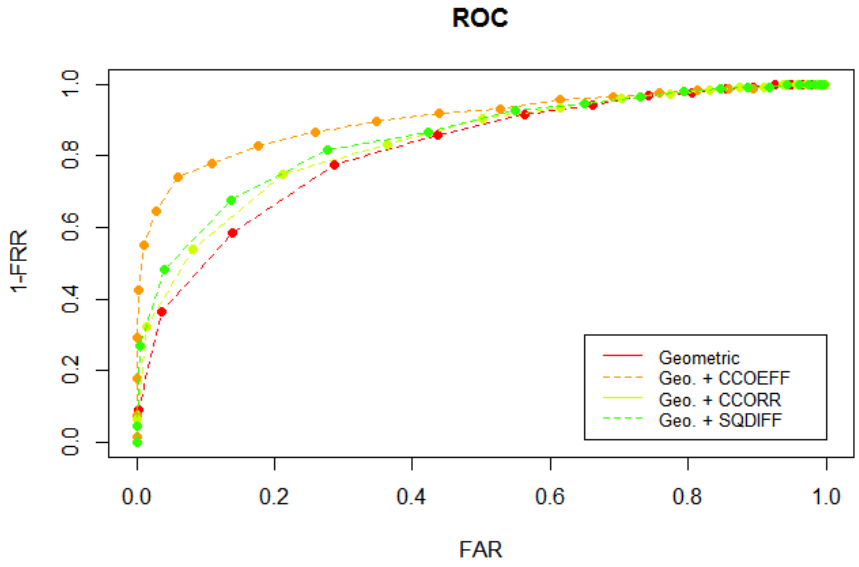
Tabela 8. Czas działania metody CT dla poszczególnych urządzeń mobilnych

Xiaomi Mi6			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	14,9 ms	22,4 ms	37,3 ms
Podzbiór 2	16,3 ms	19,9 ms	36,2 ms
Podzbiór 3	16,4 ms	19,1 ms	35,5 ms
Średnia	15,8 ms	20,5 ms	36,3 ms
Huawei P10 Lite			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	13,5 ms	22,1 ms	35,6 ms
Podzbiór 2	13,6 ms	21,9 ms	35,5 ms
Podzbiór 3	14,7 ms	23,4 ms	38,1 ms
Średnia	13,9 ms	22,5 ms	36,4 ms
Samsung Galaxy A5 2017			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	12,5 ms	26,4 ms	38,9 ms
Podzbiór 2	12,5 ms	25,2 ms	37,7 ms
Podzbiór 3	11,5 ms	25,2 ms	36,7 ms
Średnia	12,2 ms	25,6 ms	37,7 ms
Samsung Galaxy S5			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	14,7 ms	27,5 ms	42,2 ms
Podzbiór 2	12,5 ms	28,7 ms	41,2 ms
Podzbiór 3	13,2 ms	34,0 ms	47,2 ms
Średnia	13,5 ms	30,1 ms	43,5 ms

Do implementacji na telefonach komórkowych wybrano metodę fuzji gwarantującą najwyższą skuteczność - użyto więc sześciu cech tekstury i jednej cechy koloru zwielokrotnionej sześciokrotnie. Podczas wykonywania testów, obserwowano czas działania algorytmu. W tabeli 8 przedstawiono czasy autoryzacji dla pojedynczej próbki. Eksperyment przeprowadzono dla trzech grup próbek. Ponieważ czas podejmowania decyzji (klasyfikacja) był pomijalny, został włączony do czasu wydobycia cech.

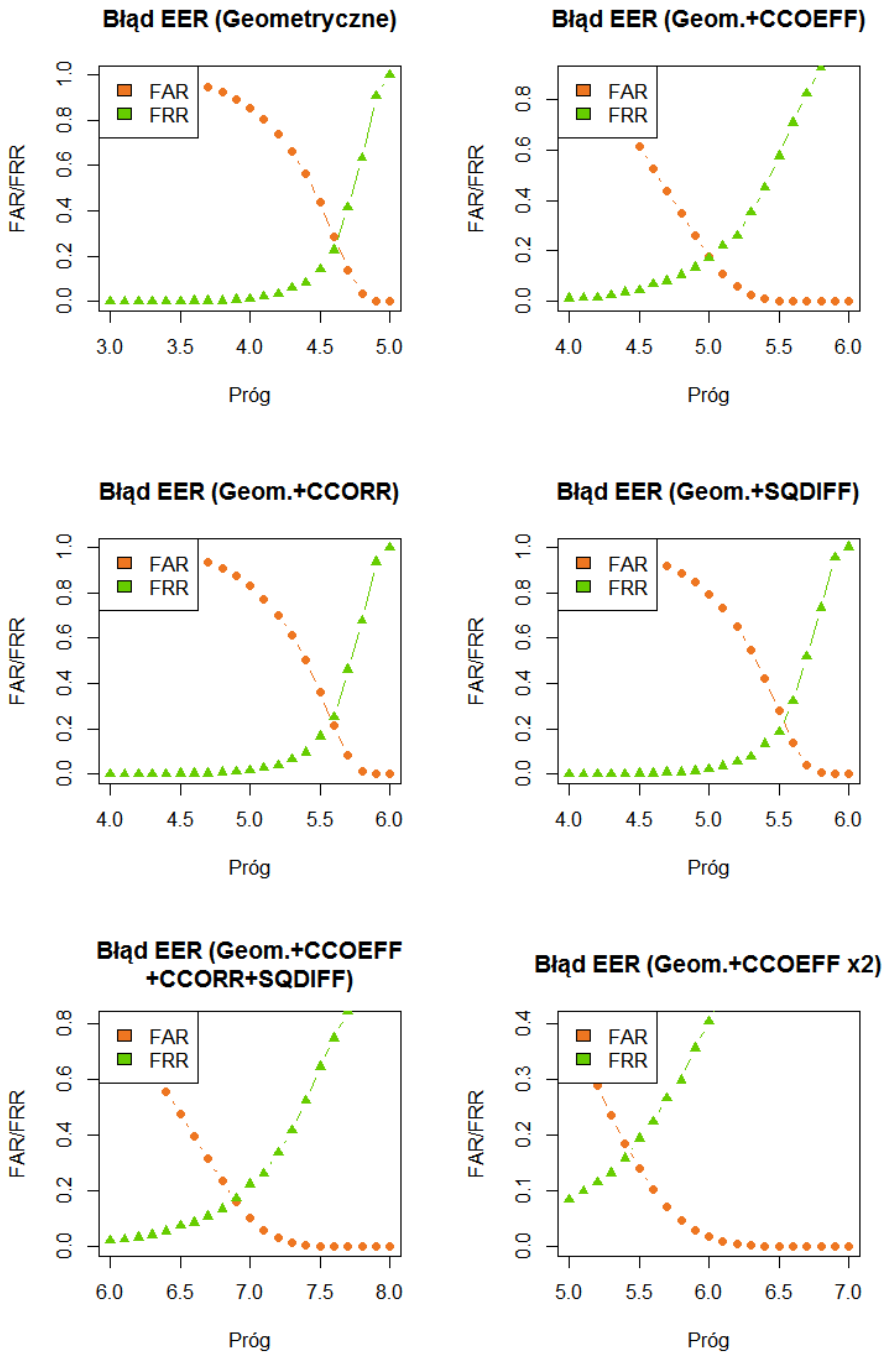
6.3. Badanie metody hybrydowej Geometric-Texture

Kolejna seria eksperymentów dotyczyła metody hybrydowej GT, w której poza cechami geometrycznymi do systemu wytypowane zostały też cechy teksturowe, czyli korelacje. Z racji tego, że próbki w bazie PolyU nie przedstawiają całej dłoni, zdecydowano się użyć innej bazy, mianowicie IITD. W pierwszym eksperymencie sprawdzono, która z trzech metod (*CCOEFF*, *CCORR* oraz *SQDIFF*) daje najbardziej obiecujące rezultaty. Wyniki tego eksperymentu są przedstawione na rysunku 37. Widać na nim krzywe ROC, które dla najlepiej działającego systemu mocno zbliżają się do lewego górnego rogu wykresu. Na



