POLITECHNIKA WARSZAWSKA

WYDZIAŁ ELEKTRONIKI I TECHNIK INFORMACYJNYCH

Rozprawa doktorska

mgr Kamila Bogna Matela

Big data w systemach rozpoznania wojskowego

Promotor

dr hab. inż. Andrzej STACHURSKI, PW

WARSZAWA 2023

Streszczenie pracy

Odpowiedni system wspomagania decyzji, dostosowany do wymogów pola walki winien być opracowany we współpracy z przyszłymi jego użytkownikami – i to nie tylko w zakresie interfejsu użytkownika, lecz także wszystkich innych jego modułów. Dlatego też specjalizowane, przetestowane systemy wspomagania decyzji dla niektórych zastosowań są niezwykle istotne [1].

Punktem wyjścia do opracowania takiego systemu są wyniki analizy przedstawione w pierwszym rozdziale, dotyczące kluczowych zagadnień z zakresu big data, widzenia komputerowego (ang. *computer vision*) oraz algorytmów klasyfikacji. Z uwagi na fakt, że dane wizualne stanowią największą część globalnego obiegu informacyjnego, praca koncentruje się na algorytmach analizy obrazu, która jednocześnie stanowi istotną część obszaru rozpoznania wojskowego.

W rozdziale drugim przedstawione zostały strategie aktywnego uczenia się (ang. *active learning*) w ramach uczenia maszynowego (ang. *machine learing*), w tym opisana została metoda MCADL (*Multi-criteria active deep learning for image classification*) będąca dorobkiem naukowców z Uniwersytetów *Hunan* i *Shandong*, którzy deklarują, iż jako pierwsi na świecie opracowali metodę wielokryterialnego doboru próbek do treningu [2]. Zaprezentowano korzyści wynikające z wyboru tej metody, jako podstawy do dalszych prac, w tym do zmiany algorytmu i dokonania jego optymalizacji. Rozdział drugi zawiera również analizę możliwości zastosowania sieci neuronowych, charakterystykę najsłynniejszych sieci oraz szczegółowy opis zastosowanych oryginalnie architektur, które w ramach niniejszej pracy zostały zmienione i przystosowane do rozwiązywanych problemów.

W rozdziale trzecim przedstawiono najważniejsze aspekty analizy wielokryterialnej związane z realizacją prac w obszarze klasyfikacji obrazów. Opisano w szczególności sposób implementacji analizy wielokryterialnej bazującej na metodzie punktu odniesienia, oraz zakres interaktywnego wyznaczenia rozwiązań efektywnych w algorytmie i powstałe w ich wyniku nowe rozwiązanie. W celu wykazania skuteczności przyjętego sposobu optymalizacji dodatkowo, została zaimplementowana metoda, którą zintegrowano z wypracowanym rozwiązaniem i dzięki temu osiągnięto rezultaty.

W rozdziale czwartym opisano przebieg eksperymentów zrealizowanych dla osiągnięcia założonych celów pracy doktorskiej. Przedstawiono charakterystykę obszaru wdrożenia - rozpoznania wojskowego. Z uwagi na zastosowaną przez autorów MCADL

implementację w technologii *Tensorflow*, która statystycznie zaczyna ustępować nowocześniejszemu framework'owi *Pytorch* [3], w docelowej implementacji metody MCADL wykorzystano własny kod, opracowany w technologii *Pytorch*, w oparciu o bazę danych MNIST[1] (ang. *Modified National Institute of Standards and Technology*). Mając to na względzie szczególną uwagę zwrócono na eksperymenty przeprowadzone na bazie CIFAR-10 (ang. *Canadian Institute For Advanced Research*), która ze względu na swą różnorodność może być traktowana analogicznie do zbiorów tworzonych w ośrodkach zobrazowania.

Tryb aktywnego uczenia (ang. *active learning)* wzmacnia efekt wykorzystania zbiorów, w których występują braki danych, gdyż zakłada uczenie się modelu na ograniczonej puli etykiet. Ponadto w rozdziale czwartym zaprezentowano wnioski z poczynionych obserwacji wraz z porównaniem z opracowanymi i zaimplementowanymi metodami dokonującymi klasyfikacji obiektów na obrazie.

Wnioski zawierają podsumowanie przyjętych założeń i uzyskanych efektów dla opisanej w niniejszej rozprawie nowej metody klasyfikacji obiektów na obrazie.

[1] MNIST (ang. *Modified National Institute of Standards and Technology database*) to zbiór danych zawierający cyfry pisane odręcznie, o którym w Rozdziale III.

SPIS TREŚCI

Streszczenie pracy 2

WSTĘP 6

1. Cele pracy 10
2. Teza pracy 10

ROZDZIAŁ I PRZEGLĄD STANU WIEDZY Z OBSZARU BIG DATA, WIDZENIA KOMPUTEROWEGO I ALGORYTMÓW KLASYFIKACJI 11

1. Od Big data do podjęcia decyzji 11
2. Widzenie komputerowe 16
3. Algorytmy klasyfikacji 19
   - 3.1. Proces klasyfikacji 19
   - 3.2. Równowaga klas 20
   - 3.3. Metryki oceny klasyfikacji 22
   - 3.3 Działanie algorytmów w procesie uczenia 24

ROZDZIAŁ II ACTIVE LEARNING W KLASYFIKACJI OBRAZU 29

1. Strategie i metody aktywnego uczenia 29
   - 1.1 Strategia niepewności 32
   - 1.2 Strategia kierowania zapytania przez komitet (ang. *Query by Committee - QBC*) 36
   - 1.3 Strategia maksymalizacji oczekiwanej zmiany modelu (ang. *Expected Model Change Maximization - EMCM*) 37
   - 1.4 Strategia oczekiwanej zmiany redukcji błędu (ang. *Expected Error Reduction*) 38
   - 1.5 Variance Reduction 40
   - 1.6 Density Weighted Methods 40
2. Wielokryterialna metoda klasyfikacji obrazu 40
3. Charakterystyka sieci neuronowej 53

ROZDZIAŁ III ANALIZA WIELOKRYTERIALNA 57

1. Adaptacyjne wyznaczanie rozwiązań efektywnych 57
   - 1.1 Algorytmy optymalizacyjne w procesie decyzyjnym 57
   - 1.2 Optymalizacja jednokryterialna 60
   - 1.3 Analiza wielokryterialna 61
2. Nowa metoda analizy wielokryterialnej 67
   - 2.1. Zastosowane zbiory danych 68
   - 2.2. Zastosowane sieci neuronowe 69
   - 2.3. Wprowadzenie nowej metody inicjalizacji i analiza koszt-efekt 72
   - 2.4. Nowa metoda klasyfikacji obrazu z punktami odniesienia 72

ROZDZIAŁ IV PRZEDSTAWIENIE WYNIKÓW PRAC I OBSZARU WDROŻENIA 89

1. Przebieg prac i ich wyniki 89

2. Rozpoznanie wojskowe 97
2.1. Rys historyczny 97
2.2. Przetwarzanie obrazu na rzecz wojskowych systemów rozpoznania 98
2.3. System rozpoznania w SZ RP 104
2.4. Wdrożenie 107
WNIOSKI 109
BIBLIOGRAFIA 112
SPIS TABEL 118
SPIS RYSUNKÓW 118

WSTĘP

Big data to angielski termin oznaczający ogromne zbiory danych, które wymagają zaawansowanych technologii oraz narzędzi analizy i przetwarzania. Funkcjonują również w obszarze rozpoznania wojskowego i w tym zakresie mogą pochodzić z różnych źródeł, takich jak:

- satelity i drony – segmenty naziemne gromadzą dane o ruchach wojsk i sprzętu, położeniu celów oraz warunkach terenowych;
- systemy wywiadowcze - przetwarzają wiele różnych źródeł informacji, takich jak dane z podsłuchów, informacje dotyczące transakcji finansowych, inwestycji, rozwoju technologicznego, naukowego i innych źródeł wywiadowczych;
- systemy sieciowe - monitorują komunikację i ruch w sieciach komputerowych i mogą dostarczać informacji o atakach cybernetycznych oraz o działaniach wrogich grup;
- systemy sensoryczne - mogą rejestrować dźwięki, obrazy i inne dane z otoczenia i przekazywać je do systemów rozpoznania.

Dzięki wykorzystaniu *big data* w systemach rozpoznania wojskowego można dokładniej analizować i interpretować informacje, co umożliwia szybsze i bardziej efektywne podejmowanie decyzji dotyczących działań wojskowych. Z uwagi na fakt, że dane wizualne stanowią największą część globalnego obiegu informacyjnego, praca koncentruje się na algorytmach analizy obrazu, która jednocześnie stanowi istotną część obszaru rozpoznania wojskowego.

Zobrazowania dostarczają informacji, które można wykorzystać do analizy i przetwarzania danych. Przykładowe zastosowania takiej analizy to:

- rozpoznawanie obiektów;
- monitorowanie zmian;
- prognozowanie zjawisk.

Jednocześnie warto mieć na uwadze, iż w ostatnich latach trudności w interpretacji obrazów pogłębia fakt, że coraz częściej na polu walki stosuje się kamuflaż i fałszywe cele. Ponadto dynamika operacji wojskowych jest coraz większa, podobnie jak liczba obiektów o krótkim czasie życia. Czynniki te wprowadzają dodatkową niepewność do procesu pracy z obrazami, a co za tym idzie, zmniejsza się niezawodność wykrywania i dokładność klasyfikacji obiektów. Eksperci widzą wyjście z tej sytuacji w poszukiwaniu nowych paradygmatów modelowania i redukcji niepewności, opracowywaniu skutecznych metod statystycznej i semantycznej fuzji danych i informacji pochodzących z różnych źródeł [4].

Współczesnym problemem w budowie systemu klasyfikacji obrazu dla potrzeb wojskowych jest posiadanie rozbudowanych zbiorów zdjęć, przygotowanych do treningu, które umożliwiłyby modelowi generalizację w stopniu pozwalającym na osiąganie dobrego poziomu predykcji. Analiza zobrazowań wymaga odpowiednich narzędzi i technologii, takich jak algorytmy uczenia się maszyn i sztucznej inteligencji, które umożliwiają automatyczną identyfikację i klasyfikację obiektów na zdjęciach. Klasyfikacja obrazów to proces przyporządkowywania etykiet lub kategorii do obrazów na podstawie ich zawartości.

Technologie klasyfikacji obrazów wykorzystują uczenie się maszyn, a w szczególności sieci neuronowe, które rozpoznają wzorce w obrazach i przypisują im odpowiednie etykiety. Dzięki temu możliwe jest przetwarzanie dużych ilości danych w krótkim czasie, co wspiera szybsze i bardziej efektywne wykorzystanie informacji.

Jedną z metod służących przyspieszeniu klasyfikacji obrazów jest wykorzystanie aktywnego uczenia. Jest to podejście do uczenia się maszyn, w którym algorytm uczący dokonuje wyboru próbek do nauki zamiast polegania na zestawie próbek statycznych. W przypadku klasyfikacji obrazu, algorytm może pytać użytkownika o etykietowanie wybranych próbek, aby nauczyć się jak najlepiej rozpoznawać i klasyfikować obrazy.
W pracy przedstawione zostały strategie aktywnego uczenia się przez maszynę, w tym wyjaśniona została metoda MCADL stanowiąca opracowanie naukowców z Uniwersytetów Hunan i Shandong, którzy deklarują, iż jako pierwsi na świecie opracowali metodę wielokryterialnego doboru próbek do treningu [2]. Metoda MCADL została wybrana do wykorzystania w ramach niniejszej pracy doktorskiej z uwagi na zaproponowane połączenie wielu kryteriów. Ich analiza wykazała, że każde z nich ma swoje zalety, ale ich połączenie może być szczególnie przydatne w przypadku ograniczonych zasobów danych oznaczonych oraz w zadaniach, w których zarządzanie niepewnością i poprawa dokładności klasyfikacji są kluczowe.

Z uwagi na przedstawioną przez autorów implementację w technologii *Tensorflow*, która statystycznie zaczyna ustępować nowocześniejszemu framework'owi *Pytorch* [5], zdecydowano o przeprowadzeniu implementacji metody MCADL również z wykorzystaniem własnego kodu, opracowanego w technologii *Pytorch*, w oparciu o bazę danych MNIST (ang. *Modified National Institute of Standards and Technology*).

Analiza wielokryterialna to podejście do podejmowania decyzji, które uwzględnia wiele kryteriów jednocześnie. W kontekście klasyfikacji obrazów, może być wykorzystana do wyboru najlepszego algorytmu klasyfikacji, który spełnia różne kryteria, takie jak dokładność klasyfikacji, szybkość uczenia się, odporność na zakłócenia, itp. W tym zakresie,

punkty odniesienia wykorzystywane są jako ramy odniesienia dla kryteriów oceny. Punkt odniesienia to wartość referencyjna dla danego kryterium. Stanowi podstawę do porównywania wyników uzyskanych dla różnych algorytmów klasyfikacji. Punkty odniesienia pozwalają na ustanowienie standardów i porównywanie wyników różnych algorytmów klasyfikacji obrazów. Przy użyciu punktów odniesienia, można określić, które algorytmy są bardziej efektywne w odniesieniu do określonych kryteriów i jakie są różnice między nimi.

W pracy przedstawiono najważniejsze aspekty z zakresu analizy wielokryterialnej związane z klasyfikacją obrazów, w tym w szczególności sposób implementacji analizy wielokryterialnej bazującej na metodzie punktu odniesienia oraz zakres interaktywnego wyznaczenia rozwiązań efektywnych w algorytmie i powstałe w ich wyniku nowe rozwiązanie. W celu wykazania skuteczności przyjętego sposobu optymalizacji zaimplementowano dodatkowo kolejną metodę, którą zintegrowano z wypracowanym rozwiązaniem i dzięki temu osiągnięto podane rezultaty.

W pracy zaproponowano algorytm, w którym ważenie kryteriów umożliwiające dokonywanie wyboru próbek do treningu zostało zastąpione metodą punktu odniesienia stosowaną w procesie interaktywnej optymalizacji wielokryterialnej zdefiniowanej w teorii wspomagania decyzji. Określono strategię wyboru punktów odniesienia i dokonano sprawdzenia działania opracowanego algorytmu na bazie MNIST, dla uzyskania właściwego efektu porównania. Przeprowadzono również eksperymenty opracowanego algorytmu na bazie zdjęć CIFAR-10, o zwiększonej różnorodności. W celu przetestowania, zrealizowano prace, które potwierdziły przydatność zaprezentowanego rozwiązania przy jednoczesnym polepszeniu poziomu dokładności.

Opracowana metoda stanowi jeden z komponentów wdrożenia projektu „Bałtyk Cyfrowy", realizowanego między innymi przez Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej (OBR CTM). Projekt koncentruje się między innymi na wsparciu procesu analiz, interpretacji i oceny sytuacji nawodnej. W ramach przedmiotowego projektu prowadzone są prace z zakresu wsparcia procesów wczesnego identyfikowania zagrożeń w celu oceny wpływu stanu bieżącej sytuacji na morskim teatrze działań oraz budowie bazy danych pozyskiwanych z rozpoznania obrazowego, w tym danych pochodzących z mobilnych i stacjonarnych układów sensorycznych oraz rozpoznania radioelektronicznego, a w perspektywie długofalowej przygotowanie do wykorzystania danych pochodzących z satelitarnych systemów rozpoznawczych. Badania i opracowanie metod przedstawionych w niniejszej pracy doktorskiej stanowią właściwą podbudowę teoretyczną i algorytmiczną do rozwoju technologii rozpoznania, co wraz z pozostałymi komponentami projektowanego systemu może przyczynić

się do poprawy zdolności do dowodzenia, rozpoznania, a także zdolności w obszarze przetrwania i zapewnienia bezpieczeństwa państwa.

1. Cele pracy

Celem niniejszej pracy jest zdefiniowanie metody klasyfikacji obrazu, która w następstwie zaproponowanej procedury optymalizacji spełni odpowiednie wymogi niezawodności oraz sprawności realizowanych obliczeń przy jednoczesnym utrzymaniu wysokiego poziomu dokładności (ang. *accuracy*), uwzględniając następujące cele szczegółowe:

a. przedstawienie aktualnych informacji na temat stanu zaawansowania algorytmów w zakresie widzenia komputerowego i trybów uczenia się maszyn, w tym wykorzystywanych w głębokim uczeniu *(*ang. *deep learning);*
b. przeanalizowanie metody MCADL, dokonanie jej implementacji, a następnie weryfikacji jej skuteczności;
c. wprowadzenie nowej metody inicjalizacji i analiz koszt-efekt;
d. opracowanie algorytmu, w którym ważenie kryteriów umożliwiające dokonywanie wyboru próbek do treningu zostanie zastąpione metodą punktu odniesienia stosowaną w procesie interaktywnej optymalizacji wielokryterialnej zdefiniowanej w teorii wspomagania decyzji;
e. określenie strategii wyboru punktów odniesienia;
f. sprawdzenie działania opracowanego algorytmu na bazie MNIST, w celu uzyskania właściwego efektu porównania;
g. potwierdzenie przydatności zaprezentowanego rozwiązania na danych z bazy i przetestowanie opracowanego algorytmu na bazie zdjęć CIFAR-10, o większej różnorodności.

