

PIOTR A. KOWALSKI*

PROCEDURA EKSTRAKCJI CECH Z OBRAZU TWARZY
DLA POTRZEB SYSTEMU BIOMETRYCZNEGOPROCEDURE OF FEATURE EXTRACTION FROM FACE
IMAGE FOR BIOMETRICAL SYSTEM

Streszczenie

Celem niniejszego artykułu jest prezentacja kompletnej procedury ekstrakcji cech z rzeczywistego obrazu twarzy. Procedura składa się z wielu algorytmów przetwarzania obrazów, takich jak binaryzacja, erozja, filtracja, metody gradientowe oraz kaskadowego klasyfikatora Haara. Otrzymany wektor cech jest zastosowany do zagadnienia identyfikacji biometrycznej ze szczególnym uwzględnieniem problemu uwierzytelniania. Stworzony system działa w trybie on-line, przetwarzając obraz otrzymany z kamery internetowej. Poprawność zaproponowanych algorytmów została sprawdzona za pomocą stworzonej bazy danych zawierającej kilkadziesiąt osób. Testom zostały poddane zarówno obrazy otrzymane z kamery, jak również syntetycznie stworzone zdjęcia zawierające różnego rodzaju przypadki uszkodzeń. Prezentowany tu algorytm został zbadany dla przypadków zmiennego oświetlenia, zakłóceń związanych z naturalną zmianą wyglądu, obrazem obróconym, jak również komputerowo zniekształconym.

Słowa kluczowe: biometryka, uwierzytelnianie, przetwarzanie i analiza obrazów, filtracja obrazu, metody gradientowe, klasyfikator Haara, klasyfikacja, sieci neuronowe

Abstract

The aim of this paper is to present a complete procedure for extracting features from the real face picture. The procedure consists of several image processing algorithms such as binarization, erosion, filtration, gradient method and Haar-like Features algorithm. The obtained feature vector used in biometric identification with particular emphasis on the problem of authentication. A system processing the image obtained from a webcam operates in an on-line regime. The correctness of the proposed algorithm was tested using the database created with dozens of people. The tests were done from the camera images as well as artificially created images with different damage cases. The algorithm was tested for cases of various types of lighting, disturbances associated with the natural change of face appearance, the image rotation and distorted image.

Keywords: biometrics, authentication, processing and image analysis, image filtering, gradient methods, Haar-like features, classification, neural network

* Dr inż. Piotr Andrzej Kowalski, Katedra Automatyki i Technik Informatycznych, Wydział Inżynierii Elektrycznej i Komputerowej, Politechnika Krakowska oraz Instytut Badań Systemowych, Polska Akademia Nauk.

1. Wstęp

Identyfikacja biometryczna jest nową i bardzo dynamicznie rozwijającą się dziedziną nauki i techniki. Polega ona na rozpoznawaniu osób na podstawie informacji biologicznych człowieka, tzn. jego cech fizycznych (zewnętrznych, mierzonych w danej chwili) lub behawioralnych (nabytych, zmiennych w czasie). Jest to proces mający ogromne znaczenie dla szeroko pojętego bezpieczeństwa ludności oraz systemów, np. teleinformatycznych. Zadanie identyfikacji jest dla dorosłego, zdrowego człowieka czynnością naturalną i najczęściej bywa nieinwazyjne. Jednak to, co wydaje się z pozoru rzeczą łatwą, staje się dość złożonym problemem wykorzystującym zaawansowane urządzenia techniczne. Procedura ta wymaga również zaprojektowania oraz zastosowania w praktyce wielu, nierzadko skomplikowanych algorytmów. Wraz z rozwojem nauki i techniki, nastąpił znaczny wzrost wydajności obliczeniowej komputerów, co powoduje możliwość badania coraz to bardziej skomplikowanych zagadnień na komputerach zarówno osobistych (często połączonych w klastry obliczeniowe na całym świecie), jak również na dedykowanych serwerach o wysokiej wydajności numerycznej. W związku z tym, cały czas powstają nowe algorytmy, które dostępne są już nie tylko dla ludzi pracujących w instytutach badawczych, lecz również w powszechnym zastosowaniu.

Sytuacja polityczna na świecie w ostatnich latach, a w szczególności zamachy terrorystyczne w Nowym Jorku, Madrycie, Londynie, Moskwie czy na wyspie Bali wzmogły zainteresowanie metodami identyfikacji biometrycznej oraz ulepszeniem dotychczas istniejących rozwiązań. Wielu ekspertów ds. bezpieczeństwa na świecie uważa, że wielu dramatycznym wydarzeniom można było zapobiec, gdyby zastosować udoskonalone metody identyfikacji biometrycznej osób. W następstwie tych oraz wielu innych wydarzeń zaczęto zwracać coraz większą uwagę na sprawy bezpieczeństwa poszczególnych obywateli. Oczywiście stało się znalezienie oraz zastosowanie jak najlepszych metod wspomagających pracę ludzi w miejscach szczególnie narażonych na ataki terrorystyczne. Tak więc naturalnym stał się intensywny rozwój, przede wszystkim systemów pracujących w rygorze on-line, czyli przetwarzających informacje w czasie rzeczywistym.

W Polsce systemy te są obecnie wykorzystywane w niewielkim procencie, jednak można zauważyć ich zwiększone zastosowanie, np. bankomaty biometryczne czy paszporty biometryczne.

Zagadnienia identyfikacji biometrycznej są obecnie jednym z najbardziej rozwijających się działów informatyki w związku z czym w niedalekiej przyszłości należy spodziewać się dużego wzrostu jej praktycznych zastosowań w wielu dziedzinach codziennego życia.

Celem niniejszej artykułu jest pokazanie systemu realizującego zadanie ekstrakcji wybranych parametrów morfologicznych człowieka dla potrzeb identyfikacji biometrycznej. Powyższe zadanie zostanie zrealizowane na przykładzie analizy twarzy człowieka na podstawie zdjęcia otrzymanego z kamery internetowej. Fundamentalnymi składnikami omawianego systemu są baza danych przechowująca dane zgromadzonych osób oraz moduł ekstrakcji cech dla wybranej biometriki. Kluczowym zadaniem przy tworzeniu systemu jest opracowanie odpowiednich algorytmów zarówno ekstrakcji cech, jak i identyfikujących lub weryfikujących osoby, na podstawie ich charakterystycznych cech [17]. Proces tworzenia samego modułu rozpoznawania nie został szczegółowo opisany w niniejszym artykule, niemniej jednak będzie on tematem osobnego artykułu naukowego, gdyż stanowi następny etap prac nad systemem biometrycznym.

Niniejszy artykuł został podzielony na sześć rozdziałów. Pierwszy z nich obejmuje wstęp do pracy, który wprowadza w tematykę identyfikacji biometrycznej, przedstawia główny jej cel, w drugim krótko scharakteryzowano systemy biometryczne. W rozdziale trzecim szczegółowo opisano zaprojektowany system ekstrakcji cech z obrazu twarzy ludzkiej wraz z objaśnieniem budowy kolejnych jego elementów oraz szczegółowo opisano użyte metody wyszukiwania kolejnych charakterystycznych cech badanej fizjonomii. W następnej części, krótko przedstawiono bazę danych biometrycznych będącą ważnym elementem łączącym moduł ekstrakcji cech z właściwym systemem identyfikacji. W kolejnym rozdziale zaprezentowano wyniki analizy numerycznej zastosowanych algorytmów z użyciem neuronowego klasyfikatora [20]. Ostatni rozdział zawiera podsumowanie oraz omówienie kierunków dalszych badań.

2. Systemy biometryczne

System biometryczny w zależności od przyjętego algorytmu identyfikacji może realizować dwa dość odmienne rodzaje zadań. Pierwszym z nich jest proces autoryzacji, czyli pozwolenia na dostęp do określonego zasobu na podstawie pewnej przesłanki, czyli identyfikatora wskazującego wstępnie na personalia badanej osoby. Przykładem takiego postępowania jest użycie np. karty magnetycznej z zapisanymi danymi personalnymi, a następnie potwierdzenie – czyli właśnie autoryzacja – poprzez zbadanie np. odcisku papilarnego [14]. Zadanie to polega na potwierdzeniu – przez określoną biometrię – danych personalnych podanych wstępnie do systemu. Drugim znacznie trudniejszym rodzajem zadania stawianym przed systemem biometrycznym jest proces uwierzytelniania, czyli rzetelnego ustalenia tożsamości badanej osoby na podstawie stworzonego wcześniej repozytorium rozważanych osób. Oba powyższe zadania stały się w dzisiejszych czasach niezbędne w wielu codziennych czynnościach, takich jak choćby identyfikacja osób wsiadających do samolotu czy wykonywanie pewnych operacji w banku itp. Weryfikacja tożsamości stała się nie lada wyzwaniem, w przypadku gdy konieczna staje się jej automatyzacja z małym prawdopodobieństwem błędu i dużą niezawodnością systemu.