Rysunek 37. Krzywe ROC dla prezentowanego systemu [opracowanie własne]

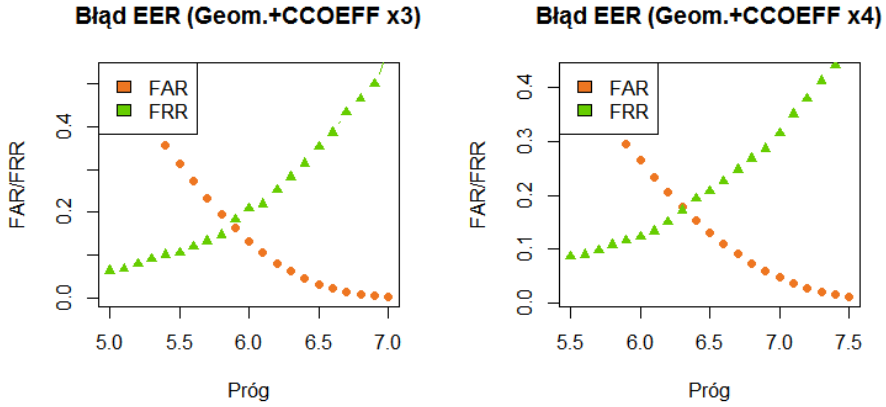
wykresie najlepszą pozycję zajmują więc wyniki oznaczone kolorem pomarańczowym, które dotyczą fuzji cech geometrycznych z korelacją *CCOEFF*. To połączenie zatem uznano za najlepiej działające. Ponieważ jednak do klasyfikacji użyto 5 cech geometrycznych i tylko jednej teksturowej, w kolejnym eksperymencie zmodyfikowano ten stosunek. Wykorzystano więc 5 cech geometrycznych oraz 3 cechy teksturowe (po jednej obliczonej metodami *CCOEFF*, *CCORR* oraz *SQDIFF*). Podejście to nie przyniosło poprawy skuteczności, która wyniosła 83%. Z tego powodu zdecydowano przeprowadzić kolejny eksperyment, w którym oprócz 5 cech geometrycznych wykorzystano wynik najbardziej obiecującej metody analizy tekstury (czyli *CCOEFF*) pomnożony przez x przyjmując wartości z przedziału $< 2, 4 >$. Okazało się jednak, że nie przyniosło to poprawy skuteczności, która utrzymała się na poziomie 83%. Podsumowanie wyników wszystkich eksperymentów przeprowadzonych podczas tego badania przedstawiono w tabeli 9. Z kolei rysunki 38 oraz 39 przedstawiają wykresy błędu EER dla wszystkich sprawdzonych fuzji testowanych w ramach tej metody. Czasy działania wszystkich kombinacji cech metody GT na urządzeniach mobilnych przedstawiono w tabeli 10. Zestawienie czasów pozwala stwierdzić, że są one bardzo porównywalne dla wszystkich zestawów cech wykorzystanych do rozpoznawania osób. Zwraca uwagę jedynie niewielkie zwiększenie czasu działania dla połączenia cech geometrycznych i trzech różnych cech tekstury.



Rysunek 38. Wykresy błędu EER dla metody GT (1/2) [opracowanie własne]

Metoda	Skuteczność
Geometryczne	74%
Geometryczne + CCOEFF	**83%**
Geometryczne + CCORR	77%
Geometryczne + SQDIFF	78%
Geometryczne + CCOEFF + CCORR + SQDIFF	83%
Geometryczne + 2 · CCOEFF	83%
Geometryczne + 3 · CCOEFF	83%
Geometryczne + 4 · CCOEFF	83%

Tabela 9. Podsumowanie wyników metody hybrydowej GT



Rysunek 39. Wykresy błędu EER dla metody GT (2/2) [opracowanie własne]

6.4. Badanie metody 3-wartościowej maski

Wyniki eksperymentów przeprowadzonych dla metody 3-wartościowej maski zostały przedstawione w postaci tabeli 11. Testy te zostały przeprowadzone na próbkach z bazy PolyU. Okazało się, że najlepszą skuteczność uzyskano przy klasyfikacji metodą SVM.

Mimo, że uzyskano wysoka skuteczność rozpoznawania (ponad 95,5%), wyniki błędów FAR i FRR nie były satysfakcjonujące - szczególnie wysoki był błąd FRR. Pojawia się on w przypadku, gdy pozytywna próbka zostaje odrzucona, gdyż w procesie podejmowania decyzji zostaje oceniona jako negatywna. Zdecydowano się więc przeprowadzić kolejne testy. Dlatego też wykonano ponowne uczenie i predykcję dla najbardziej obiecującego algorytmu uczenia maszynowego (SVM), jednak dla kodu o większej długości. Aby uzyskać reprezentację obrazu ROI w postaci wektora o długości 25 i 36 podzielono obraz ROI na większą ilość bloków. Pozostałe elementy badania pozostały niezmienione. Zauważono, że użycie dłuższego kodu wpływa pozytywnie na poprawę skuteczności,

Tabela 10. Czas działania metody GT dla urządzeń mobilnych

Xiaomi Mi6								
Próba	**Geom.**	**Geometryczne +CCOEFF**	**Geometryczne +CCORR**	**Geometryczne +SQDIFF**	**Geom.+CCOEFF +CCORR+SQDIFF**	**Geometryczne +2 x CCOEFF**	**Geometryczne +3 x CCOEFF**	**Geometryczne +4 x CCOEFF**
Podzbiór 1	32,2 ms	32,3 ms	31,9 ms	32,5 ms	37,2 ms	32,1 ms	32,8 ms	32,1 ms
Podzbiór 2	34,0 ms	33,3 ms	32,3 ms	32,3 ms	37,6 ms	32,7 ms	32,1 ms	31,7 ms
Podzbiór 3	32,4 ms	32,4 ms	32,5 ms	31,8 ms	37,7 ms	31,8 ms	31,8 ms	32,4 ms
Średnia	32,9 ms	32,7 ms	32,3 ms	32,2 ms	37,5 ms	32,2 ms	32,2 ms	32,1 ms
Huawei P10 Lite								
Próba	**Geom.**	**Geometryczne +CCOEFF**	**Geometryczne +CCORR**	**Geometryczne +SQDIFF**	**Geom.+CCOEFF +CCORR+SQDIFF**	**Geometryczne +2 x CCOEFF**	**Geometryczne +3 x CCOEFF**	**Geometryczne +4 x CCOEFF**
Podzbiór 1	58,6 ms	50,1 ms	51,3 ms	54,9 ms	58,1 ms	55,1 ms	56,2 ms	50,0 ms
Podzbiór 2	53,9 ms	52,0 ms	51,8 ms	56,4 ms	56,7 ms	52,6 ms	58,8 ms	55,2 ms
Podzbiór 3	56,0 ms	54,7 ms	55,3 ms	50,8 ms	59,3 ms	52,5 ms	53,1 ms	51,4 ms
Średnia	56,2 ms	52,3 ms	52,8 ms	54,0 ms	58,0 ms	53,4 ms	56,0 ms	52,2 ms
Samsung Galaxy A5 2017								
Próba	**Geom.**	**Geometryczne +CCOEFF**	**Geometryczne +CCORR**	**Geometryczne +SQDIFF**	**Geom.+CCOEFF +CCORR+SQDIFF**	**Geometryczne +2 x CCOEFF**	**Geometryczne +3 x CCOEFF**	**Geometryczne +4 x CCOEFF**
Podzbiór 1	80,8 ms	89,3 ms	96,8 ms	83,5 ms	101,9 ms	839, ms	91,5 ms	84,0 ms
Podzbiór 2	81,6 ms	80,5 ms	83,4 ms	81,8 ms	95,4 ms	80,3 ms	82,7 ms	81,1 ms
Podzbiór 3	75,8 ms	81,5 ms	79,9 ms	79,4 ms	94,9 ms	80,0 ms	79,8 ms	80,8 ms
Średnia	79,4 ms	83,8 ms	86,7 ms	81,6 ms	97,4 ms	81,4 ms	84,7 ms	82,0 ms
Samsung Galaxy S5								
Próba	**Geom.**	**Geometryczne +CCOEFF**	**Geometryczne +CCORR**	**Geometryczne +SQDIFF**	**Geom.+CCOEFF +CCORR+SQDIFF**	**Geometryczne +2 x CCOEFF**	**Geometryczne +3 x CCOEFF**	**Geometryczne +4 x CCOEFF**
Podzbiór 1	86,2 ms	79,5 ms	86,3 ms	82,3 ms	81,7 ms	90,3 ms	85,2 ms	87,9 ms
Podzbiór 2	66,7 ms	72,7 ms	74,2 ms	76,2 ms	82,4 ms	80,0 ms	76,4 ms	72,8 ms
Podzbiór 3	72,1 ms	72,8 ms	73,9 ms	78,3 ms	89,0 ms	78,0 ms	80,9 ms	77,8 ms
Średnia	75,0 ms	75,0 ms	78,1 ms	78,9 ms	84,4 ms	82,8 ms	80,8 ms	79,5 ms