Z uwagi na potrzebę wdrożenia wypracowanego rozwiązania oraz implementację w obszarze produktowym, praca nie ogranicza się do wymiaru naukowego, ale zawiera też dane z zakresu wojskowego obszaru zastosowań.

2. Teza pracy

Zastosowanie metody punktów odniesienia w algorytmie „*Multi-criteria active deep learning for image classification (MCADL)”*, zwiększa dokładność analizy obrazu i wykazuje wyższość nad wykorzystywaną w tymże algorytmie metodą ważenia kryteriów.

ROZDZIAŁ I
PRZEGLĄD STANU WIEDZY Z OBSZARU BIG DATA, WIDZENIA KOMPUTEROWEGO I ALGORYTMÓW KLASYFIKACJI

1. Od Big data do podjęcia decyzji

W 1997 roku dwóch naukowców NASA *Michael Cox* i *David Elisworth* użyło sformułowania „*the problem of big data*" [6] w opracowaniu przedstawiającym uwarunkowania związane z gromadzeniem danych, ich przetworzeniem i analizą. Wskazywali w nim między innymi na potrzebę opracowania dedykowanych rozwiązań do analizy zdjęć satelitarnych i lotniczych. Przedstawiali dane w dwóch wymiarach: jako zbiory danych (przykładowo z czujników lub satelitów) oraz obiekty danych (agregujące wielowymiarowe dane, jak modele pogodowe lub analizy strukturalne [7]).

Naukowcy z Uniwersytetu Oksfordzkiego w opracowaniu „*Big data, efektywna analiza danych*" wskazali na inne podejście, które zostało zdefiniowane, jako „*zdolność społeczeństwa do korzystania z informacji w nowatorski sposób, który ułatwia lepsze zrozumienie otaczającej rzeczywistości lub wytworzenie dóbr i usług o znacznej wartości*" [8]

Patrząc na problem biznesowo Bernard Marr [9] zdefiniował *big data* jako cyfrowy ślad, który generujemy w obecnej erze cyfrowej. Zgodnie z tą teorią, cyfrowy ślad składa się z wszystkich danych, które są przechwytywane, gdy używamy technologii cyfrowej. Podstawową ideą stojącą za wyrażeniem *big data* jest to, że wszystko, co robimy, w coraz większym stopniu pozostawia cyfrowy ślad, który można wykorzystać i analizować, aby uzyskać nową wiedzę. Zgodnie z teorią Marr'a siłami napędowymi w tym nowym wspaniałym świecie są: dostęp do coraz większych ilości danych oraz coraz większe możliwości technologiczne do wydobywania tych danych w celu uzyskania informacji handlowych.

Inne spojrzenie przedstawia raport firmy badawczej Gartner, który traktuje *big data*, jako zasoby informacyjne o dużej objętości, dużej szybkości i/lub dużej zmienności informacji, które wymagają efektywnych kosztowo, innowacyjnych form przetwarzania informacji umożliwiających lepszy wgląd, podejmowanie decyzji i automatyzację procesów [10].

Nie ma jednej definicji *big data,* ale istnieją pewne elementy, które są wspólne w różnych definicjach i funkcjonują w literaturze, jako komponenty "V" *big data,* definiowane, jako velocity, volume, variety, veracity (szybkość, objętość, różnorodność i prawdziwość). *Velocity* to prędkość przepływu danych, lub szybkość, z jaką dane są gromadzone. To proces, który nigdy się nie zatrzymuje. Atrybuty obejmują strumieniowanie w czasie zbliżonym do rzeczywistego lub w czasie rzeczywistym oraz lokalne i oparte na chmurze technologie, które

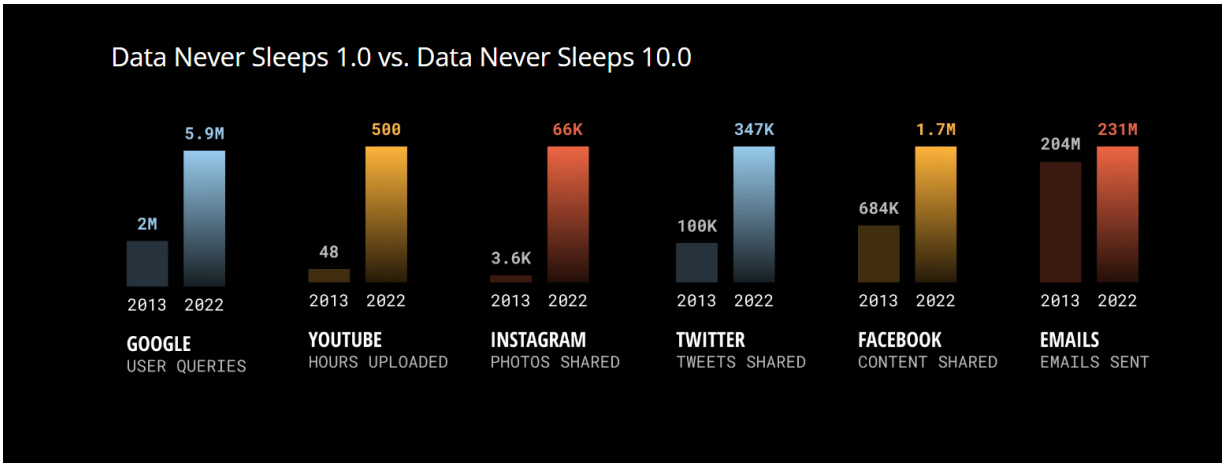
mogą przetwarzać informacje bardzo szybko. *Volume* to skala danych, czyli wzrost ilości przechowywanych danych. Na przykład eksabajty, zettabajty, yottabajty itd. Czynniki napędzające objętość to: wzrost źródeł danych, czujniki o wyższej rozdzielczości oraz skalowalna infrastruktura. *Variety* to różnorodność danych. To koncepcja, zgodnie z którą dane pochodzą z różnych źródeł, maszyn, ludzi, procesów, zarówno wewnętrznych, jak i zewnętrznych w stosunku do organizacji. Atrybuty obejmują stopień struktury i złożoności a czynnikami napędzającymi są technologie mobilne, media społecznościowe, technologie wearable, technologie geo, wideo i wiele, wiele innych [8]. *Veracity* to zgodność z faktami i dokładność. Prawdziwość odnosi się do jakości i pochodzenia danych. Atrybuty obejmują spójność, kompletność, integralność i niejednoznaczność. Czynniki warunkujące to między innymi koszt i potrzeba identyfikowalności.

Techniczne spojrzenie na *big data* wymaga określenia głównych komponentów tego zagadnienia i zdefiniowanie ich, jako między innymi: połączenie danych semistrukturalnych (jak pliki typu *XML* wraz z odpowiednimi plikami *XML Schema czy JSon*), prawie strukturalnych (jak strumienie webowe) i nieustrukturyzowanych (jak pliki tekstowe, *PDFy*, obrazy, video, tweety lub blogi) gromadzonych przez ludzi, organizacje, instytucje, które mogą być przeszukiwane w celu pozyskania informacji i wykorzystywane w projektach uczenia maszynowego, modelowania predykcji i innych zaawansowanych aplikacjach analitycznych [11]. Analityka *big data* wykorzystuje algorytmy uczenia się maszyn, dlatego większość istniejących frameworków (jak *Hadoop, Spark, Storm* czy *Samza*) jest uzupełniona o biblioteki i zestawy narzędzi służące szybkiej identyfikacji wzorców [12].

Współcześnie największą część *big data* w światowym obiegu informacyjnym stanowią dane obrazowe. Na skutek rozwoju technologii i urządzeń je wytwarzających ich ilość stała się niemożliwa do przetworzenia bez udziału komputerów. Dane multiplikują się w każdej sekundzie – są generowane nieustannie przez prawie 5 miliardów użytkowników internetu [13]. Około 6 miliardów osób [14] posiada telefon komórkowy, który zawiera kamerę umożliwiającą dostarczanie do sieci obrazów i filmów. Analizując skalę tego zjawiska warto dodać, że w każdej minucie na *YouTube* przesyłane jest 500 godzin nowych materiałów audio-wizualnych osób [14]. Liczba użytkowników tej platformy podwoiła się w ciągu tylko pięciu lat i w 2021 roku wyniosła 2,6 miliarda w stosunku do 2 miliardów w 2019 roku i 1,4 miliardów w 2016 roku [15].

Oczywistym jest, że wdrożenie technologii 5G wielokrotnie zwiększa proces wytwarzania, a następnie wykorzystania danych – przy równoczesnym przyspieszeniu czasu ich

przetwarzania. W tym kontekście akceleracja rozwoju algorytmów uczenia maszynowego będzie tylko postępować.



Rysunek 1 Infografika przedstawiająca dynamikę i trend wzrostu liczby danych na świecie na przykładzie terytorium USA. Za: [16]

Interpretacja danych wizualnych ma zastosowanie w wielu sferach życia gospodarczego i społecznego – wspierając rozwój medycyny, zarządzanie sytuacjami kryzysowymi, gospodarkę agrarną, przestrzenną oraz szerokorozumiany sektor bezpieczeństwa - w tym wywiad i rozpoznanie wojskowe. W zakresie tego ostatniego termin *big data* odnosi się do szerokiego spektrum informacji dostępnych z czujników, obrazów wideo, telefonów komórkowych, wywiadu sygnałowego i przechwytywania danych z wojny elektronicznej lub obrazów satelitarnych [15].

Analiza wyżej wymienionych danych jest procesem na który warto spojrzeć szerzej niż tylko przez pryzmat interdyscyplinarnego przedsięwzięcia obejmującego matematykę, statystykę czy informatykę. Aby dane miały wartość dla decydenta, muszą być zrozumiałe i interaktywne, najlepiej w czasie zbliżonym do rzeczywistego. A zatem jednym z krytycznych elementów systemu jest mechanizm, który wyodrębni istotne informacje, jeszcze zanim zostaną poddane analizie, gdyż z jednej strony duża część danych może nie mieć żadnej wartości, z drugiej, dane w postaci surowej mogą nie nadawać się do dalszego wykorzystania [17].

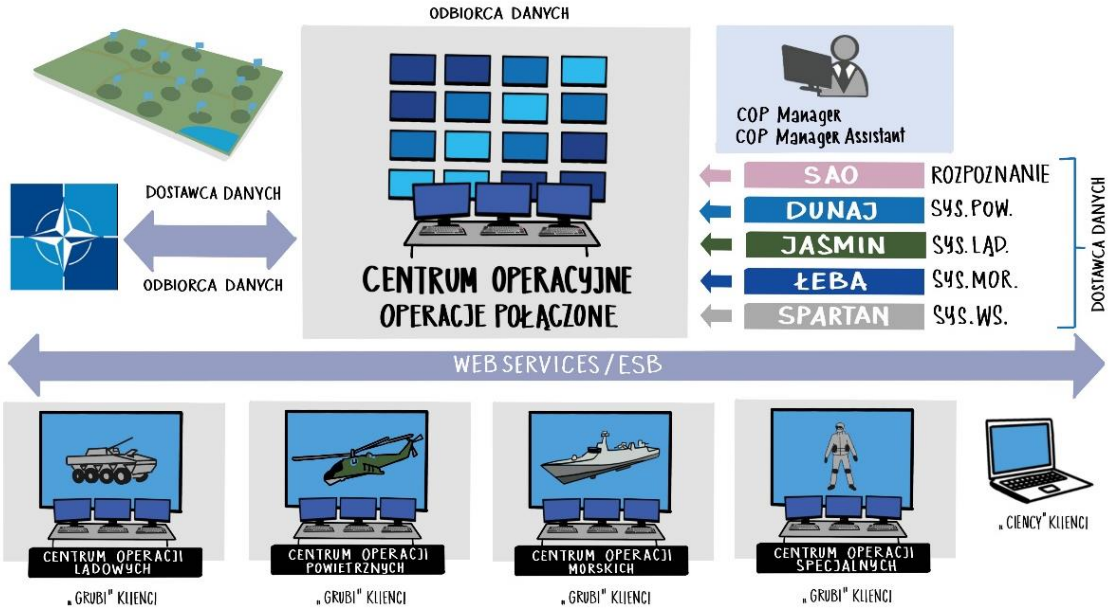
Istotnym zagadnieniem w tym zakresie będzie również *big data mining*, które zajmuje się wydobywaniem informacji z danych i wykorzystywaniem ich do przewidywania trendów i wzorców. Zasadniczo, analityka predykcyjna polega na uchwyceniu zależności pomiędzy zmiennymi objaśniającymi a zmiennymi przewidywanymi na podstawie zdarzeń z przeszłości, i wykorzystaniu ich do przewidywania nieznanego. Zaawansowane narzędzia analityki predykcyjnej umożliwiają analizę problemów związanych z danymi i przedstawianie wyników za pomocą prostych wykresów, diagramów liczb, które wskazują prawdopodobieństwo

możliwych wyników. Dokładność i użyteczność wyników zależą jednak od poziomu analizy danych i jakości założeń.

Z terminem big data ściśle związana jest analityka biznesu (ang. *business analytics*). W tym zakresie przewiduje się, że wiedza o tym, jak obsługiwać i analizować ogromne ilości danych, które są obecnie dostępne, stanie się jednym z głównych nurtów biznesowych na całym świecie. Największe firmy technologiczne, jak *Google, Apple* i wiele innych opracowują nowe podejścia do obsługi i analizy danych. Podejścia te zazwyczaj angażują tysiące lub dziesiątki tysięcy komputerów, które mogą być zaangażowane do rozwiązywania pozornie nierozwiązywalnych problemów. *Google, Yahoo* i *Facebook* posiadają centra danych o rozmiarach, które jeszcze dekadę temu były trudne do wyobrażenia. Rozwój tych ogromnych centrów obliczeniowych zmusił przemysł komputerowy do dostosowania się i opracowania procesorów, które zużywają znacznie mniej energii i generują znacznie mniej ciepła. Dodatkowo, te centra danych są obecnie budowane w pobliżu źródeł zasilania i chłodzenia (tj. rzek i dużych zbiorników wodnych) tak, aby ich koszty energii były niższe niż w przypadku poprzednich generacji. Wydajność tych nowych monstrualnie dużych centrów danych oznacza, że obserwuje się powrót do bardziej scentralizowanego przetwarzania, gdzie wiele firm może znaleźć to mniej kosztowne, aby zlecić niektóre z ich obliczeń do dostawcy chmury obliczeniowej. To z kolei rodzi szereg problemów związanych z bezpieczeństwem, niezawodnością, umowami i siecią [18].

Podobnie jest w środowisku militarnym. W obszarach obejmujących rozpoznanie wojskowe funkcjonuje również coraz więcej danych i coraz więcej zabezpieczeń musi być tworzonych, w coraz szybszym tempie.

Big data wykorzystuje się między innymi na potrzeby budowania świadomości sytuacyjnej (ang. *Common Operational Picture – COP*), nasyca wiedzą ekspercką i tworzy wspólne (na każdy szczebel decyzyjny) ramy ułatwiające identyfikację wzorców. Dane są osadzone w bazowej strukturze graficznej a system przetwarza złożone zapytania. Wykrywając wzorce system może generować różne rodzaje wizualizacji, takie jak mapy, linie czasu, zasoby przeciwnika i inne. Służy jako podstawa do podjęcia decyzji o dalszych działaniach [19]. Na rysunku 2 przedstawiono komponenty tworzenia Połączonego Obrazu Sytuacji Operacyjnej (POSO).



Rysunek 2 Koncepcja komponentów i przepływu danych na rzecz Połączonego Obrazu Sytuacji Operacyjnej. Opracowanie własne

Warto wskazać, że na rysunku uwzględniono SAO (System Analiz Obrazowych), jako źródło zobrazowań dla dowództwa, ale postępowanie na pozyskanie tego systemu zostało unieważnione w maju 2022 roku. Postępowanie na pozyskanie SPARTAN (Zintegrowany zautomatyzowany system dowodzenia operacjami specjalnymi) prawdopodobnie nie zostało jeszcze przeprowadzone.

Niewątpliwie więc, w poruszaniu się po rzeczywistości *big data* w obszarze wojskowym, wyjątkowego znaczenia nabierają nie tylko maszyny dokonujące przetworzenia wielu informacji, ale i sam proces podejmowania decyzji, który został definicyjnie przedstawiony w opracowaniu „*Teoria i Praktyka Wspomagania Decyzji*" [1], oraz jego elementy, w tym między innymi system wspomagania decyzji rozumiany, jako system komputerowy uwzględniający następujące komponenty:

- bazy danych,
- reprezentację wiedzy istotnej dla podejmowania danej klasy decyzji w formie bazy modeli sytuacji decyzyjnych (rzeczowych i preferencyjnych),
- algorytmy dla przetwarzania i wykorzystania tych danych oraz modeli,
- interfejs użytkownika, umożliwiający komunikację pomiędzy użytkownikiem a komputerem.

To właśnie część związana z opracowaniem efektywnego algorytmu klasyfikacji obrazu będzie przedmiotem szczegółowych analiz przedstawionych w niniejszej pracy.