Mając do czynienia z zadaniem uwierzytelniania, można wyróżnić kilka tradycyjnych jego środków. Pierwszym z nich jest operacja uwierzytelniania przeprowadzona na pewnego rodzaju mieniu, czyli pewnych przedmiotach fizycznych, takich jak klucz, paszport czy „inteligentne” karty. Z łatwością można zauważyć, że wadą powyższych środków jest duże narażenie na niepowołaną zmianę ich właściciela zarówno w przypadku trywialnego pożyczenia powyższych przedmiotów, jak i poza wiedzą właściciela. Kolejnym środkiem jest wiedza, która stanowi – w zamyśle – informację znaną tylko odpowiedniej osobie, np. hasło, kod PIN itp. W tym przypadku znowu może zajść niekontrolowane przekazywanie informacji osobom nieuprawnionym do jej użytkowania. Powyższe może zaistnieć ponownie za wiedzą właściciela oraz bez niej, np. podglądnięcie wprowadzanego kodu. Innym dość negatywnym skutkiem stosowania tak prostego środka jest możliwość wymuszenia przekazania chronionej wiedzy poprzez element szantażu. Ostatnim środkiem stosowanym do uwierzytelniania są właśnie biometryki zawierające cechy osób pozwalające je odróżnić. Odpowiednio dobry wybór cech wiąże się z nieomal bezwzględnym brakiem możliwości zbicia ich na rzecz osób trzecich.

Identyfikacja biometryczna, inaczej biometria, polega na wykorzystaniu informacji biologicznej (cech fizjologicznych lub behawioralnych) w celu identyfikacji osoby [23]. Biometryki behawioralne opierają się na tym, jak dana czynność jest wykonywana, zmieniając się w czasie. Biometryki te ze względu na ich dużą niestacjonarność są podatne na zmiany. Biometryki fizjologiczne niosą informacje o cechach fizycznych, mierzonych w danej chwili. Są one na tyle bogate, że jedna próbka może wystarczyć do porównania kilku identyfikatorów biometrycznych, co w przypadku biometryki behawioralnej jest rzeczą w zasadzie niemożliwą. U podstaw biometryki fizjologicznej leży fakt, że ciało ludzkie posiada pewne niezmiennie własności, które różnią nas od innych osób.

Do biometryk behawioralnych zaliczyć można: analizę podpisu, analizę głosu, analizę chodu czy analizę ruchu ust [18]. Biometryki fizjologiczne zaś to m.in. rozpoznawanie odciśnięć palców, rozpoznawanie twarzy, tętno oka, analiza geometrii dłoni, analiza DNA czy zapachu.

Do uczynienia biometrii użyteczną należy wziąć pod uwagę pięć własności ją cechujących [1]. Pierwszą z nich jest uniwersalność, tzn. każda osoba powinna posiadać daną cechę. Drugą własnością jest jednoznaczność, a zatem żadne dwie instancje nie powinny być takie same, jeżeli chodzi o rozważaną fizjonomię. Bardzo ważnym, kolejnym warunkiem, który powinna spełniać biometria jest jej trwałość, a zatem rozważana cecha nie powinna być zmienna w czasie. Czwartym czynnikiem pozwalającym uznać metodę za użyteczną jest jej ściągłość. Oznacza to, że dana fizjonomia czy też zachowanie powinno być możliwe do zmierzenia. Dodatkowo badana populacja użytkowników nie powinna mieć obiekcji przeciw pomiarowi danej biometryki (akceptowalność), co stanowi ostatnią własność, która czyni omawianą metodykę użyteczną. O jej efektywności decyduje połączenie tych elementów. Nie ma jednak metody, spełniającej te wszystkie własności, ani nawet takiej, która całkowicie spełniałaby którąkolwiek z powyżej wymienionych.

Rozpoznawanie twarzy jest najbardziej naturalnym sposobem identyfikacji biometrycznej, gdyż praktycznie każdy codziennie używa go jako środka do rozpoznawania innych ludzi. Biometria ta jest z powodu swojej naturalności bardziej akceptowana niż inne. Od momentu wynalezienia fotografii zdjęcie twarzy stanowiło pewnego rodzaju gwarancję tożsamości i jest umieszczane w dowodzie osobistym czy paszporcie. Ze względu na konwencjonalność urządzeń oraz łatwość uchwycenia twarzy, powstało wiele profesjonalnych baz danych, takich jak policyjna, służb specjalnych a nawet archiwa telewizyjne [1]. Istnieją również repozytoria twarzy (np. *The Color FERET Database*) stworzone do celów badawczych, ze szczególnym uwzględnieniem możliwości porównania stworzonego algorytmu z innymi [22].

Systemy rozpoznawania twarzy pracę swą rozpoczynają od wykrycia twarzy w rozpatrywanym środowisku. Po zlokalizowaniu potencjalnej twarzy stosowane są metody należące do dwóch kategorii: geometria twarzy oraz jej wygląd [1]. Pierwsza metoda polega na modelowaniu ludzkiej twarzy z użyciem określonych punktów charakterystycznych twarzy, takich jak: oczy, usta, nos itp. [4]. W tym przypadku dużą rolę odgrywają zastosowane algorytmy rozpoznawania obrazów [19], natomiast identyfikacja twarzy jest wtedy kwestią porównania układów szczegółów, np. z użyciem algorytmów sieci neuronowych [24].

Drugi sposób rozpoznawania twarzy polega na zredukowaniu obrazu twarzy zbudowanego z kilkuset pikseli do jedynie kilku liczb. Problem polega na tym, aby ująć cechy naj-

bardziej istotne przy rozróżnieniu badanych obiektów, a pominięciu „szumu”. W tym celu obraz twarzy przedstawia się jako kombinację liniową obrazów bazowych, zwanych twarzami własnymi [1] i tak każdy obraz jest porównywany z twarzami własnymi umieszczonymi w bazie. Jest to metoda podobna do metod stosowanych w kryminalistyce, jednak jest ona w początkowej fazie rozwoju.

Pomimo wyraźnego postępu w ostatnich latach w dziedzinie rozpoznawania twarzy biometryka ta nie jest wystarczająco dokładna, aby możliwe było identyfikowanie osób w dużej populacji, z czym radzą sobie inne biometryki. Ponadto określenie tożsamości na podstawie zdjęcia napotyka czasami na pewne trudności, np. w przypadku bliźniąt jednojajowych. Ogólnie – wyzwania stojące przed sposobami rozpoznawania twarzy można podzielić na kategorie związane z odchyleniami, które należy uwzględnić [13]. Pierwszą z nich jest wygląd fizyczny, który obejmuje krótkotrwałe zmiany występujące podczas np. mrugania czy mówienia. Ponadto ważne są również zmiany spowodowane wiekiem, chorobą czy zmianą wizerunku (nałożenie makijażu, okularów, zapuszczenie wąsów czy brody itp.). Drugą kategorią odchyłeń jest geometria pozyskania. Przeważnie twarz na obrazie jest w nieznanym miejscu i nieznanym położeniu. Jeżeli jest on zwrócona w stronę obiektywu, to zmiany są niewielkie, jednak wykonywanie obrotów powoduje powstanie różnic w wyglądzie. Kolejnym rodzajem odchylenia są warunki obrazowania, gdyż oświetlenie twarzy może mieć duży wpływ na jej wygląd na zdjęciu. Ponadto wewnętrzne cechy aparatu (redukcja szumu czy równowaga bieli) mogą wpłynąć niekorzystnie na wynik rozpoznawania. Ostatnią klasą są zniekształcenia kompresji. Są to nieoczekiwane pogorszenia jakości obrazu spowodowane jego kompresją. Powszechnie stosowane metody kompresji (JPEG, MPEG) bazują na kompresji wycinków obrazu i nie są zoptymalizowane pod względem wyglądu twarzy ludzkiej. Może to znacząco wpłynąć na wydajność stosowanych algorytmów [1, 21].

O żadnym obecnie występującym systemie rozpoznawania twarzy nie można powiedzieć, że radzi sobie ze wszystkimi wyżej wymienionymi problemami. Aby uniknąć tych problemów nakłada się pewne ograniczenia na warunki wykonywania zdjęć. Jednak jeszcze przez jakiś czas systemy rozpoznawania twarzy będą wymagały znaczącej ingerencji człowieka.