Tabela 11. Wyniki klasyfikacji dla metody 3-wartościowej maski

Metoda	Podzbiór 1	Podzbiór 2	Podzbiór 3	Średnia
Odległość Manhattan	93,0%	93,5%	92,2%	92,9%
SVM	95,7%	95,2%	95,6%	**95,5%**
Drzewo decyzyjne	85,5%	85,6%	85,5%	85,5%

Tabela 12. Wyniki klasyfikacji dla metody 3-krotnej walidacji dla kodów różnej długości

16 elementów			
Próba	**Skuteczność**	**FAR**	**FRR**
Podzbiór 1	95,7%	4,8%	16,7%
Podzbiór 2	95,2%	5,3%	25,7%
Podzbiór 3	95,6%	4,5%	11,0%
Średnia	95,5%	4,9%	17,8%
25 elementów			
Próba	**Skuteczność**	**FAR**	**FRR**
Podzbiór 1	95,3%	5,3%	7,7%
Podzbiór 2	95,4%	5,0%	15,7%
Podzbiór 3	96,1%	5,2%	7,0%
Średnia	95,6%	5,2%	10,1%
36 elementów			
Próba	**Skuteczność**	**FAR**	**FRR**
Podzbiór 1	98,5%	2,2%	8,3%
Podzbiór 2	98,5%	2,1%	12,0%
Podzbiór 3	97,8%	3,0%	5,0%
Średnia	**98,3%**	2,4%	8,4%

a także na minimalizację błędów FAR (z $4,9\%$ do $2,4\%$) oraz FRR (z $17,8\%$ na $8,4\%$). Szczegółowe wyniki zostały przedstawione w tabeli 12. Porównano również czasy uczenia takich wersji kodu i uzyskano tylko nieznacznie dłuższy czas uczenia - dłuższe o odpowiednio $5,5\%$ i $6,7\%$ w zależności od wersji kodu. Porównano również czas weryfikacji jednej próbki na urządzeniach mobilnych. Tabela 13 zawiera czasy przetwarzania wstępnego oraz łączny czas wydobycia cech i klasyfikacji dla wszystkich urządzeń mobilnych. Wyróżniono metody klasyfikacji: DT - drzewo decyzyjne, SVM-16 - SVM dla kodu o długości 16 elementów, SVM-25 - SVM dla kodu o długości 25 elementów, SVM-36 - SVM dla kodu o długości 36 elementów, CBD - City Block Distance. Widać jednoznacznie, że czas działania poszczególnych metod jest bardzo zbliżony.

6.5. Badanie metody kodu binarnego

Podczas oceny metody kodu binarnego przeprowadzono kilka eksperymentów. Wykorzystano w nich próbki z bazy PolyU. Na samym początku przeprowadzone zostały dwa eksperymenty, które można określić jako wstępne. Zastosowano w nich oddzielnie kodowanie korzystające z miary *Haralick Sum Average* i oddzielnie z miary *Haralick Sum Variance*. Zmieniono więc nieco założenia

Tabela 13. Czas działania metody 3-wartościowej maski dla urządzeń mobilnych

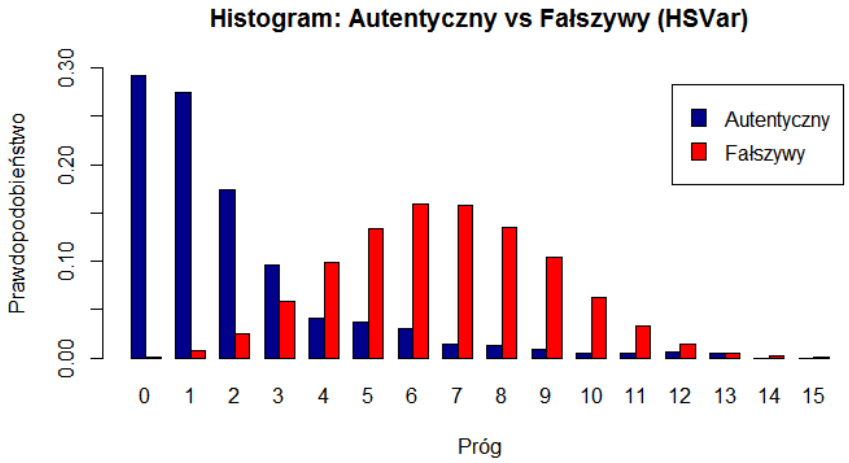
Xiaomi Mi6						
Próba	**Przet. wstępne**	**DT**	**SVM-16**	**SVM-25**	**SVM-36**	**CBD**
Podzbiór 1	14,7 ms	63,9 ms	64,1 ms	69,9 ms	73,3 ms	65,8 ms
Podzbiór 2	14,8 ms	64,2 ms	64,3 ms	73,3 ms	70,2 ms	64,3 ms
Podzbiór 3	13,9 ms	64,2 ms	65,3 ms	71,8 ms	71,9 ms	64,2 ms
Średnia	14,5 ms	64,1 ms	64,5 ms	71,8 ms	71,6 ms	64,8 ms
Huawei P10 Lite						
Próba	**Przet. wstępne**	**DT**	**SVM 16**	**SVM 25**	**SVM 36**	**CBD**
Podzbiór 1	14,2 ms	86,4 ms	89,3 ms	88,7 ms	90,0 ms	89,0 ms
Podzbiór 2	13,8 ms	85,0 ms	84,1 ms	86,4 ms	89,5 ms	83,9 ms
Podzbiór 3	14,3 ms	84,7 ms	83,8 ms	85,3 ms	86,5 ms	83,7 ms
Średnia	14,1 ms	85,4 ms	85,7 ms	86,8 ms	88,7 ms	85,5 ms
Samsung Galaxy A5 2017						
Próba	**Przet. wstępne**	**DT**	**SVM 16**	**SVM 25**	**SVM 36**	**CBD**
Podzbiór 1	10,3 ms	195,8 ms	194,3 ms	183,8 ms	190,8 ms	194,1 ms
Podzbiór 2	8,3 ms	180,4 ms	178,9 ms	181,7 ms	187,4 ms	183,2 ms
Podzbiór 3	8,1 ms	177,7 ms	180,0 ms	183,1 ms	188,8 ms	179,3 ms
Średnia	8,9 ms	184,6 ms	184,4 ms	182,9 ms	189,0 ms	185,5 ms
Samsung Galaxy S5						
Próba	**Przet. wstępne**	**DT**	**SVM 16**	**SVM 25**	**SVM 36**	**CBD**
Podzbiór 1	13,4 ms	162,8 ms	169,2 ms	173,3 ms	187,2 ms	164,8 ms
Podzbiór 2	10,3 ms	176,3 ms	178,4 ms	150,9 ms	185,3 ms	165,3 ms
Podzbiór 3	10,0 ms	168,6 ms	172,1 ms	190,4 ms	193,5 ms	177,3 ms
Średnia	11,2 ms	169,9 ms	172,5 ms	171,5 ms	188,7 ms	169,1 ms