Znaczenie *big data* w kwestiach dotyczących bezpieczeństwa będzie rosło. Związane jest to z rozwojem technologii i zmieniającym się obliczem świata, także jeśli chodzi o dynamikę współczesnych konfliktów. Ważna będzie zwłaszcza umiejętna analiza tzw. źródeł otwartych. Bo tutaj obowiązuje zasada odwróconego trójkąta – 70%, nawet 80% przydatnych informacji to dane ogólnodostępne

2. Widzenie komputerowe

Badania nad opracowaniem algorytmu, który w sposób automatyczny rozpozna obiekt przedstawiony na zdjęciu były prowadzone przez naukowców od momentu pojawienia się komputerów w XX wieku. Widzenie komputerowe (ang. *computer vision*), rozumiane jako rozpoznanie obrazu przez maszynę, zostało prawdopodobnie po raz pierwszy opisane w pracy doktorskiej *Larry Roberts* „*Block world*" w 1965 roku [20], gdzie rzeczywistość została przedstawiona w formie bloków – prostych kształtów geometrycznych, możliwych do identyfikacji a następnie odwzorowania. W ciągu kolejnych kilkudziesięciu lat powstało tysiące opracowań naukowych, w ramach których tworzono metody i algorytmy umożliwiające komputerom przetwarzanie obrazu i jego zawartości. Jednakże do końca lat 90. XX wieku rozpoznawanie świata wizualnego odbywało się na podstawie jego prostych struktur, w oparciu o ograniczoną liczby obiektów i ich charakterystyki (takie, jak figury geometryczne, proste, krawędzie, brzegi obiektów). Było to związane zarówno z techniką wykonywania samych zdjęć [21], jak i ograniczonymi możliwościami obliczeniowymi komputerów.

Wzrost ilości materiałów wizualnych, wykorzystywanych zarówno w przestrzeni naukowej, biznesowej jak i rządowej oraz innych sprawiła, że techniki uczenia się maszyn (ang. *machine learning*) zaczęły być dynamicznie rozwijane. Doskonalono narzędzia takie jak Maszyna Wektorów Nośnych (*SVM,* ang. *Support Vector Machine* [22]), głównie do zagadnień klasyfikacji, w których jedna klasa jest separowana możliwie dużym marginesem od drugiej klasy. Jednak podstawowy problem - możliwość automatycznego rozpoznania, klasyfikacji i lokalizacji każdego obiektu, na każdym zdjęciu - nie został jeszcze rozwiązany. Wiele modeli, bez względu na to czy rozważane były modele graficzne, SVM czy Adaboost [23] ulegało przetrenowaniu [24]. Wiązało się to przede wszystkim z wielością danych wizualnych (ang. *visual data*), w analizie których brały udział również złożone modele, z wyznaczonymi wieloma parametrami. Przy braku wystarczającej ilości danych treningowych modele szybko identyfikowały określony wzorzec, koncentrując się na nim i powstawał problem generalizacji

danych, uniemożliwiający propagację na nowe wzorce. Jakość wykonanych zdjęć była gorsza niż współcześnie, a produkowane wtedy komputery posiadały ograniczone moce obliczeniowe.

W 2009 roku tym zagadnieniem zajęli się naukowcy Uniwersytetu *Princeton* pod przewodnictwem *prof. Fei Fei Li*. Opublikowali opis utworzonej przez nich największej na świecie bazy obrazów *ImageNet* [25], uwzględniającej czternaście milionów etykietowanych obrazów, podzielonych na dwadzieścia dwa tysiące kategorii obiektów i scen [26]. Powstanie tego zestawu danych zapoczątkowało realizację corocznych konkursów ILSVRC (ang. *ImageNet Large Scale Visual Recognition Challenge*) [27] weryfikujących algorytmy identyfikujące obiekty w obrazach z bazy z najniższym wskaźnikiem błędu. Konkursy były realizowane do 2017 roku i w trakcie tych kilku lat dokładność w klasyfikowaniu obiektów wzrosła z 71,8% do 97,3%, przewyższając ludzkie możliwości [28].

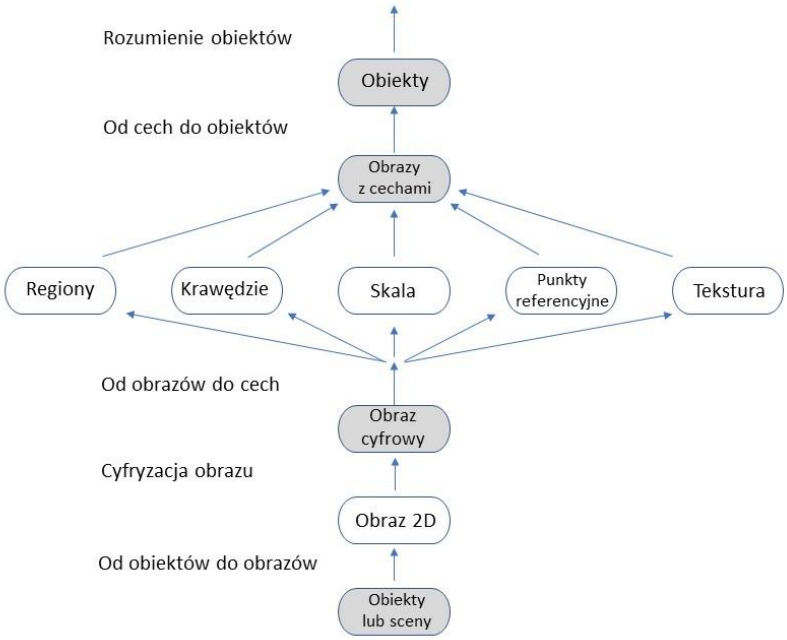
Utworzenie bazy *ImageNet* zwiększyło dynamikę rozwoju sztucznych sieci neuronowych (ANN, ang. *Artificial Neural Networks*), wśród których najbardziej efektywne w znajdowaniu wzorców na obrazie okazały się konwolucyjne sieci neuronowe (CNN, ang. *Convolutional Neural Networks*) [29], umożliwiające automatyzację rozpoznawania obrazów na niespotykaną dotąd skalę. Wprowadzenie CNN, większych zbiorów danych wizualnych i wydajnych zasobów obliczeniowych doprowadziło do szybkiego rozwoju rozwiązań dla zadań rozpoznawania obrazów. W 2012 roku, w trakcie konkursu ILSVRC zaprezentowano konwolucyjną sieć neuronową *AlexNet* [30], w której poziom błędu na zbiorze testowym (ang. *test error rate*) spadł o 10.8% w stosunku do dotychczasowych obliczeń istniejących na świecie i wyniósł 15.3%. W kolejnych latach poziom ten był systematycznie obniżany i osiągał nawet 3.6 % [31] i 2.3% [32]. Prezentowane w trakcie konkursu rozwiązania odpowiadały na problemy identyfikowane w ramach zadań uczenia nadzorowanego (ang. *supervised learning*)[2], o którym więcej w dalszej części rozdziału, będącego jedną z technik uczenia się maszyn (ang. *machine learning*)[3].

Widzenie komputerowe wykorzystuje algorytmy uczenia maszynowego, które rozpoznają wzorce w obrazach i wykorzystują te wzorce do sklasyfikowania obrazu. Zadania wizji komputerowej obejmują metody pozyskiwania, przetwarzania, analizy i rozumienia

[2] Uczenie nadzorowane występuje, gdy algorytmy otrzymają wartości docelowe dla instancji treningowych i zostaną poinformowane, jakie wartości mają przewidzieć dla instancji testowych.
[3] Uczenie się maszyn: Zdolność maszyny do zdobywania własnej wiedzy poprzez wydobywanie wzorców z surowych danych. Za: [31]

obrazów cyfrowych, a także ekstrakcji wielowymiarowych danych z rzeczywistego świata w celu uzyskania informacji numerycznych lub symbolicznych [33].

Techniki przetwarzania obrazów (ang. *image processing*) są zróżnicowane i obejmują optykę, astronomię, statystykę, matematykę, psychofizykę, neurofizykę, itp. Przetwarzanie obrazu może być postrzegane, jako metoda pozyskiwania informacji o obrazowanym obiekcie. Obiekt istnieje w świecie fizycznym z unikalnymi właściwościami fizycznymi. Obraz obiektu jest obserwacją dokonaną przez system obrazowania z własnymi geometrycznymi i spektralnymi charakterystykami [34].



Rysunek 3 Poziomy reprezentacji obrazu

Rysunek 3 przedstawia możliwe poziomy reprezentacji obrazu adekwatne do rozwiązania problemów analizy obrazu, w ramach których obiekt powinien zostać sklasyfikowany i zlokalizowany [35]. Obrazy są pobierane przez komputer, jako dane wejściowe (ang. *input data*), a właściwości obrazów są zmieniane w celu ich poprawy lub też wyodrębniane są cechy (atrybuty) upraszczające ich analizę [36]. W trakcie procesu przeprowadzanego od obrazu wejściowego do modelu redukowane są informacje zawarte w obrazie do informacji istotnych dla dziedziny zastosowania. Proces ten jest zwykle podzielony na kilka etapów i wykorzystuje kilka poziomów reprezentujących obraz. Dolna warstwa zawiera surowe dane obrazu, a wyższa warstwa interpretuje dane [35]. Przykładem tak opisanego procesu może być analiza obrazów za pomocą konwolucyjnej sieci neuronowej (ang. *convolutional neural network - CNN*), zawierająca:

a) Pobieranie danych wejściowych. Obrazy są pobierane przez komputer jako dane wejściowe. Mogą być to zdjęcia cyfrowe, ramki wideo lub inne formy obrazów.
b) Przetwarzanie wstępne. W celu poprawy jakości obrazów lub wyodrębnienia istotnych cech, przeprowadza się przetwarzanie wstępne. Może to obejmować takie operacje jak zmiana rozmiaru obrazu, normalizacja wartości pikseli, usuwanie zakłóceń lub wyrównywanie histogramu.
c) Wyodrębnianie cech. W trakcie analizy obrazu za pomocą CNN, wykorzystuje się kolejne warstwy sieci neuronowej do wyodrębniania istotnych cech. Każda kolejna warstwa może być odpowiedzialna za rozpoznawanie coraz bardziej złożonych wzorców. Na przykład, początkowe warstwy mogą wykrywać proste krawędzie, a następne warstwy mogą rozpoznawać kształty, tekstury lub obiekty.
d) Redukcja informacji. Proces analizy obrazu za pomocą CNN opiera się na stopniowym redukowaniu informacji zawartych w obrazie do istotnych dla konkretnej dziedziny zastosowania. Wyższe warstwy sieci neuronowej skupiają się na coraz bardziej abstrakcyjnych cechach, które mają znaczenie dla rozpoznawania obiektów lub wykonywania konkretnych zadań.
e) Interpretacja danych. W najwyższej warstwie sieci neuronowej następuje interpretacja zebranych informacji. Może to obejmować klasyfikację obiektów na obrazie, wykrywanie obecności lub braku pewnych cech, segmentację obrazu na różne regiony lub generowanie opisów obrazu.

Opisany proces jest często realizowany przez wiele warstw konwolucyjnych i warstw poolingowych, które działają na obrazie wejściowym, aby stopniowo redukować informacje i budować coraz bardziej abstrakcyjne reprezentacje. CNN jest jednym z najczęściej stosowanych modeli do analizy obrazów i znajduje zastosowanie w wielu dziedzinach, takich jak rozpoznawanie obiektów, detekcja twarzy, samochodów, medycyna obrazowa i wiele innych.

3. Algorytmy klasyfikacji

3.1. Proces klasyfikacji

Proces klasyfikacji obiektów na zdjęciu to jeden z kluczowych elementów w dziedzinie widzenia komputerowego. Polega on na przypisaniu obiektom na zdjęciu odpowiednich etykiet lub kategorii. Proces ten wymaga zastosowania zaawansowanych algorytmów przetwarzania obrazów, które analizują piksele na zdjęciu i wyciągają z nich informacje

o kształcie, kolorze, teksturze i innych cechach. Następnie te informacje są przetwarzane przez modele uczenia maszynowego, które uczą się rozpoznawać i klasyfikować obiekty na zdjęciach.

Klasyfikacja obiektów na zdjęciu ma wiele praktycznych zastosowań, takich jak rozpoznawanie twarzy, wykrywanie defektów w produktach przemysłowych czy rozpoznawanie chorób na zdjęciach medycznych. Klasyfikacja jest procesem, w którym model jest uczony danej etykiety lub wzorca. Polega na rozpoznaniu niewidzialnego wzorca (*x*), czyli przyporządkowania obiektu do jednej z predefiniowanych *n* klas – K

$$\mathrm{K}: \{K_1, K_2, \ldots K_n, \} \tag{1}$$

Klasa obiektu jest pojęciem abstrakcyjnym i stanowi zbiór zawierający podobne wektory cech

$$\mathrm{x} = [x_1, x_2, x_3, \ldots x_n] \tag{2}$$

wyznaczających kierunki wielowymiarowej przestrzeni nazywanej przestrzenią cech (ang. *feature space*).

Klasyfikacja danych obejmuje w pierwszej kolejności budowę modelu (klasyfikatora, który służy do predykcji wartości atrybutu decyzyjnego (klasy)) opisującego predefiniowany zbiór klas danych lub zbiór pojęć, a w drugiej zastosowanie opracowanego modelu do klasyfikacji nowych danych.

Dokonanie klasyfikacji przebiega w oparciu o dane podzielone na część treningową na bazie, której budowany jest model i część testową, czyli drugi zbiór służący do testowania klasyfikatora, który umożliwia wypracowanie odpowiedniej jakości modelu. Zbiór treningowy stanowiący podstawę do uczenia się przez model można wyrazić wzorem:

$$\{< x_i, K_j >\}, \text{ gdzie } i = 1,\ldots n \;\; j = 1, \ldots, n \tag{3}$$

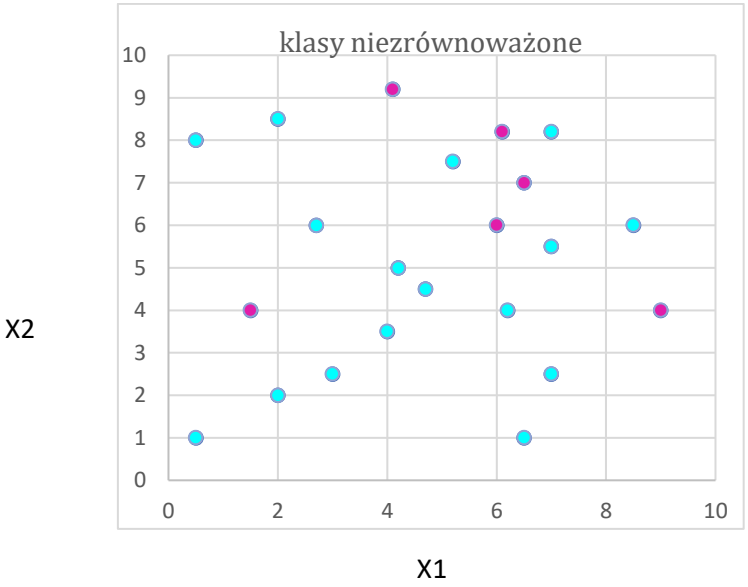
Często wyodrębniana jest również partia danych do walidacji modelu.

Wybór odpowiednich klas zależy od kontekstu i celu zadania klasyfikacji. Poprawne zdefiniowanie klas jest kluczowe dla skutecznego treningu modelu i osiągnięcia wysokiej dokładności w predykcji klas dla nowych danych.

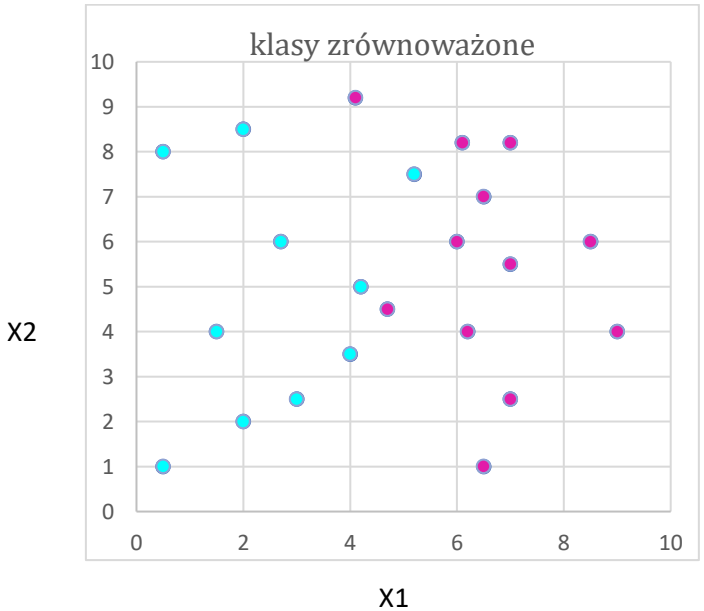
3.2. Równowaga klas

Zbiór treningowy budowany jest na bazie historycznych danych, które mogą być niepełne. Równowaga klas jest pożądana, ponieważ pomaga w skutecznym uczeniu modelu klasyfikacyjnego, a wyniki predykcji są bardziej wiarygodne dla wszystkich klas. Jeśli klasy nie są w przybliżeniu równoliczne stwierdza się niezbalansowanie klas w zbiorze uczącym. To obniża zdolność predykcyjną modelu. Przykład niezrównoważonego zbioru danych

zaprezentowano na rysunku 4, gdzie X1 i X2 oznaczają atrybuty danych, kolory zaś przyporządkowanie do klas. W zbiorze tym występuje niezbalansowanie obiektów należących do dwóch klas. Niektóre klasyfikatory pomimo wysokiej globalnej trafności nie rozpoznają klasy mniejszościowej.