3. Procedura ekstrakcji cech twarzy

Poprawna ekstrakcja cech twarzy ma decydujący wpływ na prawidłowe działanie stworzonego systemu identyfikacji twarzy. Na jakość działania tego algorytmu ma wpływ wiele czynników, m.in. szybkość sprzętu, rozdzielczość analizowanych zdjęć, obecność na twarzy obiektów typu okulary lub innych elementów, takich jak choćby zarost osoby identyfikowanej itp.

Proces ekstrakcji cech ma na celu wyznaczenie numerycznych składowych wektora przedstawiającego numeryczny opis wybranych cech twarzy. W przypadku proponowanego w niniejszym artykule systemu, procedura ekstrakcji cech składa się z następujących etapów:

Procedura ekstrakcji cech z obrazu twarzy ludzkiej**Procedura ekstrakcji cech**

1. Określenie położenia i lokalizacja twarzy na obrazie wejściowym.
2. Określenie położenie oraz rozstaw środków żrenic.
3. Poprawa orientacji twarzy na obrazie wejściowym.
4. Określenie szerokości nosa.
5. Określenie szerokości ust.
6. Określenie szerokości twarzy.
7. Wyznaczenie wartości numerycznej wektora cech.

Na podstawie wyznaczonych parametrów budowany jest wektor cech opisujący twarz, który w trybie rejestracji zapisywany jest do bazy danych, natomiast w trybie identyfikacji stanowi wejście dla algorytmu klasyfikacji [9], który realizuje proces autentykacji osoby.

3.1. Detekcja i lokalizacja twarzy

Detekcja twarzy jest pierwszym etapem działania procesu ekstrakcji cech. Celem tego etapu jest „wydobycie” z kamery wejściowej obrazu zawierającego twarz, który zostanie poddany analizie w dalszej części procesu [6].

Do wyznaczenia obszaru twarzy wykorzystany został kaskadowy klasyfikator *Haara* [12], dostępny wraz z biblioteką do przetwarzania obrazów w pakiecie *OpenCV* [2, 10]. Klasyfikatory są w stanie, za pomocą analizy kształtu, zlokalizować obiekty, jakimi zostały wytrenowane.

Działanie klasyfikatora oparte jest na metodzie *Haar-like features* [12], w której weryfikacja obrazu podzielona jest na etapy. W każdym etapie użyty jest klasyfikator wykorzystujący 4 różne techniki obliczające wagi (*Discrete Adaboost*, *Real Adaboost*, *Gentle Adaboost* i *Logitboost*), zaś podstawowym klasyfikatorem jest drzewo decyzyjne z co najmniej 2 liśmi. Na najniższym etapie decyzje podejmowane są w oparciu o tzw. cechy *Haara* (*Haar-like features*). Są to proste „maski”, które mierzą podstawowe cechy obrazu. Jest ich 14 i są podzielone na 3 grupy: rysy krawędzi, rysy linii oraz rysy środka ramki. Więcej szczegółów na ten temat można znaleźć w [12].

Obraz wejściowy jest przetwarzany (skanowany) klasyfikatorem w celu znalezienia pozycji szukanego obiektu, co więcej powyższa procedura została zaimplementowana z uwzględnieniem przypadku istnienia wykrywanych obiektów w różnych skalach. Dodatkowo zastosowana została tu technika przesuwnego okna, dzięki czemu żadna część obrazu nie jest pominięta.

Używany algorytm pozwala zlokalizować w obrazie pionowo ustawione twarze. Jest on stworzony tak, aby mógł wykryć twarz o różnych rozmiarach (w różnej odległości od obserwatora), w efekcie działania procedury *Haara* mogą być również wykryte inne obiekty, niekoniecznie twarze.

Dlatego w celu zapobiegnięcia wykrycia przez klasyfikator obiektów o innym charakterze, wprowadzono tu dodatkowe ograniczenia, tj. stosunek wysokości obrazu twarzy do wysokości całego analizowanego obrazu jest większy niż $1/3$, dodatkowo stosunek wysokości

do szerokości znalezionej obszaru jest mniejszy niż 3. Ostatnim przyjętym ograniczeniem jest założenie, że wybierany jest obraz o największej – z wyróżnionych w czasie analizy – powierzchni.

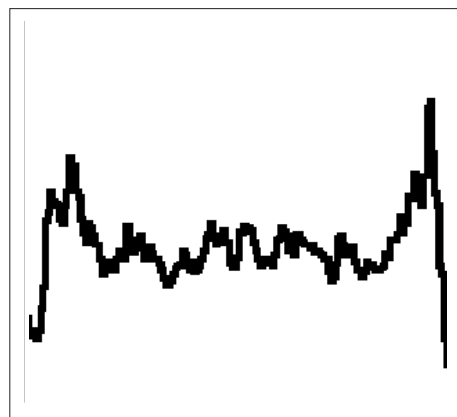
Podczas detekcji twarzy, która jest lekko pochylona bądź nierównomiernie oświetlona może wystąpić efekt przedstawiony poniżej na rys. 1, czyli zbyt duży obszar został rozpoznany jako twarz. Usterka ta może być przyczyną błędnej lokalizacji pozostałych elementów twarzy: oczu, nosa, czy ust.

Do wyznaczenia prawidłowych krawędzi twarzy zastosowano metodę projekcji wertykalnej. Na rys. 2 w miejscu krawędzi twarzy można zaobserwować znacznie większy gradient niż na pozostałej części wykresu.



Rys. 1. Wyznaczony obszar twarzy wychodzący poza jej granice

Fig. 1. The designated area of the face which goes beyond its borders



Rys. 2. Gradient pionowy dla obrazu twarzy

Fig. 2. Vertical gradient for the face image

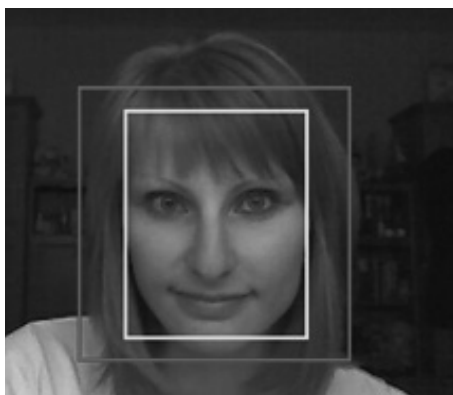
W celu poprawy lokalizacji krawędzi obrazu twarzy zaproponowany został następujący algorytm:

Algorytm 2

Procedura poprawy lokalizacji krawędzi obrazu twarzy

Procedura poprawy lokalizacji krawędzi obrazu twarzy

1. Znalezienie maksymalnego gradientu pionowego dla obszaru od lewego brzegu obrazu twarzy do 30% szerokości obrazu.
2. Znalezienie maksymalnego gradientu pionowego od 70% szerokości obrazu do prawego brzegu obrazu twarzy.
3. Zmniejszenie obrazu twarzy o wartości wyliczone w powyższych punktach odpowiednio dla lewego i prawego brzegu.
4. Zmniejszenie obrazu twarzy (od góry i od dołu) o 50% z mniejszej z wartości wyznaczonych powyżej.



Rys. 3. Obraz po poprawie krawędzi

Fig. 3. The image with the improved edge

Tak zdefiniowany obraz twarzy (rys. 3) jest podstawą do znalezienia kolejnych charakterystycznych jej elementów (tj. oczy, usta, nos) oraz reprezentujących je wartości liczbowych.

3.2. Detekcja położenia oczu

Oczy stanowią jedno z najbardziej charakterystycznych elementów cechujących twarz ludzką [16]. Błędne wskazanie ich położenia skutkuje dalszym nieprawidłowym określeniem pozostałych cech opisujących części twarzy, w tym również błędne wskazanie kąta nachylenia twarzy w rozpatrywanej płaszczyźnie XY. Zatem znalezienie prawidłowego położenia oczu jest fundamentem poprawnego działania bloku ekstrakcji cech.

Poniżej zostanie zaproponowany schemat algorytmu detekcji położenia oczu:

Algorytm 3

Procedura detekcji położenia oczu

Procedura detekcji położenia oczu

1. Wstępna lokalizacja obszaru oczu.
 2. Dla wyznaczonego w poprzednim punkcie obrazu, przeprowadzenie operacji odejmowania składowych R i B.
 3. Binaryzacja zdjęcia.
 4. Algorytm otwarcia obrazu.
 5. Wyznaczenie obrazu oczu.
 6. Wygładzenie zdjęcia.
 7. Lokalizacja pozycji środków źrenic.
-

Podstawowym zadaniem procedury wykrywania położenia oczu jest przybliżone określenie ich lokalizacji na podstawie znajomości budowy ludzkiej twarzy. W tym celu z obrazu zawierającego twarz wydzielony zostanie obraz o wymiarach: szerokości takiej, jak szerokość zdjęcia twarzy, wysokości równej 40% obrazu, umiejscowionym w 20% wyznaczonego wcześniej zarysu twarzy od góry.