Tabela 14. Porównanie wyników eksperymentów dotyczących kodów wykorzystujących oddzielnie *Haralick Sum Average* i *Haralick Sum Variance* oraz połączenie tych kodów

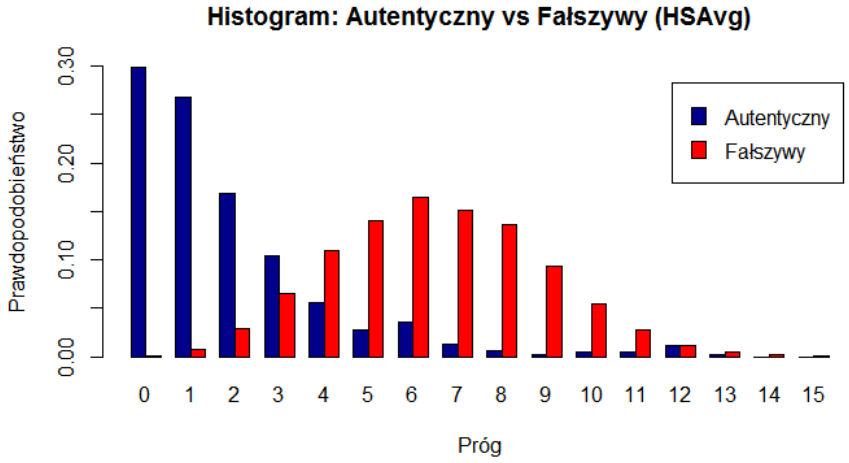
Nazwa	**HSAvg**	**HSVar**	**HSAvg + HSVar**
Próg	3	3	6
Prawd. autentyczny	83,9%	83,6%	83,5%
Prawd. fałszywy	10,0%	9,0%	7,0%
Skuteczność	89,6%	90,8%	**92,0%**

metody, bo w przypadku tych dwóch eksperymentów ROI został przedstawiony w postaci kodu o długości 16 bitów. Wynik działania zaprezentowany został w postaci histogramu zwanego *Genuine/Impostor*, czyli Autentyczny/Prawdziwy. Histogramy te widać na rysunku 40 oraz 41. Z histogramu można odczytać prawdopodobieństwo, z jakim autentyczna lub fałszywa próbka będzie oddalona od próbki uczącej o zadaną odległość *City Block Distance*. Należy tu pamiętać, iż im mniejsza jest część wspólna obu histogramów, tym lepszą skuteczność gwarantuje podejście. Następnie przeprowadzono fuzję badanych kodowań i sprawdzono czy jednoczesne wykorzystanie obu miar pozwoli na poprawę rezultatów, a wyniki przedstawione zostały w tabeli 14. Zauważono, że fuzja cech poprawia skuteczność rozpoznawania użytkowników z $89,6\%$ na $92,0\%$.

W następnym etapie badań postanowiono sprawdzić, czy skuteczność ulegnie poprawie, kiedy zwiększy się zestaw uczący. W tym celu przeprowadzono eksperyment, w którym porównywana była próbka testowa z odpowiednio trzema



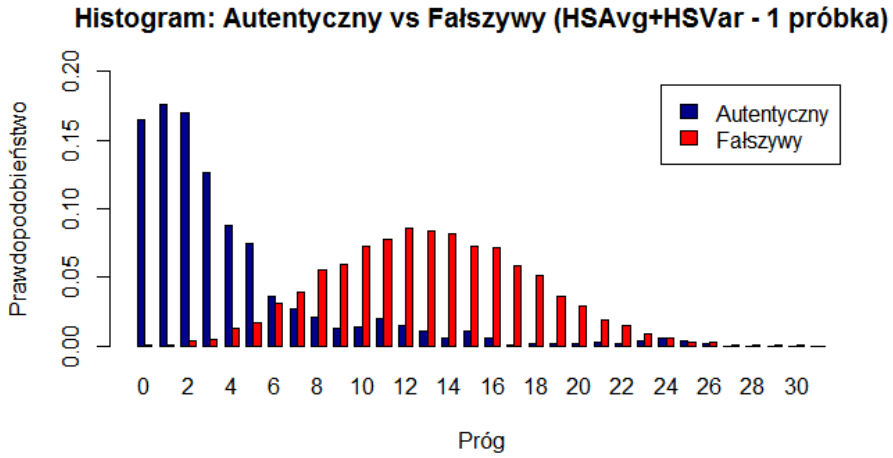
Rysunek 40. Histogram Autentyczny/Fałszywy dla kodu o długości 16 bitów korzystającego tylko z miary *Haralick Sum Variance* [opracowanie własne]



Rysunek 41. Histogram Autentyczny/Fałszywy dla kodu o długości 16 bitów korzystającego tylko z miary *Haralick Sum Average* [opracowanie własne]

Tabela 15. Wyniki uzyskane w wyniku kolejnych eksperymentów polegających na zwiększaniu zestawu uczącego

Eksperyment	Podzbiór 01	Podzbiór 02	Podzbiór 03	Średnia
1 próbka	–	–	–	91,96%
3 próbki	87,50%	92,51%	87,45%	89,15%
6 próbki	90,95%	94,56%	90,97%	**92,16%**



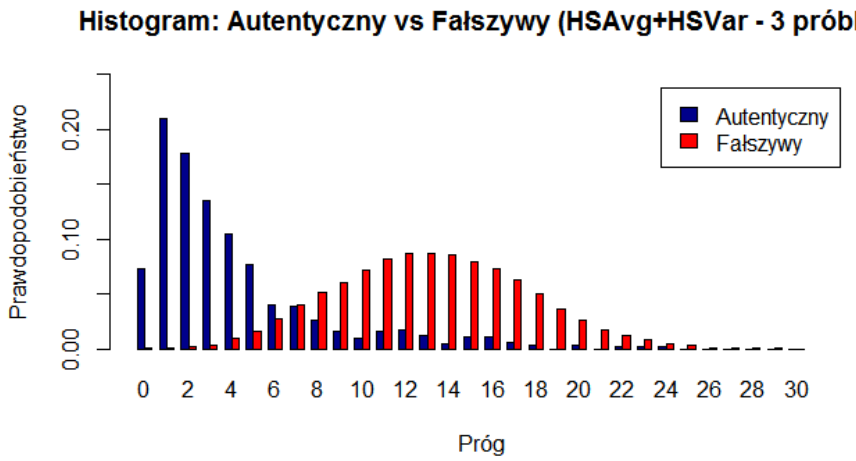
Rysunek 42. Histogram Autentyczny/Fałszywy dla kodu o długości 32 bitów korzystającego z jednej próbki uczącej [opracowanie własne]

lub sześcioma próbkami uczącymi. Wyniki eksperymentu przedstawiono w tabeli 15 oraz w postaci wykresów jako histogramy Prawdziwy/Fałszywy na rysunkach 42, 43 oraz 44. Otrzymane wyniki są dość porównywalne dla wszystkich testowanych opcji.