Rysunek 4 Niezrównoważone zbiory klas.



Rysunek 5 Zrównoważone zbiory klas

Niezbalansowanie danych w kontekście klasyfikacji można równoważyć z wykorzystaniem poniższych technik:

a) Oversampling (przesampling), Metoda ta polega na powieleniu próbek z mniejszej klasy, aby zrównoważyć liczebność klas. Można to zrobić przez losowe powielanie

próbek mniejszej klasy lub poprzez generowanie sztucznych przykładów na podstawie istniejących próbek.

b) Undersampling (niedosampling). W tej metodzie usuwa się próbki z większej klasy, aby zrównoważyć liczebność klas. Można to zrobić przez losowe usunięcie próbek większej klasy lub przez selektywne usunięcie próbek na podstawie pewnych kryteriów.
c) Zastosowanie wag. Można również zastosować wagi dla różnych klas w celu uwzględnienia niezbalansowania. Na przykład, możesz zastosować większą wagę dla próbek z mniejszej klasy, aby uczynić je bardziej istotnymi podczas uczenia modelu.
d) Generowanie sztucznych przykładów. Można wygenerować sztuczne przykłady dla mniejszej klasy, na przykład poprzez techniki takie jak SMOTE (Synthetic Minority Over-sampling Technique) lub ADASYN (Adaptive Synthetic Sampling). Te metody generują nowe próbki na podstawie sąsiedztwa istniejących próbek, aby zwiększyć liczebność mniejszej klasy.
e) Zastosowanie innych algorytmów, Istnieją również specjalne algorytmy klasyfikacji, które są bardziej odporne na niezbalansowane dane, takie jak Random Forests, Gradient Boosting Machines (GBM) czy Support Vector Machines (SVM). Te algorytmy mają wbudowane mechanizmy uwzględniające niezbalansowanie w danych.

Wybór odpowiedniej metody zależy od konkretnej sytuacji i charakterystyki danych. Często konieczne jest przetestowanie różnych technik i dostosowanie ich do swojego konkretnego problemu.

W zakresie zbiorów danych, klasyfikatory można podzielić na kilka rodzajów, w zależności od ich kompletności i zrównoważenia klas. Przykładem niekompletnego zbioru danych posiadającego wiele klas, jest zbiór zdjęć pozyskiwanych z różnych źródeł, w różnym czasie i w odniesieniu do znaczącego zasięgu geograficznego w wojskowych ośrodkach zobrazowań.

3.3. Metryki oceny klasyfikacji

Metryki oceny klasyfikacji przyjmują wartości liczbowe, które pozwalają ocenić jakość działania modelu klasyfikacyjnego na podstawie wyników predykcji. Są wykorzystywane do oceny skuteczności modelu w przewidywaniu prawidłowych klas lub etykiet dla danych testowych. Pozwalają lepiej zrozumieć różne aspekty działania modelu klasyfikacyjnego, zwłaszcza w przypadkach, gdzie istnieje nierównowaga klasowa lub klasyfikacja nie jest równie ważna dla wszystkich klas. Pomagają w dostarczeniu szczegółowych informacji na

temat jakości klasyfikacji i mogą być pomocne w dostosowywaniu modelu do konkretnych wymagań zadania. W celu zbadania poprawności i efektywności modelu wyróżnia się oceny, odzwierciedlone w macierzy zmieszania i wzorach metryk oceny przedstawionych na rys. 6.

		PRZEWIDYWANA KLASA (*ang. Predicted class*)		
		Pozytywna *(ang. Positive)*	Negatywna *(ang. Negative)*	
RZECZYWISTA KLASA (*ang. Actual class*)	Pozytywna *(ang. Positive)*	Prawdziwe Pozytywna *(ang. True positive – TP)*	Fałszywie Negatywna *(ang. False negative – FN)*	CZUŁOŚĆ *(ang.Recall)* $\frac{TP}{(TP+FN)}$
	Negatywna *(ang. Negative)*	Fałszywie Negatywna *(ang. False negative – FN)*	Prawdziwie Negatywna *(ang. True negative – TN)*	SWOISTOŚĆ *(ang. Specificity)* $\frac{TN}{(TN+FP)}$
		PRECYZJA *(ang. Precision)* $\frac{TP}{(TP+FP)}$	NEGATYWNA WARTOŚĆ PREDYKCYJNA *(ang. Negative predictive value)* $\frac{TN}{(TN+FN)}$	DOKŁADNOŚĆ *(ang. Accuracy)* $\frac{TP+TN}{(TP+TN+FP+FN)}$

Rysunek 6 Metryki oceny klasyfikacji. Opracowanie własne na podstawie [37]

Znaczenie metryk przedstawionych na rysunku 6 jest następujące:

a) Precyzja modelu (ang. *precision*) informuje, ile wśród instancji wskazanych, jako pozytywne jest prawdziwie pozytywnych i dlatego powinna przyjmować jak najwyższą wartość.

b) Negatywna wartość predykcyjna (ang. *negative predictive value*) oznacza poziom instancji zaprognozowanych negatywnie w stosunku do rzeczywiście negatywnych. Jest wynikiem dzielenia prawidłowo wskazanych negatywnych wartości (TN) przez sumę wszystkich zaprognozowanych negatywnie (z uwzględnieniem błędnie wskazanych). Powinna przyjmować wartości bliskie 1.

c) Dokładność modelu (ang. *accuracy*), stosowana dla zbioru testowego wskazuje jaki procent danych zostało zaklasyfikowanych poprawnie. Dokładność jest najczęściej wykorzystywanym wskaźnikiem, który pozwala ocenić jakość klasyfikacji.

d) Swoistość modelu (ang. *specificity* lub *True Negative Rate*) to miara negatywnych przykładów oznaczonych jako negatywne przez klasyfikator. Wysoki poziom tej miary pokazuje, że model rzadko się myli, jeśli chodzi o negatywne przypadki.
e) Czułość (ang. *recall* lub *sensitivity*) to miara pozytywnych przykładów oznaczonych jako pozytywne przez klasyfikator, również tych, które błędnie zostały zaklasyfikowane do negatywnych – FN. Jest parametrem, który powinien przyjmować jak największą wartość.

W zależności od rodzaju problemu klasyfikacji i wymagań, używane są również inne metryki oceny, takie jak wskaźnik Gini, indeks Matthews, krzywa ROC (ang. *Receiver Operating Characteristic*) i wiele innych. Wybór odpowiednich metryk zależy od kontekstu problemu i oczekiwań wobec modelu klasyfikacyjnego.
W eksperymentach przeprowadzonych w niniejszej pracy do oceny jakości modelu zastosowano metrykę dokładności.

3.3 Działanie algorytmów w procesie uczenia

W problemach uczenia się maszyn z zakresu klasyfikacji obrazu wyróżnia się kilka podstawowych grup algorytmów, w tym przede wszystkim: algorytmy uczenia nadzorowanego, nienadzorowanego oraz przez wzmocnienie (ang. *reinforcement learning*).

Najczęściej stosowane metody w uczeniu algorytmu z nadzorem to regresja (pozwalająca na przewidzenie w sposób ciągły wartości wyjściowej) i klasyfikacja (stwierdzająca dyskretną wartość wyjściową w zakresie 1 lub 0) [38]. W klasyfikacji nadzorowanej wykorzystywane są dane, które podlegały analizie empirycznej lub eksperta dziedzinowego i zostały opisane wektorem cech przyporządkowującym do jednej z predefiniowanych klas obiektu. W zakresie analizy obrazu wektor cech będący w rzeczywistości wektorem liczb zwanych wartościami cech może być wyliczony po zeskanowaniu obrazu i przypisany do określonego obiektu. Przestrzeń cech, w której znajduje się obiekt charakteryzuje ilość wymiarów odpowiadająca liczbom zawartym w wektorze. Tak zdefiniowany punkt w wielowymiarowej przestrzeni cech może zostać zapisany, jako obiekt (np. czołg).
Najpopularniejsze z algorytmów nadzorowanych przedstawiono poniżej:

- Regresja logistyczna (ang. *logistic regression*) wykorzystuje funkcję sigmoidalną (ang. *sigmoid function*) do oszacowania prawdopodobieństwa danej etykiety. Występuje często w problemach binarnych, gdzie następuje wskazanie *prawda* (ang. *True*) lub *fałsz* (ang. *False*). Jest de facto algorytmem klasyfikacji, tylko

ze wskazanym określonym poziomem (ang. *threshold*) wskazującym na przyporządkowanie próbki do klasy A lub B.

- Drzewo decyzyjne (ang. *decision tree*)[4] jest przykładem klasyfikatora gorliwego[5]. Polega na zbudowaniu gałęzi decyzyjnych odzwierciedlających najważniejsze cechy. W praktyce drzewa są strukturą danych reprezentowaną w pamięci komputera. Końcowa decyzja, co do zaklasyfikowania obiektu jest podejmowana na poziomie liści drzewa, kiedy najważniejsze cechy w podzbiorach zidentyfikują obiekt. Ustalenie klasy następuje na podstawie testowania atrybutów.
- Las losowy (ang. *random forrest*) agreguje drzewa decyzyjne, które pełnią funkcję predyktorów. Ponadto wykorzystuje technikę *baggingu*,[6] która pozwala każdemu drzewu trenowanemu na próbie losowej z oryginalnego zbioru danych na pozyskanie zbiorowych głosów. W porównaniu do drzewa decyzyjnego algorytm lasu losowego generalizuje lepiej, ale z uwagi na wielość warstw jest trudniej interpretowalny.
- Algorytm SVM jest klasyfikatorem binarnym działającym w oparciu o wyznaczoną granicę pomiędzy próbkami, która nazywana jest hiperpłaszczyzną (ang. *hyperplane*) [22]. Jedna z najważniejszych charakterystyk wynikająca z jego wykorzystania to uniknięcie dzięki zastosowaniu SVM *overfittingu* (nadmiernego dostosowania) oraz umiejętność przetwarzania danych z wieloma cechami. Uzyskał dotychczas duże znaczenie w różnych implementacjach w obszarze działalności przemysłu.
- k NN (ang. *k - Nearest Neighbour*) należy do grupy klasyfikatorów leniwych. Reprezentuje punkty w przestrzeni n-wymiarowej zdefiniowanej przez n-cech. Próbki bez etykiet są klasyfikowane w oparciu o bliskość danych oznaczonych (tzw. sąsiadów). Nie buduje więc profilu dla klasy, ale przechowuje w pamięci wszystkie cechy przypisane do klasy i używa ich, gdy musi sklasyfikować nową

[4] Publikacja pierwszego algorytmu drzewa regresji (ang. *regression tree algorithm*) miała miejsce w 1963 roku (Morgan & Sonquist, 1963), za: Loh, W.-Y. (2014). Fifty Years of Classification and Regression Trees. International Statistical Review / Revue Internationale de Statistique, 82(3), 329–348. http://www.jstor.org/stable/43298996

[5] Klasyfikacja algorytmów uczenia maszynowego na leniwe i gorliwe wynika z ich fundamentalnych różnic w obsłudze i przetwarzaniu danych. Kluczowe rozróżnienie między leniwym i gorliwym uczeniem się w uczeniu maszynowym wynika z tego czy i kiedy uogólniają one dane treningowe. Gorliwe algorytmy robią to podczas treningu, podczas gdy algorytmy leniwe unikają wyprowadzania ogólnych reguł lub budują lokalne modele dla każdego obiektu, który mają sklasyfikować. Te różnice wpływają na efektywność uczenia się, zdolność adaptacji do nowych danych i elastyczność powstałych modeli. Uczenie gorliwe pojawiło się jako pierwsze, ale napotkało wyzwania związane z dużymi zbiorami danych i przewidywaniami w czasie rzeczywistym, co doprowadziło do rozwoju leniwego uczenia się w celu rozwiązania tych kwestii. Za: [108].

[6] *Bagging* jest jedną z ostatnich i udanych, intensywnych obliczeniowo metod poprawy niestabilnej estymacji lub schematów klasyfikacji. Jest ona przydatna w przypadku dużych, wielowymiarowych problemów z zestawem danych, gdzie znalezienie dobrego modelu lub klasyfikatora w jednym kroku jest niemożliwe z powodu złożoności i skali problemu. Za: [109].

instancję. Jako najbliższych sąsiadów klasyfikowanego obiektu należy rozumieć najbardziej podobne do niego, pod względem przyjętej miary podobieństwa, obiekty ze zbioru referencyjnego. W tym zakresie nie ma potrzeby tworzenia uogólnionego modelu danych, ani definiowania sposobu rzutowania przestrzeni cech pozwalającego na stworzenie funkcji opisującej granice pomiędzy obiektami należącymi do różnych klas dla całego zbioru danych uczących [39]. Natomiast jest to strategia obarczona dużym kosztem, gdyż algorytm za każdym razem musi obliczać *n* wartości podobieństwa, gdzie *n* to liczba instancji wykorzystanych do uczenia;

- Naiwny Bayes (ang. *naive Bayes*) to algorytm oparty o twierdzenie Bayesa [40]. Przyjmuje poziom prawdopodobieństwa szacowany w oparciu o wcześniej posiadaną wiedzę i „naiwne" założenie, że wszystkie cechy są niezależne od siebie. Ma on zastosowanie w aktualizacji wiedzy na podstawie nowych informacji oraz w estymacji prawdopodobieństw warunkowych. Mając obiekt X i zakładając, że prawdopodobieństwo P(X) jest takie samo dla każdej klasy, klasyfikator szuka klasy, dla której wartość wyrażenia zdefiniowanego we wzorze 4 jest największa.

$$\mathrm{F}(K_i) = \mathrm{P}(\mathrm{X}|\mathrm{K} = K_i)\mathrm{P}(\mathrm{K} = K_i) \tag{4}$$

gdzie:

P(X | K) - prawdopodobieństwo wystąpienia zdarzenia X, przy założeniu, że zdarzenie K jest prawdziwe.

P(K) - prawdopodobieństwo wystąpienia zdarzenia K niezależnie od zdarzenia X.

F(K_i) - funkcja, która estymuje prawdopodobieństwo zdarzenia K_i, mając dane X.

Wzór Bayesa umożliwia aktualizację a priori prawdopodobieństwa K_i na podstawie nowych obserwacji X. Gaussowski klasyfikator Bayesowski, oparty na normalnym rozkładzie i mieszaninie wielomianów, jest powszechnie stosowany w klasyfikacji, estymacji i wnioskowaniu na podstawie dostępnych danych.

Opisane algorytmy często wymagają dużych zbiorów danych do treningu w związku z potrzebą nauczenia się wielu parametrów. W przypadku niewystarczającej liczby próbek stosuje się metody poszerzania danych (ang. *data augmentation*) lub transfer learningu, by wzmocnić aspekt generalizacji [41].

W uczeniu przez wzmacnianie nie przygotowuje się zestawu danych uczących tylko środowisko, z którego model będzie zbierał dane automatycznie. Systemowi uczącemu się ze wzmocnieniem nie są dostarczane przykłady trenujące, a jedynie wartościująca informacja trenująca, oceniająca jego dotychczasową skuteczność.

W uczeniu nienadzorowanym, algorytm wskazuje wzorce w danych (opisane wektorem cech), które nie są zdefiniowane, gdyż dane nie posiadają etykiet. Wykrywając podobieństwo pomiędzy punktami algorytm może dokonać klastrowania[7] (ang. *clustering*) lub powiązać relacje pomiędzy zmiennymi (ang. *association algorythms*) bądź przeprowadzić redukcję wymiaru (ang. *dimensionality reduction*). Działanie takiego algorytmu polega na zdefiniowaniu zbioru obiektów o podobnych cechach z wykorzystaniem danego kryterium lub miary podobieństwa. Podejścia oparte na klasteryzacji wykorzystują strukturę danych, aby wybrać reprezentatywne instancje [42].

Przykładem takiego rozwiązania jest algorytm k-średnich (ang. *k-means*), gdzie punkty danych są przypisane do K grup. K reprezentuje liczbę klastrów w oparciu o odległość od centroidu każdej grupy. Punkty danych znajdujące się najbliżej danej centroidy będą skupione w tej samej kategorii. Większa wartość K będzie wskazywać na mniejsze zgrupowania o większej ziarnistości, podczas gdy mniejsza wartość K będzie miała większe zgrupowania i mniejszą ziarnistość. Stanowi najbardziej znaną i stosowaną metodę klastrowania. *K-means* jest przykładowo implementowane w zakresie segmentacji rynku, grupowaniu dokumentów, segmentacji obrazów i kompresji obrazów. Ta metoda jest przedmiotem implementacji również w zakresie niniejszej pracy, o czym napisano w kolejnych rozdziałach.