Rys. 4. Obszar zawierający oczy

Fig. 4. The area containing the eyes

Z tak powstałego obrazu tworzony jest obiekt graficzny będący różnicą składowej czerwonej i niebieskiej (rys. 5 – lewy), co można opisać następującą zależnością:

$$I(x, y)_{R-B} = I(x, y)_R - I(x, y)_B \quad (1)$$

w której $I(x, y)_{R-B}$ oznacza wartość piksela w pozycji (x, y) obrazu będącego różnicą składowych czerwonej $I(x, y)_R$ i niebieskiej $I(x, y)_B$.

Następnie tak powstały obiekt jest poddany operacji binaryzacji z progiem dobieranym dynamicznie (rys. 5 – środkowy). W kolejnym etapie w celu usunięcia drobnych zakłóceń obraz jest poddawany operacji otwarcia (rys. 5 – prawy).



Rys. 5. Obraz oka będący różnicą składowych R i B (L), po binaryzacji (Ś) oraz po otwarciu (P)

Fig. 5. Image of the eye contains the difference components of R and B (left) after binarization (middle) and after opening process (right)

Z tak otrzymanego obszaru zostają wydzielone najniżej leżące rozłączne podobszary, o szerokości i wysokości większej niż 3 piksele. Spowodowane jest to uniknięciem zinter-

pretowania jako przestrzeni oczu strefy, w której występują brwi. Za przybliżony środek oczu przyjmujemy środki wydzielonych podobszarów. Za przybliżoną strefę każdego oka przyjęte zostaje pole, którego szerokość stanowi 30% szerokości obrazu twarzy oraz wysokość – 65% wyznaczonej szerokości obszaru oka (rys. 6).

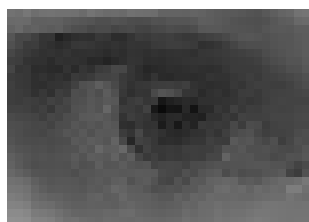


Rys. 6. Wyznaczone obszary oczu

Fig. 6. Designated areas of the eyes

Tak powstałe obszary oczu stanowią dość dobre przybliżenie położenia środka oczu, co pozwala na dalszą, bardziej precyzyjną analizę.

Bazując na dokładnie wyznaczonych obszarach oczu można przejść do dokładnego wyznaczania lokalizacji środka źrenic. W tym celu wszelkie operacje dokonywane są na wydzielonym polu oczu, a w szczególności w kanale składowej czerwonej. W kolejnym etapie algorytmu, obszar każdego oka poddany zostaje operacji wygładzenia maską 5×5 . W efekcie tego procesu powstaje poniższy obraz (rys. 7).

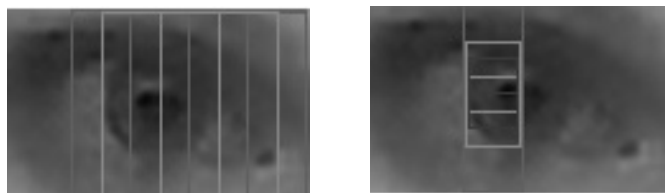


Rys. 7. Składowa czerwona (R) obrazu oka

Fig. 7. The red fraction of the eye image

Na tak powstałe projekcje zostaje nałożonych 7 okien pionowych oraz 5 okien poziomych (rys. 8), których szerokość stanowi 20% szerokości obrazu oka. Podobną proporcję przyjmuje się w stosunku do wysokości okna.

Poszczególne okna przesuwane są co 10% szerokości w kierunku środka twarzy oraz podobnie dla projekcji wertykalnej. Początkowe ustawienia okien wynoszą odpowiednio dla szerokości – 30% szerokości obrazu oka lewego, 70% szerokości oka prawego oraz dla wysokości – 30% wysokości obrazu oczu.



Rys. 8. Wyznaczanie okien pionowych (L) oraz poziomych (P)

Fig. 8. Determination of vertical windows (left) and horizontal (right)

W następnym etapie dla każdego okna obliczana jest funkcja będąca sumą jasności pikseli, odpowiednio poziomo i pionowo. Maksima tych funkcji wyznaczają położenie współrzędnej pionowej oraz poziomej środków źrenic.

3.3. Korekcja orientacji twarzy w płaszczyźnie XY

Po wyznaczeniu współrzędnych środków źrenic można określić kąt nachylenia twarzy w płaszczyźnie XY. Korekcja ta ma sens jedynie dla kątów powyżej 7° , gdyż małe kąty nachylenia twarzy najczęściej nie wpływają negatywnie na jakość procesu rozpoznawania cech biometrycznych. Natomiast kąty powyżej 27° świadczą o bardzo dużym nachyleniu, a co za tym idzie o nieprzydatności obrazu w procedurze identyfikacji.

Kąt nachylenia twarzy względem osi X wylicza się z następującej zależności:

$$\pm\varphi = a \tan \frac{y}{x} \quad (2)$$

gdzie:

- φ – kąt nachylenia twarzy względem osi X,
- x oraz y – rozstaw oczu w poziomie oraz w pionie odpowiednio.

Jeżeli prawe oko jest położone wyżej od lewego kąt φ przyjmuje znak ujemny. W przypadku gdy wyliczony kąt jest większy niż 27° powstały obraz zostaje odrzucony jako potencjalny nieprzydatny wzorec twarzy, gdyż prawdopodobnie środki źrenic zostały błędnie zinterpretowane lub nieprawidłowo wyznaczone. Wpływ na to mogą mieć różne okoliczności, takie jak zła jakość oświetlenia, użycie okularów czy posiadanie włosów przesłaniających oczy. Zupełnie inny przypadek mogą stanowić błędnie zinterpretowane brwi lub inne elementy twarzy potraktowane jako obszar oka.

Po ustaleniu kąta nachylenia twarzy następuje obrót obrazu o ustaloną wartość (2) oraz wyznaczenie macierzy transformacji, która pozwoli obliczyć współrzędne oczu w nowym układzie współrzędnych. Podczas wykonywania obrotu obrazu w płaszczyźnie XY rozmiary obrazu zwiększają się (rys. 9), w związku z powyższym należy uwzględnić ten fakt i przeskalować tak otrzymany obraz.

Kolejne etapy ekstrakcji cech będą opierały się na analizie obrazu obróconego o wcześniej obliczony kąt φ . Zatem otrzymane wyniki należy przetransformować do układu współrzędnych obrazu wejściowego.



Rys. 9. Wyznaczone środki źrenic twarzy pochylonej (L) oraz obraz obrócony (P)

Fig. 9. Designated means pupils for rotated face (left), face after rotation (right)

3.4. Wykrywanie parametrów ust

Usta, podobnie jak oczy, są bardzo charakterystyczną cechą twarzy ludzkiej. Jednak w przeciwieństwie do oczu są trudniejsze do lokalizacji. Ich kształt często ulega zmianie (np. podczas mowy, śmiechu). Dodatkowo, w przypadku posiadania zarostu usta mogą stać się niewidoczne, a co za tym idzie niemożliwa staje się ich lokalizacja. Jednak, w większości przypadków ich kolor wyraźnie odcina się od pozostałej części twarzy. Staje się to szczególnie zauważalne podczas, gdy są one otwarte.

Algorytm 4

Procedura wyznaczania parametrów ust

Procedura wyznaczania parametrów ust

1. Wyznaczenie obrazu zawierającego przybliżone położenie ust.
 2. Wyznaczenie poziomej linii ust.
 3. Wyznaczenie obrazu ust.
 4. Zastosowanie operacji erozji.
 5. Wzmocnienie kontrastu.
 6. Zastosowanie operacji otwarcia oraz binaryzacji.
 7. Usunięcie skrajnych pikseli.
 8. Wyznaczenie położenia kącików ust.
-

Przyjmując oczywisty fakt, że usta są zawsze położone poniżej linii oczu, na podstawie wyznaczonego wcześniej obrazu twarzy określany jest obszar zawierający usta, w obrębie którego będzie poszukiwana pozioma linia ust. Jest to powierzchnia, której szerokość stanowi 50% szerokości obrazu twarzy oraz wysokość wynosząca 17%, a górna jego krawędź położona zaś będzie na wysokości 75% obrazu twarzy.