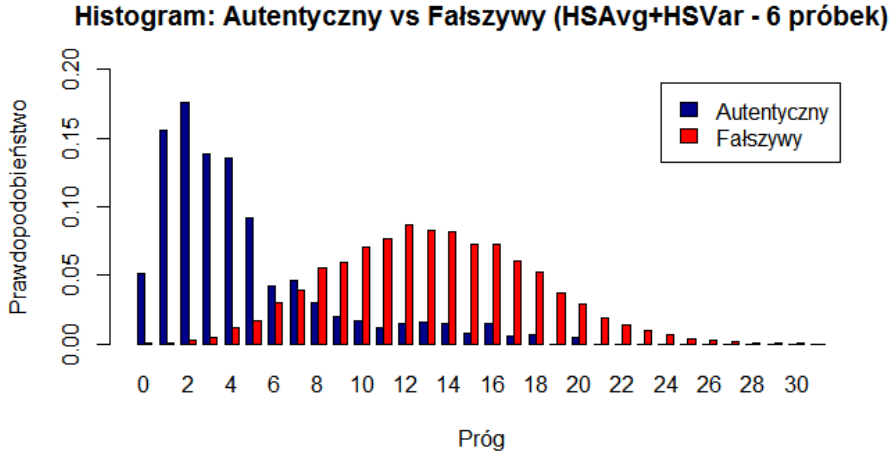
Przydatność metody kodu binarnego zweryfikowano również dla urządzeń mobilnych. Zaimplementowano wszystkie kolejne kroki algorytmu: przetwarzanie wstępne, ekstrakcję cech oraz klasyfikację na czterech urządzeniach mobilnych. Czasy poszczególnych etapów zostały zaprezentowane w tabeli 16. W tabeli zrezygnowano jednak z prezentowania czasu działania klasyfikacji, który był pomijanie mały. Czasy działania metody na każdym z urządzeń testowych były podobne.

6.6. Badanie metody energii tekstury

Zaproponowana metoda przewiduje wykorzystanie metody uczenia maszynowego SVM, co zobligowało do stworzenia zestawów próbek uczących. Dla



Rysunek 43. Histogram Autentyczny/Fałszywy dla kodu o długości 32 bitów korzystającego z trzech próbek uczących [opracowanie własne]



Rysunek 44. Histogram Autentyczny/Fałszywy dla kodu o długości 32 bitów korzystającego z sześciu próbek uczących [opracowanie własne]

Tabela 16. Czas działania metody kodu binarnego dla urządzeń mobilnych

Xiaomi Mi6			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	15,0 ms	14,6 s	14,6 s
Podzbiór 2	14,9 ms	14,5 s	14,5 s
Podzbiór 3	14,8 ms	14,4 s	14,4 s
Średnia	14,9 ms	14,5 s	14,5 s
Huawei P10 Lite			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	13,9 ms	13,9 s	13,9 s
Podzbiór 2	14,3 ms	13,8 s	13,8 s
Podzbiór 3	13,8 ms	14,5 s	14,5 s
Średnia	14,0 ms	13,8 s	13,8 s
Samsung Galaxy A5 2017			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	13,4 ms	13,8 s	13,8 s
Podzbiór 2	11,8 ms	13,7 s	13,7 s
Podzbiór 3	10,6 ms	13,7 s	13,7 s
Średnia	12,1 ms	13,7 s	13,7 s
Samsung Galaxy S5			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	15,1 ms	15,3 s	15,3 s
Podzbiór 2	12,8 ms	15,5 s	15,5 s
Podzbiór 3	12,8 ms	15,6 s	15,6 s
Średnia	13,5 ms	15,5 s	15,5 s

każdego użytkownika z bazy PolyU przygotowano zestaw uczący, który składał się z 10 próbek tego użytkownika i 10 innych losowych próbek. W całym badaniu użyto w sumie 7720 zdjęć. W pierwszej części badań przetestowano system, który składał się wyłącznie z cech pochodzących z energii tekstury. System więc opierał się na 64 liczbach binarnych. Wyniki skuteczności metody przedstawiono w tabeli 17. Następnie w ten sam sposób przetestowano metodę dla dłuższego kodu, który uwzględniał cechy obliczone na podstawie energii tekstury oraz długości przebiegów.

Tabela 17. Skuteczność działania metody energii tekstury z wykorzystaniem kodu o długości 64 i 70

Próba	**Kod krótki - 64 liczb**	**Kod długi - 70 liczb**
Podzbiór 1	84,78%	94,80%
Podzbiór 2	84,73%	95,01%
Podzbiór 3	83,53%	94,05%
Średnia	84,35%	**94,62%**

Otrzymane wyniki pokazują, że dodanie 6 elementów związanych z długością przebiegów do wektora cech powoduje zwiększenie skuteczności działania systemu o ponad 10%. Użycie dłuższego kodu pozwala osiągnąć prawie 95% skuteczności (średnia z wykonanych pomiarów dla różnych zestawów próbek

Tabela 18. Czas działania metody energii tekstury dla poszczególnych urządzeń mobilnych

Xiaomi Mi6			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	10,42 ms	67,71 ms	76,13 ms
Podzbiór 2	11,08 ms	66,50 ms	77,58 ms
Podzbiór 3	13,26 ms	65,72 ms	78,98 ms
Średnia	11,59 ms	65,98 ms	77,57 ms
Huawei P10 Lite			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	12,17 ms	93,20 ms	105,37 ms
Podzbiór 2	13,02 ms	95,11 ms	108,13 ms
Podzbiór 3	12,87 ms	93,58 ms	106,45 ms
Średnia	12,69 ms	93,96 ms	106,65 ms
Samsung Galaxy A5 2017			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	11,72 ms	169,19 ms	180,91 ms
Podzbiór 2	10,68 ms	170,00 ms	180,68 ms
Podzbiór 3	11,23 ms	173,50 ms	184,73 ms
Średnia	11,21 ms	170,90 ms	182,11 ms
Samsung Galaxy S5			
Próba	**Przet. wstępne**	**Eks. cech + klasyfikacja**	**Suma**
Podzbiór 1	13,10 ms	161,94 ms	175,04 ms
Podzbiór 2	12,78 ms	165,89 ms	178,67 ms
Podzbiór 3	13,20 ms	156,19 ms	169,39 ms
Średnia	13,03 ms	161,34 ms	174,37 ms

uczących). Czas weryfikacji jednej próbki dla poszczególnych urządzeń został przedstawiony w tabeli 18. Dane te dotyczą kodu o długości 70 elementów.

7. Podsumowanie i wnioski

Niniejsza praca doktorska przedstawia nowe metody identyfikacji osób na podstawie analizy obrazu dłoni na urządzeniach mobilnych. Autorka zawarła w niej sześć własnych metod, które umożliwiają weryfikację użytkownika na podstawie wybranej cechy biometrycznej. Ponadto praca zwiera wyniki badań przeprowadzonych nad popularnymi metodami przetwarzania wstępnego oraz opis bazy danych, która w przyszłości będzie mogła zostać wykorzystana w badaniach nad systemami analizującymi obraz dłoni.

Porównywane metody przetwarzania wstępnego umożliwiły poprawę działania metody opartej na HOG w porównaniu do użycia surowych, niezmienionych próbek. Wszystkie analizowane metody poza wyostrzeniem gwarantowały poprawę skuteczności rozpoznawania. Najwyższą skuteczność osiągnięto dla filtru bilateralnego, którego cechą charakterystyczną jest dobre zachowanie krawędzi. Metoda ta była również najwolniejszą spośród analizowanych metod przetwarzania wstępnego.