Kolejnym przykładem uczenia nienadzorowanego jest przyjęcie modelu probabilistycznego, który wspiera rozwiązania związane z estymacją gęstości lub tak zwanym "miękkim" grupowaniem. W klasteryzacji probabilistycznej punkty danych są grupowane na podstawie prawdopodobieństwa o przynależności do określonego rozkładu. Model Mieszaniny Rozkładu Gaussa (GMM) jest jedną z najczęściej stosowanych metod grupowania probabilistycznego. Składa się z nieokreślonej liczby funkcji rozkładu prawdopodobieństwa. GMM wykorzystuje się przede wszystkim do określenia, do którego rozkładu prawdopodobieństwa należy dany punkt danych. Jeżeli znane są średnia i wariancja, to można określić, do którego rozkładu należy dany punkt danych. Jednak w GMM zmienne te nie są znane, więc zakładamy, że istnieje ukryta zmienna, aby odpowiednio pogrupować punkty danych.

[7] Klastrowanie jest techniką eksploracji danych, która grupuje nieoznakowane dane na podstawie ich podobieństw lub różnic.

Inną metodą, która wpływa na dokładność klasyfikacji zarówno dzięki danym oznaczonym, jak i bez etykiet jest *Expectation-Maximization (EM).* Stanowi ona klasę algorytmów iteracyjnych opracowanych w celu zdefiniowania maksymalnych oszacowań prawdopodobieństwa lub maksymalnej estymacji a posteriori w problemach z niekompletnymi danymi. Oznacza to, że w badaniu przestrzeni prawdopodobieństwa danych, znajduje parametry klasyfikatora, które lokalnie maksymalizują prawdopodobieństwo wszystkich danych - zarówno tych oznaczonych, jak i nieoznaczonych [43]. Jest on powszechnie stosowany do oszacowania prawdopodobieństwa przypisania danego punktu danych do określonego klastra danych.

Praktycy głębokiego uczenia (ang. *deep learning*) stosujący w coraz większym stopniu modele do rozwiązywania problemów w różnych dziedzinach, od medycyny przez rynek nieruchomości po określanie poziomu ryzyka finansowego przedsiębiorstw, w sposób nieoptymalny obciążali ekspertów etykietowaniem dużych ilości danych do treningu [43]. Nawet więc jeśli wiele algorytmów stosowanych w trybie uczenia nadzorowanego było w stanie osiągnąć 97% precyzję, coraz więcej prac zaczęło koncentrować się na rozwiązaniach w trybie aktywnego uczenia (ang. *active learning*), ponieważ etykietowanie wszystkich danych okazało się zbyt kosztowne i zajmowało zbyt dużo czasu [44].

Mając na względzie, iż wypracowany w ramach niniejszej pracy algorytm, został zdefiniowany właśnie dla klasyfikacji obiektów w trybie aktywnego uczenia się maszyn, z wykorzystaniem sieci neuronowej, szczegółowy zakres jego funkcjonowania i samego *active learningu* zostanie przedstawiony w następnym rozdziale.

ROZDZIAŁ II
ACTIVE LEARNING W KLASYFIKACJI OBRAZU

1. Strategie i metody aktywnego uczenia

Sprawna analiza i wnioskowanie z danych umożliwia pozyskanie wiedzy o charakterze między innymi operacyjnym i strategicznym, niezbędnym do funkcjonowania danej jednostki. Kluczowe dla ekstrakcji najbardziej adekwatnych i potrzebnych informacji z dużych zbiorów danych jest przyjęcie właściwej strategii (ang. *sample selection strategy*) ich wyboru.

W przeciwieństwie do uczenia nadzorowanego, aktywne uczenie - czasami nazywane w literaturze nauką przez zapytanie (ang. *query learning*) lub optymalnym projektem eksperymentu (ang. *optimal experimental design*) - zakłada, że jeśli algorytmowi uczącemu pozwoli się wybierać dane, które wydają mu się najbardziej interesujące, to będzie osiągał lepsze wyniki przy mniejszej ilości treningu [45]. W przeciwieństwie do klasycznego uczenia pasywnego[8], w którym przykłady do etykietowania są wybierane losowo z puli nieoznakowanych przykładów, aktywne uczenie ma na celu staranny wybór próbek, minimalizujący w ten sposób koszt uzyskania danych oznaczonych. Jest to szczególnie interesujące w problemach, gdzie istnieją duże ilości danych (czego najlepszym przykładem są ośrodki zobrazowań wojskowych), a etykiet jest mało lub ich koszt wytworzenia jest wysoki [46]. Inaczej ujmując, aktywne uczenie ma na celu opracowanie takich algorytmów, które efektywnie przyporządkują etykiety w następstwie wskazania najbardziej adekwatnych próbek do oznaczenia. Wykorzystywane w tej metodzie procesy treningowe pomagają w osiąganiu najwyższej dokładności klasyfikacji przy użyciu jak najmniejszej liczby etykiet [47].

Typowy proces aktywnego uczenia się maszyny można w skrócie opisać w następujący sposób [48]:

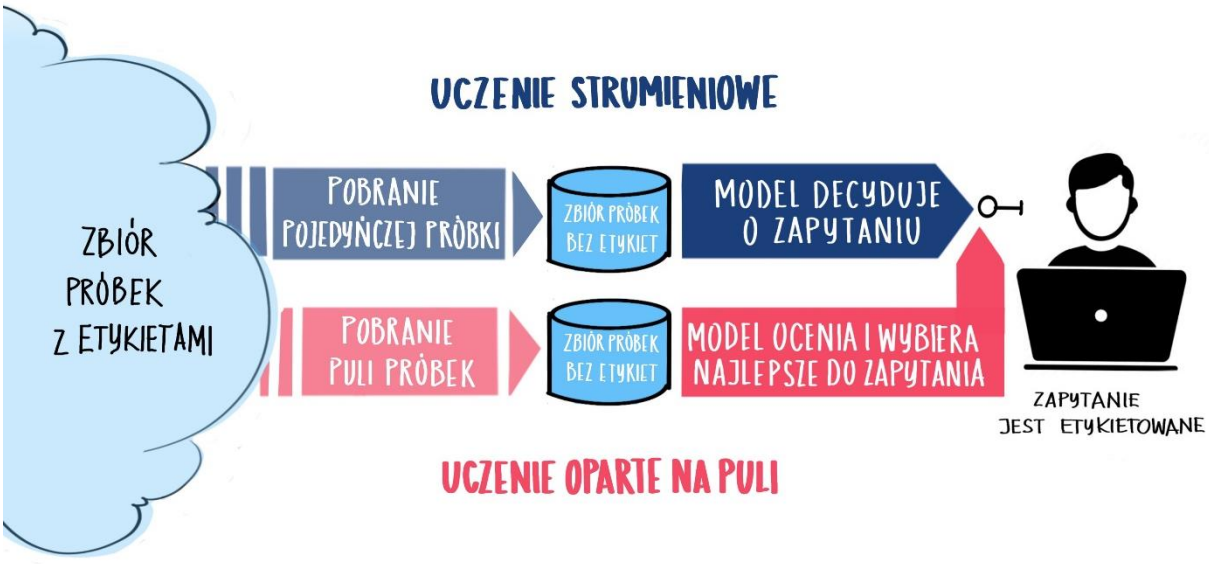
a) Generowanie modelu bazowego na podstawie niewielkiego, początkowego zbioru treningowego.
b) Wybranie instancji/próbek za pomocą funkcji próbkowania z dużego zbioru nieoznakowanych danych i nadanie im etykiet.
c) Dodanie nowo oznakowanych przykładów do zbioru treningowego i aktualizacja modelu.
d) Powtórzenie procesu do momentu osiągnięcia oczekiwanej wydajności lub wyczerpania budżetu przeznaczonego na etykietowanie.

[8] Powszechnie stosowaną metodą zbierania danych jest uczenie pasywne (ang. *passive learning*), w którym próbki do treningu są losowo wybierane z rozkładu bazowego i ręcznie opatrywane etykietami przez człowieka.

Trudność polega na zdefiniowaniu ilości adnotacji wystarczającej dla danej bazy danych, oraz najlepszego podzbioru obiektów do etykietowania.

Istnieje wiele scenariuszy wykorzystywanych do próbkowania w aktywnym uczeniu, w tym między innymi przedstawione na rysunku 7:

- uczenie selektywne (ang. *selective sampling*) w ramach, którego zakłada się, że uzyskanie nieoznakowanej instancji jest bezpłatne (lub niedrogie), więc może ona być najpierw próbkowana z rozkładu rzeczywistego, a następnie uczący się może zdecydować, czy skierować zapytanie. Takie podejście jest czasami nazywane strumieniowym (ang. *stream-based*) lub sekwencyjnym aktywnym uczeniem (ang. *sequential active learning*), ponieważ każda nieoznakowana instancja jest zazwyczaj pobierana pojedynczo ze źródła danych, a uczący się musi zdecydować czy kierować zapytanie czy odrzucić [45].
- uczenie oparte na puli (ang. *pool-based learning*) gdzie algorytmowi uczącemu udostępnia się zazwyczaj dużą pulę nieoznakowanych danych z możliwością zażądania etykietowania dowolnych próbek ze zbioru nieoznakowanego, w sposób interaktywny [49]. Zapytania mogą być losowane z puli, która jest zamknięta (tj. statyczna lub niezmienna), choć nie jest to konieczne [45]. Etykietowane próbki niewielkiego zbioru są najpierw używane do trenowania klasyfikatora (lub zespołu klasyfikatorów), a następnie próbki dużego zbioru nieoznakowanego są oceniane zgodnie z pewną wcześniej zdefiniowaną miarą informacyjności aby wybrać, która z nich powinna być przekazana jako zapytanie do etykietowania [50].



Rysunek 7 Schemat uczenia strumieniowego i opartego na puli

Celem selektywnego próbkowania jest zmniejszenie liczby próbek treningowych, które muszą być oznaczane etykietami, poprzez badanie obiektów, które nie są jeszcze oznakowane, i wybieranie tych, które mają największą wartość informacyjną do etykietowania. Główna różnica między aktywnym uczeniem strumieniowym a opartym na puli danych polega na tym, że pierwsze z nich skanuje dane sekwencyjnie i podejmuje decyzje dotyczące zapytań indywidualnie, w odniesieniu do każdej próbki, podczas gdy drugie ocenia i szereguje cały zbiór przed wyborem najlepszego zapytania [45]. W zakresie uczenia strumieniowego rozważana jest każda próbka z osobna. W uczeniu opartym na puli istnieje duży zbiór próbek, w którym są one rankingowane. W zależności od ich informacyjności do etykietowania wysyłane są próbki z jej poziomem, adekwatnym do przyjętej strategii. Scenariusz oparty na strumieniu może być bardziej odpowiedni w sytuacjach, gdy pamięć lub moc obliczeniowa są ograniczone.

Aktywne uczenie przebiega w rundach. W każdej rundzie model (działający w oparciu o dostępne dotychczas próbki oznaczone etykietą) jest wykorzystywany do oceny informacyjności nieoetykietowanych danych, które wybiera zgodnie z przyjętą strategią próbkowania. Najbardziej informacyjna próbka zostaje wybrana do etykietowania i po nim dołączona do danych treningowych. Model uczy się w oparciu o nowe dane treningowe, wzbogacone ostatnimi próbkami, które dołączyły. Proces zaczyna się od nowa i trwa dopóki jest to konieczne lub pozwalają na to posiadane zasoby.

W literaturze zaproponowano wiele sposobów formułowania strategii zapytań o próbki, zgodnie z przykładami opisanymi powyżej. Chociaż nie jest możliwe uzyskanie uniwersalnie dobrej strategii aktywnego uczenia się warto nadmienić, że istnieje wiele heurystyk, które okazały się skuteczne w praktyce. Dwa szeroko stosowane kryteria wyboru to informacyjność i reprezentatywność [51]. Informacyjność mierzy, jak dobrze nieoznakowana instancja pomaga zredukować niepewność modelu statystycznego, podczas gdy reprezentatywność mierzy, jak dobrze instancja pomaga reprezentować ogólne wzorce wejściowe nieoznakowanych danych, strukturę wzorców wejściowych [46], [51].

Większość algorytmów aktywnego uczenia wykorzystuje tylko jedno z dwóch kryteriów wyboru zapytania, co może znacząco ograniczyć ich wydajność. W szczególności, podejścia faworyzujące instancje informacyjne zazwyczaj nie wykorzystują struktury nieoznakowanych danych, co prowadzi do poważnego błędu próby i w konsekwencji do niepożądanej wydajności. Podejścia preferujące reprezentatywne instancje mogą być zmuszone do odpytywania stosunkowo dużej liczby instancji, zanim znajdą optymalną granicę decyzji [51].

1.1 Strategia niepewności

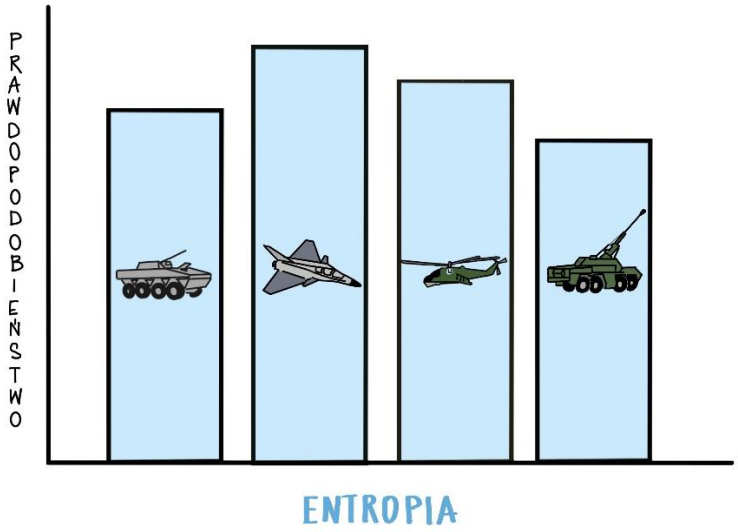
Literatura wskazuje, że najprostszą i najczęściej stosowanym podejściem do wyboru zapytań jest strategia niepewności *(ang. uncertainty sampling)*. Została opisana przez *David Lewis* i *William Gale* z *AT&T Bell Laboratories* [52]. W ramach tej strategii dobierane są próbki w zakresie, w którym model jest najmniej pewny (ang. *most uncertain*), jego poziom prawdopodobieństwa jest najniższy. Polega na wykorzystaniu tylko jednego klasyfikatora, który wskazuje klasę danej próbki i podaje wynik niepewności dla próbki danych, która nie posiada jeszcze etykiety. Kolejna próbka jest wybierana na podstawie oceny, w ramach której klasyfikator ma najmniejszą pewność [53].

Uncertainty może być mierzona w oparciu o:

a) Odległość od hiperpłaszczyzny (ang. *distance from the hyperplane*). W przypadku nieprobabilistycznych modeli uczących, takich jak maszyny wektorów nośnych (SVM), wybierane są przykłady, które są najbliżej hiperpowierzchni separującej [48].

b) Kryterium prawdopodobieństwa etykiety $P_\theta(y \mid x)$, dla modeli probabilistycznych, w ramach którego wyróżnia się następujące metody:

- Entropia [54], zgodnie z rysunkiem 8, reprezentuje ilość informacji potrzebnych do zakodowania rozkładu. W uczeniu maszynowym często jest uważana za miarę nieczystości.



Rysunek 8 Wizualizacja entropii
- wysoki poziom entropii świadczy o znaczącym zróżnicowaniu zbioru i trudno rozróżnialnych klasach

Jej wysoka wartość oznacza, że zbiór jest zmieszany, czyli pewność predykcji rozkłada się niejednoznacznie. Oznacza więc wysoką niepewność modelu, co do predykcji danej

próbki. Niska wartość entropii może być korzystna gdyż model rozpoznaje wyraźnie jedną klasę wśród innych.

$$x_{E=}^{*} \ \underset{x}{argmax} - \sum_{i} P_\theta(y_i|x) \ log_2 \ P_\theta(y_i|x) \tag{5}$$

gdzie:

x_E^* - najbardziej informacyjna instancja (najlepsze zapytanie), zgodnie ze strategią używającą entropii,

$\underset{x}{argmax} -$ – zbiór argumentów funkcji, dla których osiąga ona maksimum,

$P_\theta(y_i|x)$ – prawdopodobieństwo zajścia zdarzenia $y_i|x$

$log_2 P_\theta(y_i|x)$– logarytm dla binarnej jednostki entropii.