Rys. 10. Wyznaczony przybliżony obszar ust

Fig. 10. The estimated area of the mouth

W celu wyznaczenia poziomej linii ust wykorzystana jest metoda projekcji horyzontalnej wykorzystująca gradient poziomy. Maksimum tej funkcji określa położenie poziomej linii ust.

Mając wyznaczoną linię ust, w kolejnym kroku wyznaczany jest obszar rozciągający się wzdłuż niej o wymiarach: szerokość – 36% szerokości obrazu twarzy oraz wysokość – 12% wysokości obrazu twarzy.

W następnym etapie, wycinek ten jest poddany operacji erozji, po czym wzmacniany jest kontrast poprzez zastosowanie następującego przekształcenia:

$$Q(x, y) = \begin{cases} \min P & \text{gdy } I(x, y) - \min P < \max P - I(x, y) \\ \max P & \text{w przeciwnym przypadku} \end{cases} \quad (3)$$

gdzie:

- $Q(x, y)$ – wartość piksela obrazu po zmianie w punkcie (x, y) ,
- $I(x, y)$ – wartość piksela obrazu w skali szarości w punkcie (x, y) ,
- $\max P$ – maksymalna wartość piksela w sąsiedztwie punktu (x, y) ,
- $\min P$ – minimalna wartość piksela w sąsiedztwie punktu (x, y) .

Sąsiedztwo punktu o współrzędnych (x, y) określa prostokąt o wymiarach 5×7 . W rezultacie powstaje obraz (rys. 11), w którym obszar ust wyraźnie odcina się od pozostałej jego części.



Rys. 11. Obszar ust po operacji erozji oraz po wzmacnieniu kontrastu

Fig. 11. The mouth area after the erosion operation and the strengthening of contrast



Rys. 12. Obszar ust po binaryzacji i otwarciu (L) oraz wyznaczone kąćki ust (P)

Fig. 12. The mouth area after binarization and opening process (left) and the designated corners of the mouth (right)

Tak powstały obraz zostaje poddany operacji binaryzacji, a następnie otwarcia oraz usunięcia skrajnych pikseli, w wyniku czego powstaje obiekt graficzny zawierający tylko usta. Dla tak powstałego obrazu wyznaczane są współrzędne lewego i prawego brzegu wyznaczonego obszaru, które są jednocześnie współrzędnymi kąćków ust (rys. 12).

Następnie tak wyznaczone współrzędne należy przetransformować do układu współrzędnych obrazu wejściowego.

3.5. Detekcja obszaru nosa

Kolejnym, charakterystycznym elementem ludzkiej twarzy jest nos, którego pewne parametry, takie jak: jego szerokość, położenie centralnego punktu czy lokalizacja otworów nosowych mogą być bardzo cenne w systemie identyfikacji. W zaproponowanym algorytmie ekstrakcji cech nos jest reprezentowany za pomocą jego szerokości. Wybór ten jest wynikiem uniezależnienia procedury od położenia otworów nosowych, które nie zawsze są widoczne, a zatem ich lokalizacja mogłaby być w pewnych przypadkach w zasadzie niemożliwa.

Algorytm 5

Procedura lokalizacji obszaru nosa

Procedura lokalizacji obszaru nosa

1. Wyznaczenie obrazu zawierającego przybliżone położenie nosa.
 2. Wyznaczenie poziomej linii nosa.
 3. Wyznaczenie obrazu nosa.
 4. Wyrównanie histogramu.
 5. Zastosowanie operacji binaryzacji.
 6. Wyznaczenie krawędzi nosa.
-

Na podstawie uprzednio wyznaczonego położenia środków źrenic oraz położenia ust, w łatwy sposób można wyznaczyć obraz zawierający nos (rys. 13). Jest to obszar o wymiarach: szerokość – 80% rozstawu oczu oraz wysokości będącej ok. 30% wysokości obrazu twarzy poniżej linii oczu.

Na podstawie tak wyznaczonego obszaru zostaje obliczona pozioma linia nozdrzy metodą projekcji horyzontalnej. Maksimum funkcji projekcji stanowi poziomą linię nosa.

Po wyznaczeniu owej linii ustalany jest nowy obraz rozciągający się wzdłuż niej, którego szerokość wynosi 90% szerokości poprzednio wyznaczonego obszaru, natomiast wysokość – 10% wysokości badanego obrazu.



Rys. 13. Wyznaczony obszar nosa

Fig. 13. The designated area of the nose

Następnie obraz ten poddawany jest filtracji obejmującej wyrównanie histogramu oraz binaryzację dla każdego punktu osobno. Nowo powstały obraz binarny obliczany jest według wzoru:

$$\text{bin}(x, y) = \begin{cases} 1 & \text{gdy } I(x, y) \leq \text{prog}(x, y) \\ 0 & \text{w przeciwnym przypadku} \end{cases} \quad (4)$$

gdzie:

- $\text{bin}(x, y)$ – wartość piksela obrazu po binaryzacji w punkcie (x, y) ,
- $I(x, y)$ – wartość piksela obrazu w skali szarości w badanym punkcie,
- $\text{prog}(x, y)$ – wartość progu binaryzacji w danym punkcie.

Próg ten dla każdego punktu obliczany jest oddzielnie, a jego wartość zależy od wartości sumy pikseli obrazu w skali szarości na danym obszarze (w rozważanym przypadku 7×7) o środku w punkcie (x, y) . Wylicza się go według następującej formuły:

$$\text{prog}(x, y) = b \cdot \text{sr}(x, y) \quad (5)$$

$$\text{sr}(x, y) = \frac{\sum_{i=x-3}^{x+3} \sum_{j=y-3}^{y+3} I(i, j)}{\text{wys} \cdot \text{szer}} \quad (6)$$

gdzie:

- b – współczynnik binaryzacji dobrany doświadczalnie,
- wys, szer – wysokość i szerokość obszaru o środku w punkcie (x, y) ,
- $\text{sr}(x, y)$ – średnia wartość w skali szarości na obszarze o środku w punkcie (x, y) .

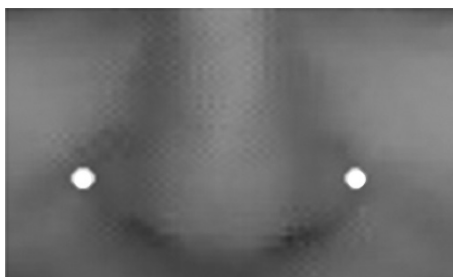


Rys. 14. Obszar nosa po binaryzacji punktowej

Fig. 14. The nose area after point binarization

Obraz powstały w wyniku binaryzacji punktowej został przedstawiony na rys. 14.

Na tak powstałym obrazie wyraźnie widoczne są krawędzie nosa, określone przez maksima funkcji będącej sumą wartości pikseli obrazu binarnego wzdłuż poziomej osi. Dzięki temu zostaje obliczona szerokość nosa, która będzie stanowić składową wektora cech.

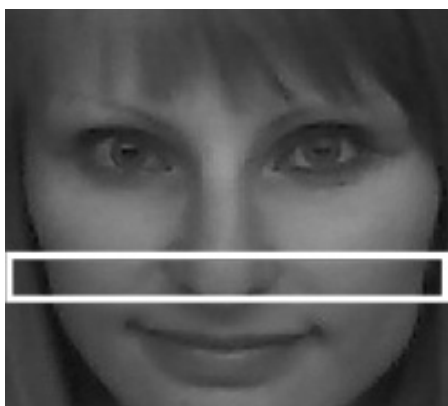


Rys. 15. Wyznaczone kąćki nosa

Fig. 15. Designated corners of the nose

3.6. Wyznaczanie parametrów konturów twarzy

Po wyznaczeniu parametrów opisujących wybrane cechy oczu, ust i nosa, w kolejnym etapie procedury należy wyznaczyć kontury twarzy. W zaproponowanym systemie będzie to szerokość twarzy na wysokości linii nozdrzy (rys. 16). Zatem zdefiniowany zostaje obszar



Rys. 16. Wyznaczony obszar zawierający krawędzie twarzy

Fig. 16. The designated area containing the edges of the face

rozcigający się symetrycznie wzdłuż linii nozdrzy zawierający nos, ograniczony krawędziami obrazu wejściowego (zgodnie z opisem w poprzedniej części).

Następnie obraz ten poddany jest operacji binaryzacji punktowej (podobnie jak w przypadku wyznaczenia krawędzi nosa) w wyniku czego powstaje nowy obraz (rys. 17), na podstawie którego wyznaczone zostaną kontury twarzy.