Przedstawione w pracy metody rozpoznawania osób gwarantują różną skuteczność działania. Wszystkie propozycje metod oraz wybrane metody znane z literatury zostały przedstawione w tabeli 19. Zawarto w niej nazwę metody wraz z maksymalną otrzymaną skutecznością oraz średnim czasem, jaki był potrzebny do analizy jednej próbki w ten sposób. Najbardziej obiecującą z proponowanych metod jest metoda 3-wartościowej maski, która umożliwiała weryfikację osób ze skutecznością przekraczającą 98%, a czas jej działania nie przekraczał 0,1s. Można więc uznać ją za najlepszą spośród proponowanych w pracy. Niestety nie wszystkie proponowane metody udało się z sukcesem przenieś do scenariusza mobilnego. Tu należy wymienić metodę kodu binarnego, która choć była oparta na bardzo krótkim kodzie i gwarantowała skuteczność przekraczającą 92%, była zbyt skomplikowana obliczeniowo. Czas przetwarzania jednej próbki wyniósł bowiem prawie 14 sekund. Warto również zauważyć, że czas działania poszczególnych metod na urządzeniach mobilnych nie był zależny od długości wektora. Doskonałym tego przykładem była metoda oparta na HOG, która pomimo najdłuższego wektora cech miała najkrótszy czas działania. Porównanie wyników pokazuje również, że proponowane metody w przeważającej większości gwarantowały krótszy czas działania niż metody znane z literatury. Niestety to porównanie może okazać się niepełne, gdyż w znacznej części publikacji nie

Tabela 19. Porównanie proponowanych metod i metod znanych z literatury

Nazwa	Maks. skuteczność	Min. czas
Moco et al. [53]	FRR=9,27% FAR=0,03%	466 ms
Kim et al. [43]	EER=2,88%	685 ms
Fang [26]	EER=4,5%	brak danych
Ungureanu et al. [73]	90%	brak danych
Tiwari et al. [70]	EER=5,55%	889,2 ms
Leng et al. [51]	EER powyżej 2%	brak danych
Zhang et al. [87]	90%	162 ms
Metoda oparta na HOG	97,1%	33,1 ms
Metoda hybrydowa CT	92,0%	36,3 ms
Metoda hybrydowa GT	83,0%	32,7 ms
Metoda 3-wart. maski	**98,3%**	86,1 ms
Metoda kodu binarnego	92,2%	13700 ms
Metoda energii tekstury	94,5%	77,6 ms

podano czasu działania dla jednej próbki. W tych przypadkach w tabeli wpisano komentarz „brak danych".

We wszystkich proponowanych metodach czasy wykonywania były oceniane przez implementację danego systemu na kolejnych, czterech urządzeniach mobilnych, które różniły się wersją systemu operacyjnego Android, procesorem oraz wielkością pamięci RAM. We wszystkich eksperymentach telefony Xiaomi Mi6 oraz Huawei P10 Lite gwarantowały szybsze od pozostałych dwóch działanie. **Niemniej jednak można jednoznacznie stwierdzić, że zaprezentowane metody potwierdziły tezę pracy, a wszystkie jej cele zostały zrealizowane.**

Należy jednak pamiętać, że tworzenie skutecznych i efektywnych pod względem czasu działania systemów to niejedyny problem biometrii. Jakie są więc kolejne kroki rozwoju obrazu dłoni jako cechy biometrycznej i jej zastosowań? Aktualnie wskazuje się kilka palących problemów biometrycznego rozpoznawania osób, które można uznać za plany dalszych działań naukowych Autorki.

Pierwszym z nich jest kontrola żywotności próbki. Jest to sposób zabezpieczenia systemu przed sytuacją, w której osoba atakująca system przedłoży przed obiektyw aparatu telefonu zdjęcie lub wydruk dłoni należącej do właściciela urządzenia. Obecnie wydaje się, że możliwe są co najmniej dwa rozwiązania tego problemu. Wykrycie fałszywej próbki można oprzeć na analizie obrazu i wykorzystaniu sztucznej inteligencji. Można również zmienić algorytm pobierania próbki od użytkownika i w ten sposób zobligować go do wykonania najpierw losowej sekwencji ruchów, a następnie wykonać analizę obrazu dłoni.

Innym palącym problemem jest starzenie się próbki. Biometria jest na tyle młodą dziedziną informatyki, że wciąż brakuje baz danych zbieranych na przestrzeni długiego czasu. Zwykle próbki do bazy pobiera się w kilku sesjach, jednak są one oddalone od siebie o kilka dni lub kilka miesięcy. Wobec tego pojawia się

problem skuteczności weryfikacji tożsamości osoby, w przypadku gdy system został nauczony raz, a ta osoba chciałaby z niego skorzystać po 20 latach. Problem ten mogłaby rozwiązać technika ustawicznego uczenia (ang. *lifelong learning*). System korzystający z takiego rozwiązania co jakiś określony czas miałby douczać swój klasyfikator.

Inną sprawą jest bezpieczeństwo próbki biometrycznej, sposoby jej ochrony. Ten temat jednak można rozszerzyć w ogóle do cyberbezpieczeństwa, bezpieczeństwa użytkownika w sieci i bezpieczeństwa danych. W tej tematyce z pewnością jeszcze wiele można odkryć.

Bibliografia

[1] Afsal S. et al. 2016. A novel approach for palm print recognition using entropy information features. [W:] International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, ss. 1439–1442.

[2] Ahmadi M. oraz Hossein S. 2019. Palmprint image registration using convolutional neural networks and Hough transform, arXiv:1904.00579, [dostęp: 15-02-2020].

[3] Amraoui A. et al. 2018. Multispectral palmprint recognition based on fusion of local features. [W:] 6th International Conference on Multimedia Computing and Systems (ICMCS), IEEE, ss. 1–6.

[4] Bailador G. et al.2018. Flooding-based segmentation for contactless hand biometrics oriented to mobile devices. IET Biometrics 7(5), ss. 431–438.

[5] Baza obrazów wewnętrznej części dłoni CASIA, `http://biometrics.idealtest.org/index.jsp` [dostęp: 06-03-2017].

[6] Baza obrazów wewnętrznej części dłoni IITD, `http://www4.comp.polyu.edu.hk/~csajaykr/database.php` [dostęp: 06-03-2017].

[7] Baza obrazów wewnętrznej części dłoni PolyU, `http://www4.comp.polyu.edu.hk/~biometrics/` [dostęp: 06-03-2017].

[8] Bochenek A. oraz Reicher M. 2014. Anatomia człowieka, t. 1, PZWL Wydawnictwo Lekarskie Warszawa.

[9] Bolle R. M. et al. 2004. Guide to Biometrics, Springer Cham.

[10] Buoncompagni S. et al. 2018. Efficient Sketch Recognition Based on Shape Features and Multidimensional Indexing. [W:] International Conference on Computer Recognition Systems (CORES), Springer, ss. 159–169.

[11] Chaudhary G. oraz Srivastava S. 2019. A robust 2D-Cochlear transform-based palmprint recognition. Soft Computing, ss. 1–18.

[12] Chen J. et al. 2001. Palmprint recognition using crease. [W:] International Conference on Image Processing, IEEE, ss. 234–237.

[13] Chen J. et al. 2010. Palmprint authentication using a symbolic reresentation of images. Image and Vision Computing 28(3), ss. 343–351.

[14] Choraś R.S. oraz Choraś M. 2006. Hand shape geometry and palmprint features for the personal identification. [W:] International Conference on Intelligent Systems Design and Applications, IEEE, ss. 1085–1090.

[15] Choraś M. et al. 2008. A novel shape-based approach to palmprint detection and identification. [W:] International Conference on Intelligent Systems Design and Applications, IEEE, ss. 638–643.

[16] Choraś M. oraz Kozik R. 2010. Feature extraction method for contactless palmprint biometrics. [W:] International Conference on Intelligent Computing, Springer, ss. 435–442.