- Dla problemów z trzema lub więcej etykietami klas, bardziej ogólny wariant próbkowania niepewności może odpytywać instancję, której przewidywania są najmniej pewne (ang. *least confident*) [45]. Bierze pod uwagę tylko informacje o najbardziej prawdopodobnej etykiecie. W ten sposób algorytm odrzuca informacje o pozostałym rozkładzie etykiet.

$$x_{LC}^{*}= argmax_x \ 1 - P_\theta \ (\hat{y}|x) \tag{6}$$

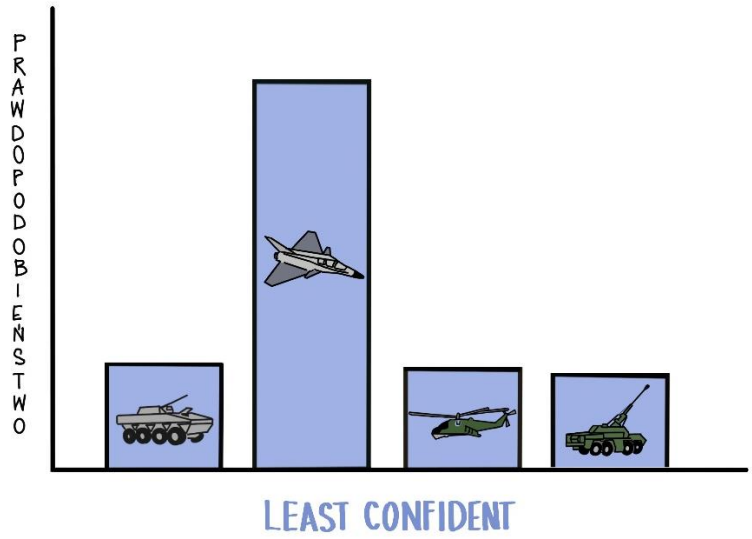
gdzie:

x_{LC}^*- najbardziej informacyjna instancja (najlepsze zapytanie), zgodnie ze strategią używającą *least confident,*

$argmax_x$ – zbiór argumentów funkcji, dla których osiąga ona maksimum,

$P_\theta \ (\hat{y}|x)$– prawdopodobieństwo zajścia zdarzenia y|x

$\hat{y}$ – etykieta klasy z najwyższym prawdopodobieństwem a posteriori w ramach modelu θ.



Rysunek 9 Wizualizacja metody least confident
- rozważa najbardziej prawdopodobną etykietę, nie rozpatrując pozostałych klas

Do etykietowania wybierana jest ta próbka danych *x**, co do których przewidywań model jest najmniej pewny.

- Jednak kryterium dla najmniej pewnej strategii bierze pod uwagę tylko informacje o najbardziej prawdopodobnej etykiecie. Aby to skorygować, niektórzy badacze używają innego wariantu wieloklasowego próbkowania niepewności zwanego próbkowaniem marginesu (ang. *margin sampling*) [55].

$$x^*_{SM} = argmin_x \, P_\theta(\hat{y}_1|x) - P_\theta(\hat{y}_2|x), \qquad (7)$$

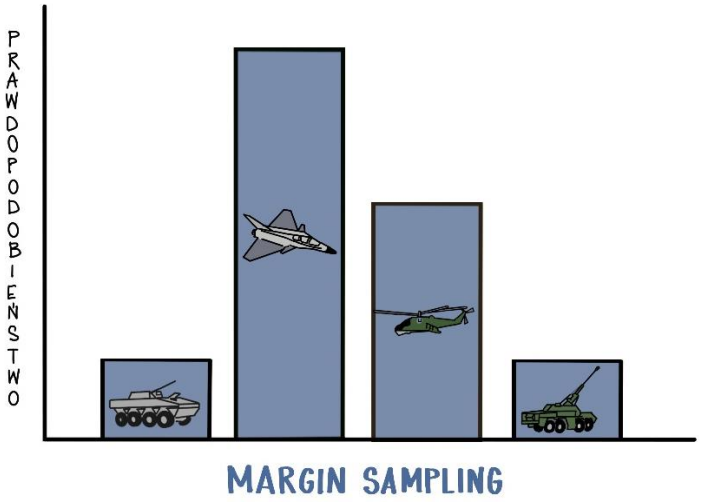
gdzie:

x^*_{SM} - najbardziej informacyjna instancja (najlepsze zapytanie), zgodnie ze strategią używającą *margin sampling*,

$argmax_x$ – zbiór argumentów funkcji, dla których osiąga ona maksimum,

$P_\Theta(y|x)$ – prawdopodobieństwo zajścia zdarzenia y|x

$\hat{y}_1$, $\hat{y}_2$ – odpowiednio pierwsza i druga najbardziej prawdopodobna etykieta klas w ramach modelu θ.



Rysunek 10 Wizualizacja metody margin sampling
- wskazuje dwie najbardziej prawdopodobne etykiety klas, czyli myśliwiec i śmigłowiec

gdzie $\hat{y}_1$ i $\hat{y}_2$ są odpowiednio pierwszą i drugą najbardziej prawdopodobną etykietą klasy w ramach modelu. Intuicyjnie, w przypadku wystąpienia dużych marginesów klasyfikator ma niewielkie wątpliwości w rozróżnianiu pomiędzy dwiema najbardziej prawdopodobnymi etykietami klas. Instancje z małymi marginesami są bardziej niejednoznaczne, więc znajomość prawdziwej etykiety pomogłaby modelowi skuteczniej rozróżniać między nimi. Jednakże, w przypadku problemów z bardzo dużymi zbiorami etykiet, przedmiotowe podejście nadal ignoruje znaczną część rozkładu wyjściowego dla pozostałych klas [45].

Metoda *margin sampling* została zaimplementowana w ramach eksperymentów realizowanych na potrzeby niniejszego opracowania.

W przypadku klasyfikacji binarnej, próbkowanie oparte na entropii sprowadza się do strategii *margin* i *least confident*. W rzeczywistości wszystkie trzy są równoważne zapytaniu o instancję z prawdopodobieństwem klasy najbliższym 0,5 [45].

Metoda wyznaczania próbek z wykorzystaniem kryterium niepewności nie unika problemu powtarzalności próbek dlatego też w celu zoptymalizowania wyboru próbek informacyjnych do strategii niepewności włączane jest kryterium różnorodności [56]. Różnorodność zapewnia, że wybrane próbki są niepodobne, co może prowadzić do redukcji redundancji informacji.

Istnieje również strategia aktywnego uczenia się agregująca strategię *uncertainty* ze strategią gęstości danych (ang. *density*) [57]. Działa ona najlepiej, gdy można pobierać większą liczbę nieoznakowanych próbek [58].

1.2 Strategia kierowania zapytania przez komitet (ang. *Query by Committee - QBC*)

W ramach algorytmu QBC [58], w pierwszej kolejności, tworzony jest komitet klasyfikatorów (C), w którym każdy ma indywidualne nastawienie do klasyfikacji. Komitet może być utworzony w drodze wyboru różnych modeli z rozkładu prawdopodobieństwa lub dzięki wykorzystaniu metod łączonych/zespołowych[9] (ang. *ensemble methods*), w skład których wchodzi najczęściej technika agregacji bootstrapów do tworzenia wielu różnych modeli z jednego zbioru danych treningowych (ang. *bagging*) lub technika tworzenia różnych modeli z rozkładu próbkowania zmieniającego się za każdym razem tak, aby coraz bardziej skupiać się na tej części danych treningowych, na której poprzednio uzyskana hipoteza wypadła słabo (ang. *boosting*) [59]. Modele uczą się w oparciu o zbiór aktualnych danych posiadających etykiety, a następnie głosują wyrażając poziom prawdopodobieństwa dla próbek na zbiorze danych nieoznaczonych. Do etykietowania zostaje wybrana próbka wobec której występuje największa różnica zdań między klasyfikatorami [58]. Stosując zatem strategię QBC należy optymalnie dobrać metodologię pomiaru niezgodności pomiędzy modelami. Najpowszechniejszą w wykorzystaniu jest *vote entropy*:

$$x_{VE}^{*} = \underset{x}{argmax} - \sum_{i} \frac{V(y_i)}{C} log \frac{V(y_i)}{C} \tag{8}$$

gdzie:

x_{VE}^{*}- najbardziej informacyjna instancja (najlepsze zapytanie), zgodnie ze strategią używającą *margin sampling,*

$\underset{x}{argmax}$ – zbiór argumentów funkcji, dla których osiąga ona maksimum,

y_i - określa wszystkie możliwe etykiety,

$V(y_i)$- oznacza liczbę głosów otrzymanych na etykietę y.

W pracy [60] zastosowano mechanizm QBC i połączono aktywne uczenie z tradycyjnym algorytmem maksymalizacji oczekiwań (ang. *Expectation-Maximization*)[10].

[9] Celem każdego problemu związanego z uczeniem się maszyn jest znalezienie odpowiedniego modelu, który najlepiej będzie przewidywał pożądane wyniki. Zamiast tworzyć jeden model i mieć nadzieję, że jest on najlepszym czy najdokładniejszym predyktorem, jaki można stworzyć, metody grupowania uwzględniają niezliczoną liczbę opcji i pozwalają na uśrednienie tych modeli celem wypracowania jednego, ostatecznego.
Powszechne jest używanie zestawów do głębokiego uczenia przez szkolenie różnorodnych i dokładnych klasyfikatorów. Różnorodność można osiągnąć dzięki zmianom w architekturze, ustawieniach parametrów i technikach szkoleniowych. Metody grupowania odniosły duży sukces w wyznaczaniu rekordowej wydajności na trudnych zbiorach danych i należą do grona zwycięzców konkursów Kaggle'a.
Za: https://geek.justjoin.it/ensemble-learning-czym-czym-polega, dostęp z dnia 30.04.2022.

[10] Algorytmy z rodziny *Expectation-Maximization* mają długą historię i nie są nowością w literaturze statystycznej. Natomiast w tej pracy EM jest stosowany do dokumentów nieoznakowanych zarówno po to, by pomóc

Eksperymenty pokazały poprawę w klasyfikacji. Stwierdzały również o potrzebie zastosowania jeszcze bardziej złożonych modeli mieszanych, które mogłyby lepiej odpowiadać rozkładom danych tekstowych.

W obszarze analizy obrazu opracowano algorytm zwany współtestowaniem [61]. Jest on podobny do algorytmu QBC i został zaprojektowany do stosowania w przypadku problemów z nadmiarowymi widokami lub problemów z wieloma rozłącznymi zestawami atrybutów (cech), które mogą być użyte do nauki atrybutu docelowego [53]. Początkowo użytkownik dostarcza kilka oznaczonych próbek oraz pulę instancji nieoznakowanych. Tworzony jest klasyfikator dla każdego widoku. Następnie klasyfikatory wskazują próbki nieoznakowane w wyniku czego definiowane są punkty sporne stanowiące próbki, co do których dwa klasyfikatory wskazały inaczej. W kolejnym kroku wybierany jest jeden z punktów spornych do oznaczenia, dodawany do zbioru treningowego i cały proces zostaje powtórzony. Dla każdego obiektu otrzymywana jest lista prawdopodobieństw, z których każde wskazuje na prawdopodobieństwo, że ten obiekt posiada jeden z atrybutów.

1.3 Strategia maksymalizacji oczekiwanej zmiany modelu (ang. *Expected Model Change Maximization - EMCM*)

Algorytm maksymalizacji oczekiwanej zmiany w modelu [48] powstał w celu zwiększenia efektywności aktywnego uczenia zarówno dla regresji liniowej, jak i nieliniowej. Stanowi rozwinięcie strategii oczekiwanej zmiany modelu (ang. *Expected Model Change*) [45], w której kluczowe jest wybranie takiej próbki z etykietą, której włączenie do modelu powoduje w nim największą zmianę [45].

$$x^*_{EGL} = \underset{x}{\operatorname{argmax}} \sum_i P_\theta(y_i|x) \; \| \nabla l_\theta(\mathcal{L} \cup \langle x, y_i \rangle) \| \tag{9}$$

gdzie:

x^*_{EGL} - najbardziej informacyjna instancja (najlepsze zapytanie), zgodnie ze strategią używającą *Expected Model Change*,

$\underset{x}{\operatorname{argmax}}$ – zbiór argumentów funkcji, dla których osiąga ona maksimum,

$P_\theta(y_i|x)$ – prawdopodobieństwo zajścia zdarzenia $y_i|x$,

y_i - określa wszystkie możliwe etykiety,

algorytmowi w wyborze dokumentów do etykietowania, jak i w celu zwiększenia dokładności przy użyciu dokumentów, które pozostają bez etykiet.

L - oznacza zbiór próbek etykietowanych,

$\nabla l_\theta(L)$ - oznacza gradient funkcji celu względem parametrów modelu θ,

$||\nabla l_\theta(L \cup (x, y_i))||$ - oznacza normę euklidesową nowego gradientu funkcji celu względem parametrów modelu θ, uzyskanego przez dodanie krotki szkoleniowej (x, y_i) do L.

Dla porównania warto spojrzeć na metodę k-średnich (ang. *k-means*), która przyporządkuje punkt do jednego z dwóch klastrów (ang. *hard-clustering*). W odróżnieniu od niej metoda EM obliczy prawdopodobieństwo, że dany punkt należy do jednego z dwóch klastrów, a zatem każda z próbek będzie cyfrą pomiędzy 0, a 1, odzwierciedlającą prawdopodobieństwo przyporządkowania do jednego z dwóch klastrów (ang. *soft-clustering*).

Algorytm EM jest używany do znalezienia lokalnych parametrów maksymalnego prawdopodobieństwa modelu statystycznego, w przypadku braku danych lub ich niekompletności. Algorytm EM podąża za krokami w celu znalezienia parametrów modelu w obecności zmiennych ukrytych. Zmiana modelu jest mierzona jako różnica między bieżącymi parametrami modelu a zaktualizowanymi parametrami po treningu. W tym celu wykorzystywany jest algorytm SGD (ang. *Stochastic Gradient Descent*) [62]. Zmiana jest obliczana, jako gradient straty względem próbki do ewentualnego wskazania [48].

Zakłada się, że prawdopodobieństwo będzie rosło z każdą iteracją algorytmu. Niemniej algorytm EM ma bardzo powolną zbieżność i następuje ona tylko do optimum lokalnego. Ograniczeniem tej metody jest wymaganie przez algorytm obliczenia zarówno prawdopodobieństwa wyprzedzającego, jak i wstecznego.

1.4 Strategia oczekiwanej zmiany redukcji błędu (ang. *Expected Error Reduction*)

Celem tej metody jest zmniejszenie przyszłego błędu generalizacji modelu, prowadzące do obniżenia poziomu niepoprawnych predykcji. Generalizacja umożliwiająca minimalizację błędu straty może przebiegać w oparciu o optymistyczny poziom straty i wnioskowanie pesymistyczne [63].

Formułą stosowaną w tym zakresie jest poniższy wzór:

$$x^*_{0/1} = \underset{x}{\operatorname{argmin}} \sum_i P_\theta(y_i|x) \left(\sum_{u=1}^{U} 1 - P_{\theta^{+<x,y_i>}}(\hat{y} \mid x^{(u)}) \right) \tag{10}$$

gdzie:

$x^*_{0/1}$ – minimalna oczekiwana strata 0/1,

$\underset{x}{\operatorname{argmin}}$ – zbiór argumentów funkcji, dla których osiąga ona minimum,

$P_\theta(y_i|x)$ – prawdopodobieństwo zajścia zdarzenia $y_i|x$,

y_i - określa wszystkie możliwe etykiety,

$\theta^{+<x,y_i>}$ - oznacza nowy model, który w każdej iteracji powinien być uczony od nowa z nowymi danymi <x, y_i>,

U - oznacza zbiór próbek nieoznaczonych,

$\hat{y}$ – etykieta klasy z najwyższym prawdopodobieństwem a posteriori w ramach modelu θ.

Przedmiotowa formuła jest przykładem potwierdzającym, że metody oparte na minimalizacji błędu wymagają zazwyczaj dużego wysiłku obliczeniowego [56]. Świadczy o tym nie tylko potrzeba prowadzenia obliczeń w pętli dostarczanych w każdej iteracji nowych danych, ale dodatkowo fakt potrzeby minimalizacji przyszłego błędu, stanowiącej kolejny wysiłek obliczeniowy.

Inną formułą obliczania poziomu błędu może być funkcja *log loss* przedstawiona wzorem 11:

$$x^*_{log} = \underset{x}{\operatorname{argmin}} \sum_i P_\theta(y_i|x) \left(-\sum_{u=1}^{U} \sum_j P_{\theta^{+<x,y_i>}}(y_j|x^{(u)}) \; log_2 P_{\theta^{+<x,y_i>}}(y_j|x^{(u)}) \right) \tag{11}$$

gdzie:

x^*_{log} – minimalna oczekiwana strata log-loss,

$\underset{x}{\operatorname{argmin}}$ – zbiór argumentów funkcji, dla których osiąga ona minimum,

$P_\theta(y_i|x)$ – prawdopodobieństwo zajścia zdarzenia $y_i|x$,

y_i - określa wszystkie możliwe etykiety,

$\theta^{+<x,y_i>}$ - oznacza nowy model, który w każdej iteracji powinien być uczony od nowa z nowymi danymi <x, y_i>,

U - oznacza zbiór próbek nieoznaczonych.

Metoda pozwala na optymalizację algorytmu i maksymalizację działania miar oceny, takich jak: dokładność, precyzja, czułość.