Rys. 17. Obszar po binaryzacji punktowej

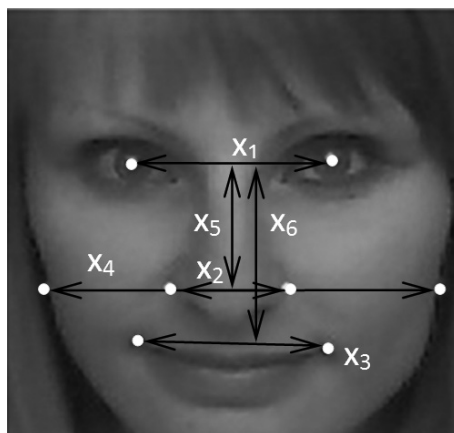
Fig. 17. The area after the point binarization operation

Na rysunku 17 można zauważyć krawędzie twarzy, określone przez maksima funkcji będącej sumą wartości pikseli obrazu binarnego wzdłuż poziomej osi. Punkty te oznaczają odpowiednio lewą i prawą krawędź twarzy na wysokości nosa.

3.7. Wektor cech

Mając wyznaczone charakterystyczne punkty twarzy, budowany jest wektor cech numerycznych opisujący twarz będącą przedmiotem rozważań. Do jego konstrukcji wykorzystane zostaną następujące cechy:

- odległość między środkami oczu – x_1 ,
- szerokość nosa – x_2 ,
- szerokość ust – x_3 ,
- szerokość twarzy – x_4 ,
- odległość między linią oczu i linią nosa – x_5 ,
- odległość między linią oczu i linią ust – x_6 .



Rys. 18. Rezultat działania stworzonej procedury ekstrakcji cech

Fig. 18. The result of created feature extraction procedure

Na rysunku 18 przedstawiono rezultat działania procedury ekstrakcji cech z zaznaczonymi punktami oraz odległościami charakterystycznymi.

Ostatecznie wektor cech przyjmuje następującą postać:

$$w = [wc_1, wc_2, ..., wc_6] \quad (7)$$

a poszczególne jego składowe wyznaczane są jako:

$$wc_1 = \frac{x_1}{x_2} \quad (8)$$

$$wc_2 = \frac{x_1}{x_3} \quad (9)$$

$$wc_3 = \frac{x_2}{x_3} \quad (10)$$

$$wc_4 = \frac{x_1}{x_4} \quad (11)$$

$$wc_5 = \frac{x_1}{x_5} \quad (12)$$

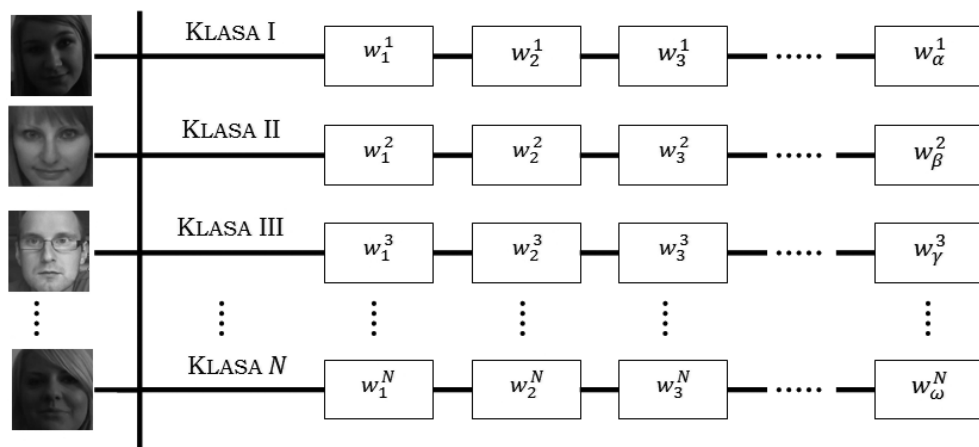
$$wc_6 = \frac{x_1}{x_6} \quad (13)$$

Powyższe składowe wektora cech są wyrażone w odniesieniu do parametru związanego z rozstawem oczu. Ma to związek z dość dobrym pomiarem tej cechy, a zatem skala niedokładności algorytmów przetwarzania obrazu (np. rotacja) zostaje w ten sposób uwzględniona. Wektor cech może również zawierać wiele innych współrzędnych uwzględniających np. brodę, wysokość głowy czy długość nosa itp. Niestety w tych przypadkach, podczas prób numerycznych, system zawierał informacje o wysokim stopniu niedokładności, a zatem mało przydatnych w kontekście omawianej metodyki. Dla wielkości niedokładnych np. przedziałowych można użyć odpowiedni dla tego typu struktur danych algorytm klasyfikacji [8]. Dodatkowym negatywnym aspektem jest powiększający się wymiar rozpatrywanego wektora cech, co znacznie zmniejsza szybkość obliczeń numerycznych i w konsekwencji oddala całą procedurę od możliwości wykonania jej w trybie on-line. Zagadnienie zwiększenia wymiarowości problemu również wiąże się z zwiększonym zapotrzebowaniem na dane uczące, a w szczególności może prowadzić do tak zwanej klątwy wielowymiarowości.

4. Baza wzorców biometrycznych

Ważnym elementem budowy każdego systemu biometrycznego jest jego baza danych, która dobrze zaprojektowana pozwala zwiększyć skuteczność jego działania. Na wzrost efektywności działania systemów ogromny wpływ ma ilość klas – odpowiadająca liczba osób – występujących w bazie danych oraz liczba zgromadzonych wzorców w obrębie każdej z rozpatrywanych klasy. Systemy biometryczne, które w ramach jednej klasy zawierają wiele wzorców cechuje znacznie większa skuteczność. Ową skuteczność można również zwiększyć, jeśli reprezentujące przedstawiony obiekt wzorce zostały zgromadzone w różnych warunkach (np. oświetleniowych).

W zaprojektowanym systemie wzorce przedstawione są jako obrazy kolorowe, różniące się datą wykonania zdjęcia (rozpiętość ok. 1 roku), rozmiarem, kątem nachylenia twarzy zarówno w poziomie, jak w pionie oraz warunkami oświetleniowymi panującymi podczas ich wykonywania. Dzięki „urozmaiceniu” wzorców system może działać ze znacznie większą efektywnością. W proponowanym systemie, w ramach pojedynczej klasy, występują dane opisujące twarz, nazwane tu wektorami cech, o wymiarze $N = 6$. Są one wynikiem detekcji charakterystycznych punktów fizjonomii twarzy opisanych w poprzednim rozdziale.



Rys. 19. Biometryczna baza wzorców

Fig. 19. Biometrical base of patterns

Na rysunku 19 została przedstawiona struktura bazy danych zaprojektowanego systemu identyfikacji biometrycznej, w którym w_j^i stanowi j -ty wzorec i -tej klasy.

5. Weryfikacja numeryczna procedury ekstrakcji cech

Głównym czynnikiem wpływającym na poprawne działania zaproponowanego tu systemu jest ekstrakcja cech obarczona możliwe jak najmniejszym błędem. Doświadczenia nu-

meryczne zostały przeprowadzone na twarzach otrzymanych z zewnętrznej kamery internetowej oraz z obrazów dostępnych w istniejących repozytoriach danych [22].

Poniżej w tabeli 1 zaprezentowane zostaną wyniki testów działania stworzonego systemu w zależności od warunków zewnętrznych panujących podczas weryfikacji procedury. Wykonane symulacje przeprowadzono dla neuronowego algorytmu identyfikacji [11] – krótko opisanego w dalszej części niniejszego artykułu. Testy zostały wykonane z użyciem bazy danych liczącej 20 osób.

Tabela 1

Wyniki testów dla różnych warunków zewnętrznych

Warunki zewnętrzne	Jakość identyfikacji z użyciem algorytmu klasyfikacji opartego na SSN propagacji wstecznej
Naturalne oświetlenie	80%
Sztuczne oświetlenie	79%
Słabe oświetlenie	67%
Mocne oświetlenie	60%

W kolejnej części zaprezentowane zostaną rezultaty działania stworzonego systemu w zależności od orientacji twarzy na obrazie wejściowym. Ten rodzaj testów przeprowadzono głównie na obrazach twarzy uzyskiwanych z kamery przy oświetleniu naturalnym, co jest spowodowane łatwością pozyskania obrazów poddawanych analizie. Weryfikację numeryczną przeprowadzono z użyciem wszystkich opisanych wcześniej algorytmów graficznych, przy bazie danych liczącej 20 osób oraz dla kątów odchylenia twarzy nie przekraczających $\pm 15^\circ$, ponieważ powyżej tej wartości pojawiały się problemy z poprawną detekcją parametrów twarzy na obrazie wejściowym.