[17] Choraś M. oraz Kozik R. 2011. Fast Feature Extractors for Palmprint Biometrics. [W:] Computer Information Systems–Analysis and Technologies, Springer, ss. 121–127.
[18] Choraś M. oraz Kozik R. 2012. Contactless palmprint and knuckle biometrics for mobile devices. Pattern Analysis and Applications 15(1), ss. 73–85.
[19] Dasgupta D. et al. 2017. Multi-Factor Authentication. [W:] Advances in User Authentication, Springer, ss. 185–233.
[20] Devinaga R. oraz Yuen Y.Y. 2016. Use Acceptance of Biometric Authentication in Malaysian ATMs. International Business Management 10, ss. 3607–3610.
[21] Dubey P. oraz Kanumuri T. 2015. Optimal Local Direction Binary pattern based palmprint recognition [W:] International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, ss. 1979–1984.
[22] Dubey P. et al. 2018. Sequency codes for palmprint recognition. Signal, Image and Video Processing 12(4), ss. 677–684.
[23] El-Abed M. et al. 2012. Evaluation of Biometric Systems. [W:] New Trends and Developments in Biometrics, InTech, ss. 149–169.
[24] El-Badawy O. oraz Kamel M. 2002. Shape-based image retrieval applied to trademark images. International Journal of Image and Graphics 2(3), ss. 375–393.
[25] El-Tarhouni W. et al. 2016. Multispectral palmprint recognition based on local binary pattern histogram fourier features and gabor filter. [W:] 6th European Workshop on Visual Information Processing (EUVIP), IEEE, ss. 1–6.
[26] Fang L. 2015. Mobile based palmprint recognition system. [W:] International Conference on Control, Automation and Robotics, IEEE, ss. 233–237.
[27] Funada J. et al. 1998. Feature extraction method for palmprint considering elimination of creases. [W:] International Conference on Pattern Recognition, IEEE, ss. 1849–1854.
[28] Genovese A. et al. 2014. Touchless palmprint recognition system, Springer Cham.
[29] Genovese A. et al. 2019. PalmNet: Gabor-PCA convolutional networks for touchless palmprint recognition. IEEE Transactions on Information Forensics and Security, 14(12), ss. 3160–3174.
[30] Grzeszyk Cz. 1993. Kryminalistyczne badania śladów linii papilarnych, Wydawnictwo Centrum Szkolenia Policji Legionowo.
[31] Haralick R.M. et al. 1973. Textural features for image classification. IEEE Transactions on systems, man, and cybernetics 6, ss. 610–621.
[32] Imtiaz H. oraz Fattah S.A. 2013. A histogram-based dominant wavelet domain feature selection algorithm for palm-print recognition. Computers & Electrical Engineering 39(4), ss. 1114–1128.
[33] Imtiaz H. oraz Fattah S.A. 2013. A wavelet-based dominant feature selection algorithm for palm-print recognition. Digital Signal Processing 23(1), ss. 244–258.
[34] International Civil Aviation Organization, DOC 9303: Machine readable travel documents, `https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf`, [dostęp: 2018-12-10].
[35] Ito K. oraz Aoki T. 2018. Recent advances in biometric recognition. ITE Transactions on Media Technology and Applications 6(1), ss. 64–80.

[36] Jaafar H. et al. 2015. A Robust and Fast Computation Touchless Palm Print Recognition System Using LHEAT and the IFkNCN Classifier. Computational intelligence and neuroscience, ss. 1–17.
[37] Jadhav S.B. et al. 2016. A Low-Cost Contactless Palm Print Device to Recognize Person based on Texture Measurement. International Journal of Engineering, Technology, Science and Research 3(2), ss. 1–7.
[38] Jain A. et al. 2000. Biometric identification. Communications of the ACM, 43(2), ss. 90–98.
[39] Jain A.K. 2004. Biometric recognition: how do I know who you are? [W:] Signal Processing and Communications Applications Conference, IEEE, ss. 3–5.
[40] Jain A.K. et al. 2016. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters 79, ss. 80–105.
[41] Javidnia H. et al. 2016. Palmprint as a smartphone biometric. [W:] International Conference on Consumer Electronics (ICCE). IEEE, ss. 463–466.
[42] Jia W. et al. 2017. Palmprint recognition based on complete direction representation. IEEE Transactions on Image Processing 26(9), ss. 4483–4498.
[43] Kim J.S. et al. 2015. An empirical study of palmprint recognition for mobile phones. IEEE Transactions on Consumer Electronics 61(3), ss. 311–319.
[44] Kong W.K. oraz Zhang D. 2002. Palmprint texture analysis based on low-resolution images for personal authentication. [W:] International Conference on Pattern Recognition, IEEE, ss. 807–810.
[45] Kozik R. oraz Choraś M. 2010. Combined shape and texture information for palmprint biometrics. Journal of Information Assurance and Security 5, ss. 58–63.
[46] Kumar A. 2018. Toward more accurate matching of contactless palmprint images under less constrained environments. IEEE Transactions on Information Forensics and Security, 14(1), ss. 34–47.
[47] Kumar A. oraz Zhang D. 2006. Personal recognition using hand shape and texture. IEEE Transactions on image processing 15(8), ss. 2454–2461.
[48] Laws K. I. 1980. Rapid texture identification. Image processing for missile guidance 238, ss. 376–381.
[49] Lei S. oraz Qi M. 2016. Multimodal recognition method based on ear and profile face feature fusion. International Journal of Signal Processing, Image Processing and Pattern Recognition 9(1), ss. 33–42.
[50] Liu Y. oraz Kumar A. 2020. Contactless Palmprint Identification using Deeply Learned Residual Features. IEEE Transactions on Biometrics, Behavior and Identity Science.
[51] Leng L. et al. 2018. Palmprint recognition system on mobile devices with double-line-single-point assistance. Personal and Ubiquitous Computing, 22(1), ss. 93–104.
[52] Matkowski W. M. et al. 2020. Palmprint Recognition in Uncontrolled and Uncooperative Environment. IEEE Transactions on Information Forensics and Security.
[53] Moco N. F. et al. 2014. Smartphone-based palmprint recognition system. [W:] 21st International Conference on Telecommunications (ICT), IEEE, ss. 457–461.
[54] Mokni R. oraz Kherallah M. 2016. Novel palmprint biometric system combining several fractal methods for texture information extraction. [W:] International Conference on Systems, Man, and Cybernetics (SMC), IEEE, ss. 2267–2272.

[55] Mokni R. et al. 2017. Fusing multi-techniques based on LDA-CCA and their application in palmprint identification system. [W:] International Conference on Computer Systems and Applications (AICCSA), IEEE, ss. 350–357.
[56] Mokni R. et al. 2017. Multiset Canonical Correlation Analysis: Texture Feature Level Fusion of Multiple Descriptors for Intra-modal Palmprint Biometric Recognition [W:] Pacific-Rim Symposium on Image and Video Technology, Springer, ss. 3–16.
[57] PN:ISO/IEC 19092:2010 - Usługi finansowe. Biometria. Podstawy bezpieczeństwa [dostęp: 2019-06-02].
[58] PN:ISO/IEC 27001:2014 - Information technology – Security techniques [dostęp: 2019-02-20].
[59] ITU: statystyki, `https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx` [dostęp: 27-02-2017].
[60] Ray R.B. oraz Misra R. 2015. Palm print recognition using hough transforms. [W:] International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, ss. 422–425.
[61] Ross A. oraz Jain A.K. 2004. Multimodal biometrics: An overview. [W:] European Signal Processing Conference, IEEE, ss. 1221–1224.
[62] Sanchez-Reillo R. et al. 2019. How to implement EU data protection regulation for R&D in biometrics. Elsevier Computer Standards & Interfaces 61, ss. 89–96.
[63] Sequeira A.F. et al. 2014. Mobbio: a multimodal database captured with a portable handheld device. [W:] International Conference on Computer Vision Theory and Applications (VISAPP), IEEE, ss. 133–139.
[64] Shao H. et al. 2019. Efficient deep palmprint recognition via distilled hashing coding. [W:] Conference on Computer Vision and Pattern Recognition Workshops (CVPR), IEEE.
[65] Shu W. oraz Zhang D. 1998. Palmprint verification: an implementation of biometric technology [W:] International Conference on Pattern Recognition, IEEE, ss. 219–221.
[66] Tabejamaat M. oraz Mousavi A. 2018. Generalized Gabor filters for palmprint recognition. Pattern Analysis and Applications 21(1), ss. 261–275.
[67] Taouche C. et al. 2014. Multimodal biometric systems. [W:] International Conference on Multimedia Computing and Systems (ICMCS), IEEE, ss. 301–308.
[68] Tarawneh A. S. et al. 2018. Pilot comparative study of different deep features for palmprint identification in low-quality images,arXiv:1804.04602. [dostęp: 19-12-2019].
[69] Teixeira R.F.S. oraz Leite N.J. 2017. A New Framework for Quality Assessment of High-Resolution Fingerprint Images. IEEE transactions on pattern analysis and machine intelligence 39(10), ss. 1905–1917.
[70] Tiwari K.et al. 2016. A palmprint based recognition system for smartphone. [W:] Future Technologies Conference (FTC), IEEE, ss. 577–586.
[71] UE: Rozporządzenie Parlamentu Europejskiego 2016/679 o ochronie danych osobowych RODO z dn. 27 kwietnia 2106 roku [dostęp: 2019-02-12].
[72] Unar J.A. et al. 2014. A review of biometric tech-nology along with trends and prospects. Pattern Recognition 47(8), ss. 2673–2688.