Powyższe algorytmy stosowane są niezależnie od rodzaju modelu, który zostanie wybrany. Natomiast ich implementacja jest praktykowana w przypadkach binarnej klasyfikacji i w takiej sytuacji ogranicza się do wyboru spośród dwóch etykiet, a złożoność czasowa obliczana jest parametrami: U (nieoznakowana etykieta), L (bieżący zbiór treningowy), G (liczba obliczeń gradientu). W przypadku zwiększenia liczby klas w zbiorze złożoność czasowa jest zwiększana o parametr M^2, gdzie M jest etykietą klasy i przedstawiana, jako ($M^2\ ULG$).

1.5 Variance Reduction

Istnieje kilka odmian metody redukcji wariancji, której celem jest niebezpośrednia minimalizacja wariancji wyniku działania algorytmu. Pozwala na zmniejszenie błędu, którego rozwiązanie może występować w formie zamkniętej pośrednio. Jednakże, metody te są nadal empirycznie znacznie wolniejsze niż prostsze strategie zapytań, takie jak próbkowanie niepewności [45].

1.6 Density Weighted Methods

Najbardziej informacyjna instancja w tym algorytmie będzie nie tylko zależna od miary niepewności, ale będzie rozważać również reprezentatywność danego rozkładu. Największą informacyjność w oparciu o miarę gęstości będzie miała instancja wynikająca z poniższego obliczenia:

$$x_{ID}^{*} = \underset{x}{\operatorname{argmax}}\, \emptyset_A\,(\mathrm{x})\ \mathrm{x} \left(\frac{1}{U} \sum_{u=1}^{U} sim(x, x^{(u)}) \right)^{\beta} \tag{12}$$

gdzie:

x_{ID}^{*}– najbardziej informacyjna instancja (najlepsze zapytanie), zgodnie ze strategią używającą metody gęstości,

$\underset{x}{\operatorname{argmax}}$ – zbiór argumentów funkcji, dla których osiąga ona maksimum,

y_i - określa wszystkie możliwe etykiety,

$\emptyset_A(\mathrm{x})$ - reprezentuje informacyjność x zgodną ze strategią zapytań A (taką jak próbkowanie niepewności lub podejście QBC),

$sim(x, x^{(u)})$ - podobieństwo do wszystkich innych instancji w rozkładzie wejściowym, otrzymanym ze zbioru próbek nieoznaczonych,

β – parametr sterujący udziałem gęstości.

Część wzoru reprezentowanego przez $\emptyset_A$ stanowi o niepewności (U) modelu, a x może uwzględniać różne jej metody, jak wyżej wymienione QBC lub US. Zadaniem parametru β jest kontrola informacji o gęstości mając na względzie zastosowaną funkcję $\emptyset_A\,(x)$.

2. Wielokryterialna metoda klasyfikacji obrazu

W pracy *Representative sampling for text classification using support vector machines* [64] badacze proponują metodę reprezentatywnego próbkowania, która wykorzystuje algorytm

k-średnich do grupowania danych w ramach marginesu klasyfikatora SVM i wybiera centroidy klastrów do etykietowania.

Wcześniejsze rozwiązania, które próbowały znaleźć balans pomiędzy badaniem niepewności próbki i jej reprezentatywności uwzględniały najczęściej wybór próbki z klastrów (ang. *cluster based approach*) [65] w początkowym zbiorze danych. Nie pracowały dynamicznie. Metoda zespołu *Barama* zakładająca już interaktywny dobór strategii próbkowania spośród trzech istniejących, w zależności od zbioru danych, dla których odbywał się trening skupiała się na wyborze, która metoda próbkowania jest optymalna dla danego zbioru danych, która strategia ma być użyta w każdej iteracji [66].

W metodzie powstałej przy współpracy naukowców *Carnegie Mellon University* z Pittsburga oraz *Microsoft* (2007) zaproponowano dynamiczne podejście dualne (***Du****al strategy for* ***A****ctive* ***L****earning* - *DUAL*), w którym parametry wyboru strategii są adaptacyjnie aktualizowane w oparciu o szacowaną przyszłą wartość redukcji błędu resztowego (ang. *future residual error reduction*) po każdym aktywnie próbkowanym punkcie [57]. Strategią DUAL wprowadzono schemat aktywnego uczenia w późniejszej części procesu, w miejsce tradycyjnych metod, które koncentrują się głównie na początkowym etykietowaniu zbioru danych. Badacze utworzyli taką kombinację próbkowania niepewności ważonej gęstością (ang. *density weighted uncertainty sampling*) i standardowego (jednolitego) próbkowania metodą *uncertainty*, żeby wykazać efektywność metody dla różnych domen oraz różnej wielkości zbiorów danych z etykietami [57].

Algorytmy doboru najlepszych próbek mogą działać w oparciu o wiele kryteriów. Dla przedstawienia algorytmu będącego przedmiotem tej pracy istotne jest określenie rodziny klasyfikatorów działających przez przechowywanie jawnej reprezentacji kategorii, w ramach którego model oblicza podobieństwo (ang. *similarity*) nowych wzorców z profilami klas przyporządkowując je do klas z wynikiem największego podobieństwa. Po utworzeniu profili klas modele wykorzystują funkcje dokonujące pomiaru podobieństwa wzorców do profili klasy. Najczęściej występujące funkcje podobieństwa stosowane do określania odległości zostały przedstawione wzorami 13, 14 i 15.

Odległość Minkowskiego (ang. *Minkowski distance*) jest metryką używaną do obliczania odległości między dwoma punktami w przestrzeni n-wymiarowej. Jest to uogólnienie różnych innych metryk, takich jak odległość Euklidesowa (przedstawiona wzorem 15) lub odległość Manhattan (przedstawiona wzorem 14). Odległość Minkowskiego opisuje

różnice między wartościami poszczególnych składowych wektorów i zależy od parametru *m*, który określa, jak bardzo należy uwzględniać różnice między składowymi.

$$d\ (x_{i,}\ x_j\ )\ =\ ||x_i - x_j||\ =\ \sqrt[m]{\sum_{t}^{|V|}\left(x_{i,t} - x_{j,t}\right)^m} \tag{13}$$

gdzie:

$d(x_{i,}\ x_j\ )$ – odległość i-tego oraz k-tego obiektu,

$|V|$- liczba badanych cech,

$x_{i,t}, x_{j,t}$ – realizacja cechy t na obiekcie i-tym oraz j-tym,

m – liczba naturalna, określająca rodzaj metodyki.

Odległość miejska (ang. *Manhattan distance* lub ang. *City-block*), to metryka używana do mierzenia odległości między dwoma punktami w przestrzeni euklidesowej. Jak sama nazwa wskazuje, jest używana w planowaniu urbanistycznym, gdzie jest brana pod uwagę przy projektowaniu układu ulic, rozmieszczeniu budynków i tworzeniu przestrzeni publicznych A ponadto wykorzystuje się ją powszechnie w innych dziedzinach, jak systemy nawigacji, projektowaniu obwodów drukowanych czy analizie tras transportowych.

$$d(x_i, x_j) = \sum_{t}^{|V|} |x_{i,t} - x_{j,t}| \tag{14}$$

gdzie:

$d(x_{i,}\ x_j\ )$ – odległość i-tego oraz k-tego obiektu,

$|V|$- liczba badanych cech,

$x_{i,t}, x_{j,t}$ – realizacja cechy t na obiekcie i-tym oraz j-tym.

Najbardziej popularna i najczęściej wykorzystywana do obliczeń odległości między punktami w przestrzeni euklidesowej jest właśnie odległość euklidesowa (ang. *Euclidean distance*). Z matematycznego punktu widzenia występuje, jako pierwiastek kwadratowy sumy kwadratów różnic między wartościami dla pozycji i domyślnie dla danych przedziałowych, co zostało przedstawione we wzorze 15. Z praktycznego punktu widzenia warto podkreślić jej powszechne zastosowanie w wielu dziedzinach, jak: geometria i nauki przyrodnicze, planowanie tras na potrzeby transportu samochodowego czy lotniczego, porównywanie i analiza sygnałów o różnych właściwościach, przetwarzanie obrazów (jak porównywanie

histogramów, wykrywanie podobieństwa między obrazami, segmentacja obrazu i innych technikach) oraz w analizie danych.

$$d\left(x_i, x_j\right) = \left\|x_i - x_j\right\| = \sqrt{\sum_{t}^{|V|}\left(x_{i,t} - x_{j,t}\right)^2} \tag{15}$$

gdzie:

$d(x_{i,}\, x_j\,)$ – odległość i-tego oraz k-tego obiektu,

$|V|$- liczba badanych cech,

$x_{i,t}, x_{j,t}$ – realizacja cechy t na obiekcie i-tym oraz j-tym.

Przedstawione powyżej miary służą do obliczania odległości między punktami w przestrzeni n-wymiarowej, biorąc pod uwagę różnice w składowych wektorów. Natomiast dla niniejszej pracy najbardziej istotna jest odległość kosinusowa, która służy do obliczania podobieństwa między wektorami cech, reprezentującymi obiekty w różnych dziedzinach. Może być stosowana w analizie obrazów, analizie danych biologicznych i wielu innych przypadkach, gdzie istnieje potrzeba porównywania podobieństwa między wektorami cech.

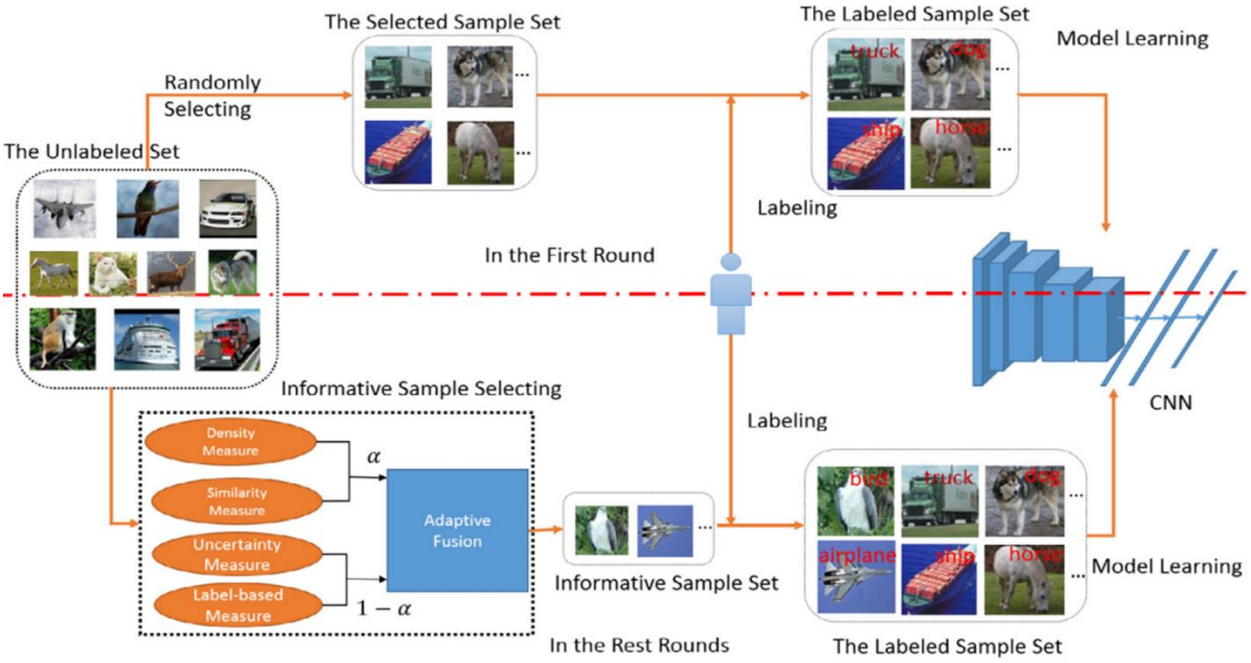
Odległość kosinusowa jest szczególnie przydatna w przypadku rzadkich wektorów cech, gdzie większość wartości w wektorach jest równa zero. Przez uwzględnienie tylko niezerowych wartości, odległość kosinusowa skupia się na istotnych aspektach danych i może dawać lepsze rezultaty niż inne metryki. Jest użyteczna, gdy dane są reprezentowane przez wektory w przestrzeni o niskiej wymiarowości i długościach porównywalnych z sobą.

Ponadto odległość kosinusowa mierzy kąt między dwoma wektorami, a nie ich długość. Zamiast porównywać wartości bezwzględne, jak w przypadku innych metryk, odległość kosinusowa ocenia podobieństwo kierunkowe między wektorami. To oznacza, że odległość kosinusowa jest bardziej odporna na różnice w skali danych.

Odległość kosinusowa jest zwykle używana jako miara podobieństwa między dwoma wektorami. Im bliżej wartości odległości kosinusowej jest do zera, tym bardziej wektory są podobne. Wyższa wartość oznacza większe podobieństwo, a niższa wartość oznacza większą różnicę.

Zastosowanie pojęcia odległości zostanie opisane w dalszej części rozdziału z uwagi na znaczące wykorzystanie jego praktycznego wymiaru w pracy badaczy Uniwersytetów z *Hunan* i *Shandong* w Chinach oraz *Hewlett Packard Enterprise* z Singapuru, którzy zaprezentowali

wielokryterialną metodę klasyfikacji obrazów (*MCADL*) w trybie uczenia aktywnego z wykorzystaniem sieci neuronowych [56].



Rysunek 11 – Schemat działania metody MCADL., na podstawie [2]

Jak widać na rysunku 11 w metodzie MCADL, zakres początkowego zestawu próbek jest w eksperymentach ustalany ręcznie. W pozostałych rundach, model CNN (ang. *Convolutional Neural Network*) jest stosowany do oceny próbek z puli nieoznakowanej. Następnie strategia próbkowania wybiera najbardziej informacyjne próbki do etykietowania przez użytkowników z nieoznakowanego zbioru poprzez adaptacyjną integrację informacji zgodnie z miarą gęstości, podobieństwa, niepewności i opartą na etykiecie. W kolejnym kroku, model CNN jest aktualizowany. Proces ten powtarza się do momentu, aż zbiór bez etykiet jest pusty lub wydajność jest satysfakcjonująca.

MCADL wykorzystuje miary *gęstości* (ang. *density*) i *podobieństwa* (ang. *similarity*) do redukcji redundancji informacji oraz uzyskuje informacje z nieoznakowanych próbek w oparciu o *uncertainty* i miarę opartą na etykietach (ang. *label-based measure*). Celem jest przyspieszenie zbieżności modelu dzięki wykorzystaniu miary niepewności oraz poprawy wydajności modelu dzięki zastosowaniu miary opartej na etykietach. Wybrane próbki informacyjne są wprowadzane do modelu CNN w celu aktualizacji parametrów i uzyskania wyższej wydajności [56]. Wykorzystanie miary niepewności dostosowuje granicę decyzji poprzez próbkowanie z regionów, w których klasyfikator jest najmniej pewny, niezależnie od gęstości nieoznaczonych danych.

Podsumowując sposób doboru kryteriów przedstawionych w metodzie MCADL naukowcy skoncentrowali prace na dwóch głównych grupach kryteriów:

1. Pierwsza grupa, dokonująca pomiaru informacyjności próbek z etykietami z wykorzystaniem miar *gęstości* i *podobieństwa* (gdzie praktyczność tych strategii okazała się ograniczona z uwagi na cechy próbek ze zbioru danych MNIST, które nie różnią się wizualnie w sposób znaczący między sobą).
   Miara badająca gęstość dobrze sprawdza się przy minimalnej ilości danych z etykietą, ponieważ próbkuje z regionów o maksymalnej gęstości próbek nieoznaczonych etykietami, a tym samym pomaga ustalić początkową granicę decyzji, tam gdzie ma ona największy wpływ na pozostałe nieoznakowane dane [57]. W metodzie MCADL miara gęstości wskazuje na bliskość próbek. Duże zagęszczenie (ang. *high density*) próbek (x_i) wskazuje na redundancję informacji i marginalną informacyjność. Niski poziom zagęszczenia może wskazywać na wysoki poziom informacyjności z uwagi na niski poziom powtarzalności informacji:

$$Inf^{Den}(x_i|D_L) = 1 - \frac{1}{|D_L^S|}\sum_{x_j \in D_L^S} Cosdis(x_i, x_j) \tag{16}$$

gdzie:

$Inf^{Den}(x_i|D_L)$ –informacyjność dla kryterium gęstości ,
s - pseudo-etykieta x_i nadana przez model CNN,
D_L^S - zbiór próbek z klasy s należącej do zbioru D_L ,
Cosdis(...) - metryka odległości kosinusowej próbek.

Miara *similarity* działa podobnie, ale w tym zakresie liczona jest maksymalna odległość pomiędzy próbkami. Im większa jest odległość między próbkami, tym podobieństwo pomiędzy nimi jest mniejsze i wzrasta informacyjność zbioru. Miara wskazuje na różnorodność zbioru.

$$Inf^{Simi}(x_i|D_L) = 1 - \max_{x_j \in D_L^S} Cosdis(x_i, x_j) \tag{17}$$

gdzie:

$Inf^{Sim}(x_i|D_L)$ – informacyjność dla kryterium podobieństwa
s - pseudo-etykieta x_i nadana przez model CNN,
D_L^S - zbiór próbek z klasy s należącej do zbioru D_L ,
Cosdis(...) - metryka odległości kosinusowej próbek.