Tabela 2

Wyniki testów dla różnych orientacji twarzy

Kąt odchylenia twarzy	Jakość identyfikacji przy użyciu alg. klasyfikacji opartego o SSN propagacji wstecznej
$\pm 5^\circ$ w pionie	78%
$\pm 10^\circ$ w pionie	76%
$\pm 15^\circ$ w pionie	62%
$\pm 5^\circ$ w poziomie	78%
$\pm 10^\circ$ w poziomie	69%
$\pm 15^\circ$ w poziomie	57%

Dodatkowo przeprowadzono odrębne badania zaproponowanego systemu w zależności od stopnia uszkodzenia obrazu wejściowego. Ten rodzaj testów przeprowadzono głównie na obrazach twarzy uzyskanych z istniejących repozytoriów twarzy. Powyższe jest związane

z łatwością komputerowego, a zatem syntetycznego, zniekształcenia takiego obrazu. Weryfikację działania zaproponowanej tu procedury dokonano w zależności od dodatkowych elementów zakłócających obraz wejściowy twarzy, takich jak okulary czy zarost. W wymienionych przypadkach algorytm często radził sobie z postawionym zadaniem, jednak przy kilku zakłóceniach obrazu szczególnie takich, jak duże zaczernianie lub zmatowienie algorytm stawał się bezradny.

W trakcie prac związanych z weryfikacją numeryczną przeprowadzono również wiele symulacji dla przykładów obejmujących zarówno różne warunki oświetlenia, jak i różną orientację twarzy. Uzyskane rezultaty w zależności od przyjętych parametrów nie zawsze dawały satysfakcjonujący rezultat. W związku z powyższym należy przyjąć, że opisany w niniejszej pracy algorytm, należy stosować wyłącznie w dobrym oświetleniu naturalnym lub sztucznym dla obrazów twarzy zbliżonych do typu *en face*.

Z uzyskanych wyników zauważyć można, iż sieć nauczona algorytmem wstecznej propagacji błędu (wraz z różnymi jego wariantami), charakteryzuje się dobrą skutecznością rozpoznania osób. Najlepsze efekty otrzymane zostały w przypadku topologii 2 warstw ukrytych oraz sumie liczby neuronów w tych warstwach zbliżonych lub równych do liczby osób w bazie danych, w stosunku 3:2 odpowiednio w każdej z rozpatrywanych warstw. Również bardzo korzystne wyniki działania aplikacji otrzymano dla początkowego współczynnika szybkości uczenia równego 0,5. Wadą tego algorytmu trenowania sieci jest dość duży czas potrzebny na naukę sieci, który w porównaniu z innymi algorytmami (takimi jak klasyfikator Bayesa [9], k-NN [5] czy PNN [15]) jest większy. Szczególnie ma to znaczenie przy dużej liczbie osób znajdujących się w biometrycznej bazie danych.

Biorąc pod uwagę wpływ warunków oświetleniowych na jakość rozpoznawania osób, należy uwzględnić wpływ tych czynników na poprawną ekstrakcję cech, gdyż nie mają one już bezpośrednio wpływu na sam proces klasyfikacji dedykowany rozpoznawaniu osób. Główną tego przyczyną jest fakt, że sieć neuronowa czy inny klasyfikator użyty do tego zadania bazuje tylko na pobranym wcześniej wektorze cech, a nie jest w stanie ocenić warunków zewnętrznych panujących podczas procesu identyfikacji biometrycznej. Podobnie jest w przypadku zaistnienia elementów zakłócających obraz czy podczas jego uszkodzenia. Jeżeli poprawnie została przeprowadzona ekstrakcja cech, na prawidłowe rozpoznanie osoby nie ma wpływu żaden zewnętrzny czynnik tylko użyty algorytm rozpoznania rozważanej biometrii.

Przy wystąpieniu naturalnego bądź sztucznego oświetlenia rezultaty identyfikacji są podobne. Gorzej wygląda sytuacja, gdy obserwowane jest sztuczne wzmocnienie lub osłabienie oświetlenia. Zwiększenie jasności obrazu powoduje zanikanie widoczności konturów oraz rysów twarzy, natomiast zmniejszenie jasności – zmniejszenie widoczności rysów twarzy, takich jak linia nosa czy linia oczu, co uniemożliwia w tych przypadkach poprawną ekstrakcję cech, a w konsekwencji satysfakcjonującą jakość identyfikacji. Jednak pomimo tych problemów, stworzony system radzi sobie również w takich warunkach z akceptowalną jakością klasyfikacji. Trudno wyobrazić sobie algorytm rozpoznawania twarzy działający ze znikomym błędem w całkowitej ciemności lub przy bardzo mocnym oświetleniu, gdyż wymagany jest tutaj sprzęt wysokiej klasy, wykorzystujący rejestrację fal o innej częstotliwości niż światło widzialne.

Zmiana orientacji twarzy o około 5–10 stopni w pionie i w poziomie nie ma niemal żadnego wpływu na poprawne działania systemu. Jeżeli twarz zostanie obrócona ponad 10 stopni w poziomie pojawia się problem zasłonięcia krawędzi twarzy, co uniemożliwia poprawne stworzenie wektora cech, ponieważ nie występuje jedna z wielkości ją charakteryzujących.

Zmiana orientacji twarzy w pionie powyżej 10 stopni nie ma wielkiego wpływu na jakość rozpoznawania. Problem pojawia się, gdy twarz na obrazie wejściowym zostanie skierowana ponad 15 stopni w dół. Następuje wtedy zasłonięcie oczu, co całkowicie uniemożliwia poprawną ekstrakcję cech. Ustalenie położenia oczu jest sprawą kluczową dla procesu identyfikacji. Jeżeli twarz obrazu wejściowego zostanie obrócona o ponad 25–30 stopni w każdą stronę, poprawna identyfikacja staje się wręcz niemożliwa ze względu na brak możliwości wyznaczenia co najmniej kilku z niezbędnych elementów składowych wektora cech.

Podczas numerycznej weryfikacji zostało stwierdzone, że elementy zakłócające obraz, takie jak okulary, zarost nie mają wpływu na jakość rozpoznawania. Problem pojawia się w przypadku wystąpienia zarostu zasłaniającego całkowicie usta czy okularów, które całkowicie zasłaniają oczy, np. przeciwsłonecznych. W owych przypadkach rozpoznanie osoby staje się również niemożliwe.

Podczas analizy zaburzonego obrazu wejściowego, jeżeli uszkodzone nie zostały rysy twarzy w newralgicznych jej punktach, proces identyfikacji przebiega jakby takiego mankamentu nie było. Problem pojawia się podczas takiej deformacji obrazu, która zakryje, bądź wyeliminuje widoczność którejs z charakterystycznych cech twarzy, podobnie jak ma to miejsce przy elementach zakłócających (tj. okulary, zarost).

Dodatkowym czynnikiem mającym wpływ na prawidłowe rozpoznawanie osób jest liczba zdjęć za pomocą, których reprezentowana jest dana osoba. Najlepsze wyniki, co jest oczywiste, uzyskuje się dla równej liczby zdjęć dla każdej rozpatrywanych w bazie klas. W przypadku dużej różnicy liczności zdjęć mogą wystąpić duże błędy procesu identyfikacji, szczególnie gdy klasyfikator nie uwzględnia tego faktu. Podczas użycia procedur korzystających z metodologii sztucznych sieci neuronowych należy zwrócić uwagę na rozsądną liczbę wzorców, gdyż znaczna ich liczność powoduje spore wydłużenie procesu uczenia, nie zawsze idące w parze ze zwiększeniem dokładności systemu identyfikacji biometrycznej.

6. Podsumowanie

Komputerowe rozpoznawanie osób na podstawie obrazu ich twarzy pomimo coraz szybszego rozwoju techniki nie zawsze osiąga zadowalającą efektywność. Głównie za pomocą obrazu twarzy rozpoznajemy codziennie otaczające nas osoby. Zrealizowanie automatycznego systemu identyfikacji biometrycznej, rozpoznającego ludzi na podstawie tego typu reprezentacji jest zadaniem relatywnie bardzo trudnym. Główną zaletą takiego systemu jest możliwość zastosowania go bez ingerencji ze strony użytkownika, choć ciągle wymagane jest zatrzymanie się przed obiektywem kamery, aby w pełni móc zbadać jej charakterystyczne cechy.