[73] Ungureanu A. oraz Costache C. 2016. Palm print as a smartphone biometric: Another option for digital privacy and security. IEEE Consumer Electronics Magazine 5(3), ss. 71–78.
[74] Ungureanu A. S.et al. 2020. Towards Unconstrained Palmprint Recognition on Consumer Devices: a Literature Review. arXiv:2003.00737, [dostęp: 09-03-2020].
[75] Ungureanu A. S. et al. 2017. Unconstrained palmprint as a smartphone biometric. IEEE Transactions on Consumer Electronics 63(3), ss. 334–342.
[76] Verma S. B. oraz Chandran S. 2016. Analysis of SIFT and SURF feature extraction in palmprint verification system. [W:] International Conference on Computing, Communication and Control Technology (IC4T), ss. 27–30.
[77] Verma S. oraz Chandran S. 2019. Contactless Palmprint Verification System using 2-D Gabor Filter and Principal Component Analysis. International Arab Journal of Information Technology 16(1), ss. 23–29.
[78] Viola P. oraz Jones M. 2001. Rapid object detection using a boosted cascade of simple features. [W:] Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, ss. 1–5.
[79] Wen J. J. et al. 2013. A palmprint recognition method based on multi-step representation, Optik 124, ss. 5727–5731.
[80] Wenxin L. et al. 2005. Texture-based palmprint retrieval using a layered search scheme for personal identification. IEEE Transactions on Multimedia 7(5), ss. 891–898.
[81] Xia Z. et al. 2017. Rotation-invariant Weber pattern and Gabor feature for fingerprint liveness detection. Multimedia Tools and Applications, ss. 1–14.
[82] Xu Y. et al. 2013. A sparse representation method of bimodal biometrics and palmprint recognition experiments. Neurocomputing 103 (2013). ss. 164—171 .
[83] Younesi A. oraz Amirani M. C. 2017. Gabor filter and texture based features for palmprint recognition. Procedia Computer Science 108, ss. 2488–2495.
[84] Zhang D. et al. 2003. Online palmprint identification. IEEE Transactions on pattern analysis and machine intelligence 25(9), ss. 1041–1050.
[85] Zhang K. et al. 2017. An optimized palmprint recognition approach based on image sharpness. Pattern Recognition Letters 85, ss. 65–71.
[86] Zhang L. et al. 2018. Palmprint and palmvein recognition based on DCNN and a new large-scale contactless palmvein dataset. Symmetry 10(4), ss. 7–8.
[87] Zhang, Y. et al. 2019. Pay By Showing Your Palm: A Study of Palmprint Verification on Mobile Platforms. International Conference on Multimedia and Expo (ICME). IEEE, ss. 862–867).
[88] W. Zhao et al. 2018. Palmprint recognition using a modified competitive code with distinctive extended neighbourhood. IET Computer Vision 12(8), ss. 1151-–1162
[89] Zhao S. oraz Zhang B. 2020. Deep discriminative representation for generic palmprint recognition. Pattern Recognition 98, s. 107071.
[90] Zhong D. et al. 2019. Decade progress of palmprint recognition: A brief survey. Elsever Neurocomputing 328, ss. 16–28.

Spis rysunków

Spis tabel

Streszczenie

Rozpoznawanie osób na podstawie analizy obrazów dłoni za pomocą urządzeń mobilnych

Każdy z nas jest jednocześnie użytkownikiem wielu systemów, z które wymagają odpowiednich sposobów zabezpieczenia. Przez to użytkownicy są przeładowani ilością loginów, haseł i kodów. Z tego powodu została opracowana biometria, umożliwiająca wykorzystanie obrazu części ludzkiego ciała lub zarejestrowanego zachowania do jego identyfikacji. Z racji rosnącego zainteresowania biometrią, można ją uznać za jeden z głównych trendów rozwoju informatyki. Najczęściej wymienianymi wyzwaniami w tej dziedzinie są: ochrona próbki, kontrola żywotności, wciąż niewystarczająca skuteczność weryfikacji oraz dalszy rozwój rzadziej stosowanych i odkrywanie nowych modalności.

Niniejsza praca doktorska jest poświęcona biometrii obrazu wewnętrznej części dłoni oraz jej zastosowaniem w systemach scenariusza mobilnego. Scenariusz ten niesie ze sobą liczne ograniczenia np. ograniczone możliwości obliczeniowe urządzeń przenośnych. Jest on jednak niezwykle istotnym kierunkiem badań, szczególnie jeśli weźmie się pod uwagę dalszy rozwój urządzeń mobilnych oraz ich rosnącą dostępność wśród społeczeństwa. Nasze dłonie okazują się bardzo bogatymi w szczegóły, a zarazem w informacje częściami ludzkiego ciała. Chociaż cecha ta nie jest jeszcze szeroko wykorzystywana w życiu codziennym, jak pokazują dostępne badania naukowe, może gwarantować bardzo wysoką skuteczność weryfikacji tożsamości przy zachowaniu racjonalnego czasu działania całego systemu. Celem tej pracy było badanie i propozycja nowych metod rozpoznawania osób na podstawie analizy obrazów dłoni za pomocą urządzeń mobilnych.

W ramach pracy Autorka zaproponowała sześć oryginalnych metod identyfikacji użytkownika oraz przeprowadziła testy różnych metod przetwarzania wstępnego próbek. Przedstawiła też koncepcję nowej bazy danych, która w przyszłości mogłaby być używana podczas testów systemów mobilnego rozpoznawania osób na podstawie obrazów dłoni. Urządzeniami, na których prowadzono eksperymenty, były cztery telefony komórkowe. Osiągane wyniki były oceniane pod względem skuteczności działania oraz czasu przetwarzania.

Słowa kluczowe: *przetwarzanie obrazów, biometria, obraz dłoni, weryfikacja użytkowników, bezpieczeństwo*

Abstract

Palmprint-based human identification in a mobile scenario

Nowadays users have a multitude of IT systems at their disposal. Each of those systems requires appropriate security methods. Due to this fact users are overloaded with the number of logins, passwords and codes that they have to remember and change on their daily basis. Biometrics was introduced to overcome this problem. Biometrics can be understood as human identification using a part of the body or human behaviour. This technique has recently been growing in popularity, and it is one of the most crucial issues in computer science now. Among its most challenging problems the following can be listed: pattern protection, liveliness detection, insufficiently high accuracy of identification and the development of new biometric traits.

This thesis concerns palmprint-based user identification in the mobile scenario. Even though this scenario introduces some important limitations, like limited computation power, it is a significant research problem in the biometrics domain. Palmprints have rich structure with numerous wrinkles, ridges and minutiae. As presented in the literature, palmprints may be used in some systems providing high accuracy and efficient computation time, though they are not yet widely adapted in many daily life applications. The main objective of this work is to propose and evaluate new methods of palmprint-based user verification in the mobile scenario.

In order to meet the objective, six brand new methods of palmprint-based user authentication were introduced in this work. Additionally, tests of some pre-processing methods were conducted, and the concept of new biometric dataset was proposed. Four different smartphones were used during the research. The obtained results were evaluated both in terms of accuracy and computation time.

Keywords: *image processing, biometrics, palmprint, user verification, security*