W niniejszym artykule opisano proces syntezy takiego systemu. Praca rozpoczyna się od wprowadzenia do zagadnienia identyfikacji biometrycznej, gdzie przedstawione i opisane zostały podstawowe elementy procedury rozpoznawania, omówione zostały kolejne etapy automatycznej identyfikacji oraz podstawowe zagadnienia komputerowego przetwarzania obrazu. Algorytmy ekstrakcji cech i identyfikacji biometrycznej wybierano, przyjmując za kryterium jakość i efektywność ich działania oraz łatwość komputerowej implementacji – szczególnie w trybie pracy on-line. Zostały one szczegółowo przedstawione w niniejszym artykule, a otrzymane wyniki potwierdziły skuteczność ich zastosowania. Stworzony system został

oparty na rejestracji obrazu pochodzącego zarówno z plików graficznych, jak i z zewnętrznej kamery internetowej. Dokładność wyznaczenia poszczególnych charakterystycznych cech twarzy nie jest ograniczona rozdzielczością kamery [3] czy analizowanych zdjęć, ponieważ obrazy wejściowe poddawane są transformacji do rozdzielczości 640×480 . Zaletą zaproponowanego tu systemu w postaci aplikacji komputerowej jest jej w pełni automatyczne działanie. Procedura sama dobiera wszelkie parametry niezbędne do prawidłowego działania systemu, nie wymagając przy tym od użytkownika specjalistycznej wiedzy. Wspomniane tu parametry zostały ustalone przez autora pracy, w trakcie badań empirycznych odbywających się podczas implementacji poszczególnych algorytmów przetwarzania obrazu.

Do poprawnego wyznaczenia wektora cech reprezentującego daną osobę niezbędna jest prawidłowo wyznaczona pozycja twarzy. Dzięki zastosowaniu klasyfikatora kaskadowego możliwe jest określenie pozycji twarzy na obrazie wejściowym w każdych warunkach, a błędy pojawiające się na tym etapie najczęściej mają związek z całkowicie niewidoczną twarzą bądź występowaniem na obrazie wejściowym elementów bardzo podobnych do ludzkiej twarzy, pojawieniem się na nim kilku osób jednocześnie czy przede wszystkim z błędnym określeniem ramki twarzy po przez jej owal, co spowodowane jest odstępstwem od standardowych proporcji twarzy. Do wyznaczenia pozycji oczu, ust oraz nosa zastosowano metodę projekcji horyzontalnej obrazu gradientowego twarzy oraz wykorzystano – niewymagające dużego nakładu obliczeniowego – algorytmy przetwarzania obrazów [19]. Analizując wiedzę na temat tego, co dany obraz powinien zawierać i gdzie powinien się znajdować kluczowy jego element, bardzo łatwo uzyskać z niego niezbędną ilość potrzebnych informacji, przez co otrzymane wyniki wykrywania cech twarzy są w dużej mierze zadowalające. W celu wyznaczenia szerokości twarzy korzystano z operacji binaryzacji punktowej obrazu powstałego na podstawie wyznaczonych wcześniej punktów twarzy. Występujące na tym etapie błędy związane są przede wszystkim z jakością pozyskiwanych z kamery obrazów, warunków oświetleniowych lub dodatkowych elementów zakłócających obraz twarzy (okulary, broda). Pomimo to wyniki przeprowadzonych testów obejmujących występowanie wszelkiego rodzaju zakłóceń potwierdziły efektywność działania wykorzystanych algorytmów.

Przedstawione w niniejszym artykule problemy, z jakimi należy się zmierzyć podczas procesu analizy ludzkiej twarzy, dowodzą, że bardzo trudno jest stworzyć system bezbłędnie działający. Już od pewnego czasu temat ten jest przedmiotem badań instytucji zajmujących się sprawami bezpieczeństwa w czasie rzeczywistym, gdyż twarz jest niewrażliwym elementem identyfikacji osób nagranych przez kamery i często zachodzi konieczność weryfikacji takich osób przed opuszczeniem danego miejsca.

Stworzony system jest przedstawieniem możliwości wykorzystania metod biometrycznych. Możliwości jego rozwoju to przede wszystkim eliminacja występujących dotychczas błędów oraz próby rozsądnego zwiększenia liczby punktów charakterystycznych twarzy, a co za tym idzie wektora cech, np. o położenie brwi, kształt owalu twarzy, odległość między kącikami oczu, czy dokładny kształt ust. Dalsze prace związane będą z zastosowaniem innych metod neuronowej klasyfikacji, w szczególności dotyczyć to będzie rozmytych sieci neuronowych [8]. Równolegle prowadzone są prace związane z aplikacją procedury klasyfikacji informacji niedokładnej typu przedziałowego dla problemu identyfikacji biometrycznej [7, 9].

Niniejszym chciałbym podziękować Panu Arturowi Gierlachowi za pomoc przy implementacji opisanych powyżej metod podczas pisania pracy dyplomowej.

Badania prezentowane tutaj są współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, projekt „Technologie informacyjne: badania i ich interdyscyplinarne zastosowania”.

- [1] Bolle R.M., Connel J.H., Pankanti S., Ratha N.K., Senior A.W., *Biometria*, WNT, Warszawa 2008.
- [2] Bradski G., Kaehler A., *Learning OpenCV. Computer Vision with the OpenCV Library*, O'Reilly Media, Sebastopol 2008.
- [3] Chau M., Betke M., *Real Time Eye Tracking and Blink Detection with USB Cameras*, Boston University, Boston 2005.
- [4] Chiang W.K., Tai W.K., Yang M.T., Huang Y.T., Huang C.J., *A Novel Method for Detecting Lips, Eyes and Faces in Real Time*, *Real-Time Imaging*, vol. 9(4), 2003, 277-287.
- [5] Hall P., Park B.U., Samworth R.J., *Choice of neighbor order in nearest-neighbor classification*, *Annals of Statistics*, vol. 36(5), 2008, 2135-2152.
- [6] Hsu R.L., Abdel-Mottaleb M., Jain A., *Face Detection in Color Images*, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24(5), 2002, 696-706.
- [7] Kowalski P.A., Kulczycki P., *Data Sample Reduction for Classification of Interval Information using Neural Network Sensitivity Analysis*, *Lecture Notes in Artificial Intelligence*, vol. 6304, 2010, 271-272.
- [8] Kowalski P.A., *Zastosowanie wybranych algorytmów obliczeń naturalnych w procesie uczenia sieci neuronowych typu Fuzzy Flip Flop*, *Proceedings of The First International Conference on Automatic Control and Information Technology*, 2011, 1-4.
- [9] Kulczucki P., Kowalski P.A., *Bayes classification of imprecise information of interval type*, *Control and Cybernetics*, vol. 40(1), 2011, 101-123.
- [10] OpenCV Library, <http://opencv.willowgarage.com> (dostęp 30.06.2012).
- [11] Osowski S., *Sieci neuronowe w ujęciu algorytmicznym*, WNT, Warszawa 1996.
- [12] Lienhart R., *An extended set of Haar-like features for rapid object detection*, *Proceedings of The International Conference on Image Processing*, vol. 1, 2002, I-903.
- [13] Peng K., Chen L., Ruan S., Kuchariew G., *A Robust Algorithm for Eye Detection on Gray Intensity Face without Spectacles*, *Journal of Computer Science and Technology*, vol. 5(3), 2005, 127-132.
- [14] Ratha N., Bolle R., Pandit V., Vaish V., *Robust Fingerprint Authentication Using Local Structural Similarity*, *Proceedings of the International Conference on Advances in Biometrics*, 2006, 273-279.
- [15] Rutkowski L., *Metody i techniki sztucznej inteligencji*, Wydawnictwo Naukowe PWN, Warszawa, 2006.
- [16] Shafi M., Chung P.W.H., *A Hybrid Method for Eyes Detection in Facial Images*, *International Journal of Electrical and Electronics Engineering*, vol. 3(4), 2009, 231-236.
- [17] Ślot K., *Wybrane zagadnienia biometrii*, WKiŁ, Warszawa 2008.
- [18] Tadeusiewicz R., *Sygnal mowy*, WKiŁ, Warszawa 1988.
- [19] Tadeusiewicz R., Flasiński M., *Rozpoznawanie obrazów*, PWN, Warszawa 1991.
- [20] Tadeusiewicz R., *Sieci neuronowe*, Akademicka Oficyna Wydawnicza RM, Warszawa 1993.

- [21] Tadeusiewicz R., Korohoda P., *Komputerowa analiza i przetwarzanie obrazów*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1997.
- [22] The FERET Database, www.nist.gov/itl/iad/ig/colorferet.cfm/ (dostęp 30.06.2012).
- [23] Wayman J., Jain A., Davide M., Maio D., *Biometric Systems*, Springer-Verlag, Londyn 2005.
- [24] Żurada J., Barski M., Jędruch W., *Sztuczne Sieci Neuronowe. Podstawy teorii i zastosowania*, PWN, Warszawa 1996.