W obydwu powyższych przypadkach niskie wartości miar wskazują na preferencję doboru próbki. Wynika to z charakteru przyjętej miary kosinusowej, w której im większa odległość próbek między sobą (im większy kąt), tym większe prawdopodobieństwo, że model nie posiada wiedzy na temat danej instancji i wymaga ona sprawdzenia.

Warto w tym zakresie dodać, iż istnieją konkretne korzyści wynikające z połączenia tych miar, które przyczyniły się do dalszej ich eksploracji w ramach niniejszej pracy. Są to między innymi:

a) Możliwość dokonywania pełniejszej oceny danych. Miara gęstości dostarcza informacji na temat rozkładu danych, co może być przydatne w analizie zmienności lub koncentracji danych. Z drugiej strony, miara podobieństwa ocenia, jak bardzo dwa obiekty lub próbki są do siebie podobne. Połączenie tych dwóch podejść pozwala na kompleksową ocenę danych, uwzględniając zarówno rozkład jak i podobieństwo.
b) Połączenie miar gęstości i podobieństwa może pomóc w identyfikacji anomalii lub nietypowych wzorców w danych. Można porównać odległości między obiektami względem ich rozkładu (miara gęstości) oraz między obiektami względem siebie nawzajem (miara podobieństwa). To podejście pozwala na wykrywanie zarówno rzadkich wystąpień danych, jak i obiektów o nietypowym wzorcu podobieństwa.
c) Na podstawie oceny rozkładu i podobieństwa między obiektami można przyporządkować obiekty do określonych klas lub utworzyć grupy danych o podobnych właściwościach. Te podejścia mogą być szczególnie przydatne w zadaniach takich jak klasyfikacja obrazów, segmentacja danych czy analiza skupień.
d) Połączenie miar gęstości i podobieństwa może być stosowane do redukcji wymiarowości danych. Poprzez ocenę podobieństwa między obiektami, można zidentyfikować i wyeliminować zbędne lub redundantne cechy, co prowadzi do bardziej zwięzłego i efektywnego reprezentowania danych.

2. Druga grupa, wykonująca obliczenia informacyjności nieoznakowanych próbek w odniesieniu do modelu, z wykorzystaniem miary niepewności (ang. *uncertainty sampling*) w zakresie, której zapytaniu podlegają instancje objęte największą niepewnością co do etykiety, która powinna im być nadana, umożliwiającej przyspieszenie zbieżności modelu CNN i miary opartej na etykietach (ang. *the label-*

based measure), używanej do wyboru najbardziej efektywnych etykiet oraz do zapobiegania nierównowadze wyników wśród klas [56].

Do przedstawienia kryteriów miary niepewności przyjęto w niniejszym opracowaniu założenia, że klasyfikator został wytrenowany na dostępnych danych zbioru α, a po treningu klasyfikator może podać prawdopodobieństwo $P_\theta(y_i|x)$ dla modelu θ tak, że dane x ∈ μ pochodzą z klasy y_i, gdzie y_i obejmuje wszystkie możliwe etykiety klas. W zakresie miary niepewności autorzy metody MCADL zdecydowali o jej modyfikacji i zaproponowali wzór 18.

$$Inf^{Unc}(x_i|M) = 1 - \frac{1}{K}\sum_{k=1}^{K}|P(C_k|x_i;\ M) - \ Avg_K(x_i|M)| \tag{18}$$

gdzie:

$Inf^{Unc}(x_i|M)$ – miara niepewności,

$P(C_k|x_i;\ M)$ - prawdopodobieństwo a posteriori nieznakowanej próbki x_i należącej do klasy C_k zgodnie z modelem M,

$Avg_K(x_i|M)$ - średnia liczba najwyższych K klas prawdopodobieństwa.

Wartość K jest obliczana, gdy suma prawdopodobieństw klas K jest większa od 0,5.

Miara oparta na etykietach dąży do wybierania dwóch rodzajów próbek. Pierwszy typ to próbki z klas, które odnotowały szybką poprawę wydajności w ostatnim czasie. Te próbki wykazują potencjał do przyspieszenia poprawy wydajności modelu CNN. I te próbki będą używane do tego, żeby osiągnąć równowagę wydajności pomiędzy klasami. Wzmocnią klasy najgorzej rozpoznawane - klasy, które wykazują niską wydajność.

$$Inf^{Lab}(x_i|M) = W_t^S \tag{19}$$

gdzie:

$Inf^{Lab}(x_i|M)$– informacyjność dla kryterium opartego na etykietach

W_t^S – miara dla klasy S w rundzie t. Miarę wylicza się według wzoru 20.

$$w_t^m = \begin{cases} \max\left(0, \dfrac{(AR_t^m - AR_{t-1}^m)}{Z_1}\right) & \min AR_t^m < b \\ \dfrac{1/AR_t^m}{Z_2} & \min AR_t^m \geq b \end{cases} \tag{20}$$

gdzie:

AR_t^m - dokładnością klasyfikacji m-tej klasy według modelu M w rundzie t

Z_1, Z_2 - współczynniki normalizacji,

b – przyjęta wartość progowa.

Połączenie miary niepewności i miary opartej na etykietach niesie za sobą konkretne korzyści w kontekście analizy danych i uczenia maszynowego. Najważniejsze z nich można podsumować następująco:

a) Miara oparta na etykietach mierzy stopień zgodności predykcji modelu z rzeczywistymi etykietami. Jest to szczególnie przydatne w przypadku posiadania ograniczonej liczby danych oznaczonych. Jednak pozyskanie etykiet może być kosztowne i czasochłonne. Wykorzystując miarę niepewności, można skupić się na tych przypadkach, w których model jest najbardziej niepewny lub ma największe trudności w dokładnym przewidywaniu etykiety. Dzięki temu można efektywniej wykorzystać dostępne zasoby danych oznaczonych, skupiając się na tych przypadkach, które są najbardziej wartościowe dla procesu uczenia maszynowego.
b) Miara niepewności wskazuje na przypadki, w których model ma największe trudności w dokładnym przewidywaniu etykiet. Wykorzystując tę miarę w połączeniu z miarą opartą na etykietach, można skupić się na błędach klasyfikacji, które mają największe znaczenie. Można skierować uwagę na te przypadki, które są najbardziej trudne dla modelu i wymagają dalszej analizy lub poprawek w procesie uczenia.
c) Miara niepewności dostarcza informacji o stopniu pewności modelu w przewidywaniu etykiet. To może być przydatne w wielu scenariuszach, takich jak rozpoznawanie obrazów medycznych czy klasyfikacja wiadomości. Połączenie miary niepewności z miarą opartą na etykietach pozwala na lepsze zarządzanie niepewnością w procesie decyzyjnym. Można zidentyfikować przypadki, w których model ma największe trudności w przewidywaniu etykiety, jednocześnie biorąc pod uwagę informacje o zgodności predykcji z rzeczywistymi etykietami.
d) Połączenie miary niepewności i miary opartej na etykietach może pomóc w selekcji przykładów, które wymagają dalszej analizy lub interwencji. Można skupić się na tych przypadkach, które są zarówno trudne dla modelu (według miary niepewności) i mają istotne znaczenie z punktu widzenia zgodności z rzeczywistymi etykietami (według miary opartej na etykietach). Umożliwia to właściwą interwencję w procesie uczenia, co powoduje wzrost efektywności tego procesu.

Obok precyzyjnie zdefiniowanych kryteriów w metodzie MCADL wykorzystano ważenie kryteriów parametrami α i β. Przyjęto założenie, że na początku treningu model jest mało

wiarygodny i w związku z tym nacisk został położony na kryteria oparte na próbkach, a nie na modelu. Dlatego też parametr α ma na początku wyższą wartość podkreślając wagę tych metryk. *Density* i *similarity* pracują na próbkach z etykietami. Natomiast w związku z faktem, że każda z metod się w pewnym momencie wyczerpuje, a jednocześnie model stopniowo się poprawia i uzyskuje coraz lepsze wyniki to efekt miar *density* i *similarity* zmniejsza się i następuje stopniowa redukcja wagi α. Im dokładność (ang. *accuracy*) dla modelu staje się większa, tym waga α uzyskuje mniejszą wartość. Obliczanie dokładności odbywa się w odniesieniu do każdej klasy modelu, dzięki czemu podbijane są te próbki, które należą do klasy gorzej rozpoznawanej.

W celu przedstawienia charakteru, natury i zachowania algorytmu w odniesieniu do każdego kryterium dokonano wizualizacji graficznej odzwierciedlającej działanie każdego z kryterium z osobna, o czym napisano w rozdziale IV. Ponadto dokonano wizualizacji prezentującej zbieżność funkcji straty w miarę uczenia się modelu. Funkcja straty (ang. *loss function*) to funkcja o wartości rzeczywistej z dwoma parametrami:

- rozkładem prawdopodobieństwa w klasach K_1, K_2, …K_n

- liczbą całkowitą od 1 do *n* wskazującą prawdziwą klasę instancji

Jeśli dana jest instancja $\epsilon\ I$, a h(i) to rozkład prawdopodobieństwa obliczany przez klasyfikator i n (i) to prawdziwa wartość instancji I, to mając na względzie funkcję straty δ, błąd prawdziwy w odniesieniu do δ wynosi:

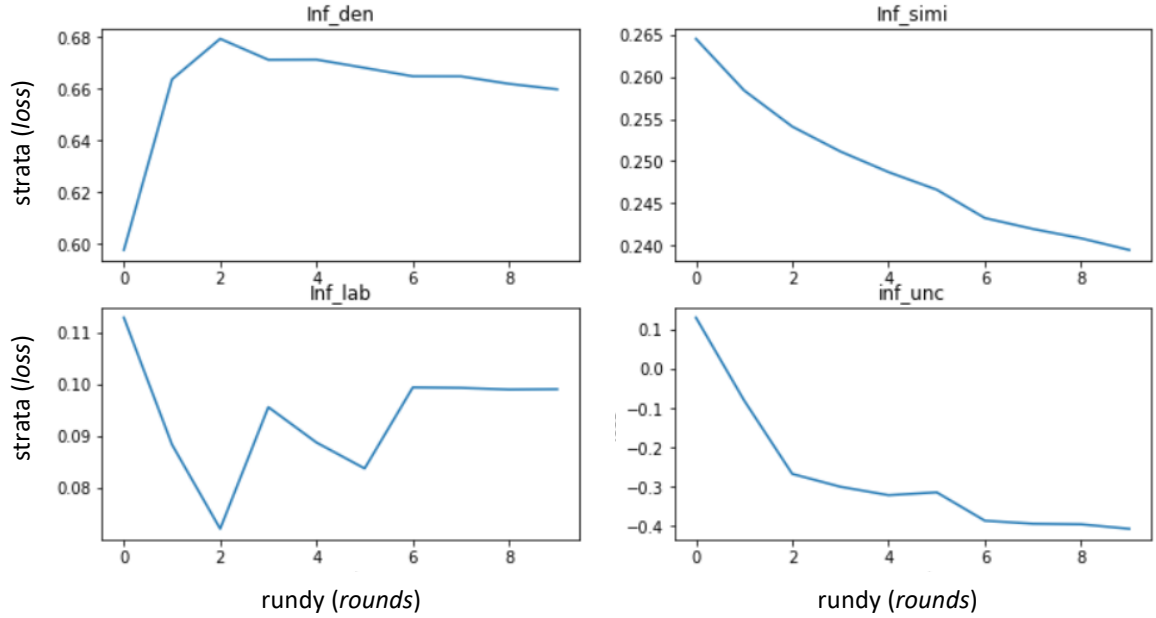
$$\text{błąd}_I\ (\text{h}) = \frac{1}{I} \sum_{i \in I} \frac{\delta\left(\text{h}(I),\ \text{K}(i)\right)}{\text{n}} \tag{21}$$

gdzie średnia jest obliczana dla rozkładu prawdopodobieństwa *I*.

Funkcja straty służy jako miara, która informuje model o tym, jak dobrze radzi sobie z danym zadaniem. Poprzez minimalizację funkcji straty, model dąży do osiągnięcia optymalnych parametrów, które maksymalizują jego zdolność do dokonywania poprawnych predykcji. Dzięki temu funkcja straty umożliwia optymalizację modelu w procesie uczenia.

W odniesieniu do miary gęstości (na rysunku 12 oznaczona, jako inf_den) funkcja straty rośnie w pierwszych rundach, ale na późniejszym etapie jej poziom systematycznie maleje. W przypadku tej miary początkowy wzrost jest najwyższy. Inaczej wygląda proces zbieżności błędu straty z kryterium zależnym od etykiet (na rysunku 12 oznaczonym, jako inf_lab), gdzie funkcja straty maleje w trakcie pierwszych rund, ale potem rośnie i nie zachowuje się stabilnie.

W przypadku kryteriów podobieństwa i niepewności (na rysunku 12 oznaczone stosownie, jako inf_simi oraz inf_unc) funkcja straty nie osiąga tak wysokiego poziomu i zawsze maleje od pierwszej rundy, co daje właściwą zbieżność funkcji straty z modelem. W zakresie kryterium niepewności poziom błędu straty osiąga poziomy ujemne.

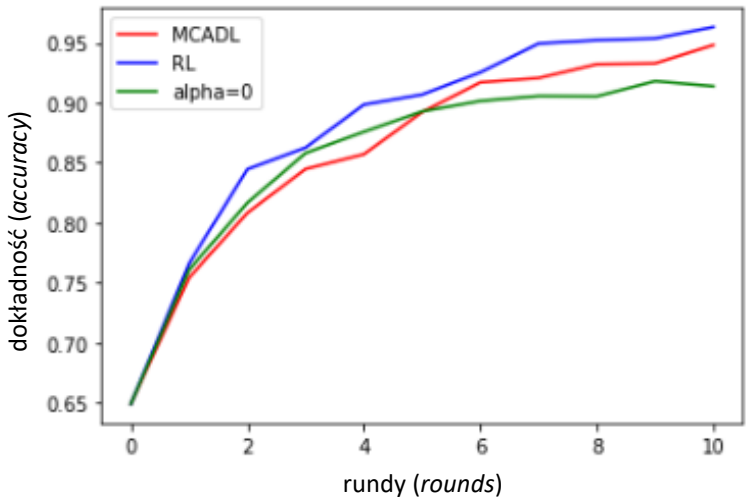


Rysunek 12 Interpretacja geometryczna funkcji straty dla każdego z czterech kryteriów

Każde z kryteriów posługuje się odrębnym mechanizmem, więc pomimo stosowania ich w ramach jednego modelu i w odniesieniu do tego samego poziomu prawdopodobieństwa dla tych samych instancji, wynik funkcji straty dla każdego z nich zachowuje się różnie. Nie mniej dla kryteriów podobieństwa i niepewności występuje właściwa konwergencja pomiędzy poziomem błędu straty, którego wartość maleje w miarę uczenia się modelu natomiast można stwierdzić, że dla pozostałych dwóch kryteriów powinna być zastosowana inna funkcja błędu.

W zakresie algorytmu, odtworzono metodę MCADL w środowisku *Tensorflow*. Dla sprawdzenia działania algorytmu przeprowadzono eksperymenty porównawcze i zestawiono:

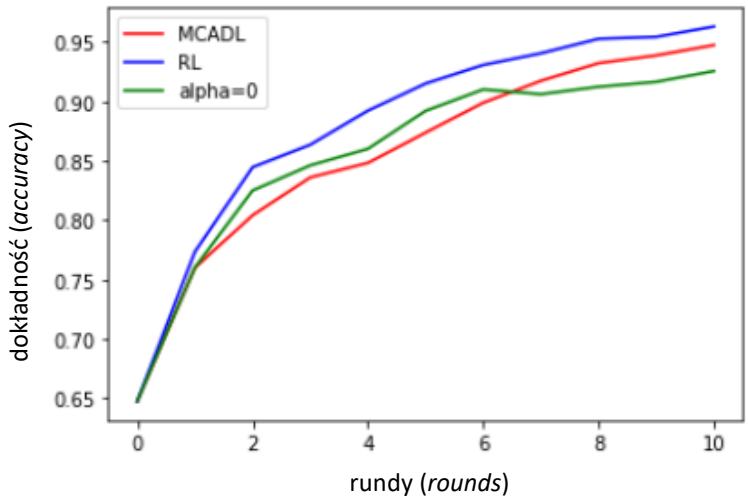
- Metodę główną MCADL, zaimplementowaną 1:1 (na wykresach oznaczoną: MCADL).
- Metodę główną MCADL, w której $\alpha = 0$, co oznacza, że informacyjność jest obliczana tylko w ramach istniejącego modelu, a miary oparte o próbki mają wagę = 0 (na wykresach oznaczoną: alpha =0), a zatem nie posiadają żadnego wzmocnienia i mogą być traktowane przez model, jako mniej ważne.
- Metodę losową (na wykresach oznaczoną skrótami RL, RD).



Rysunek 13 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz metody losowej (RL).

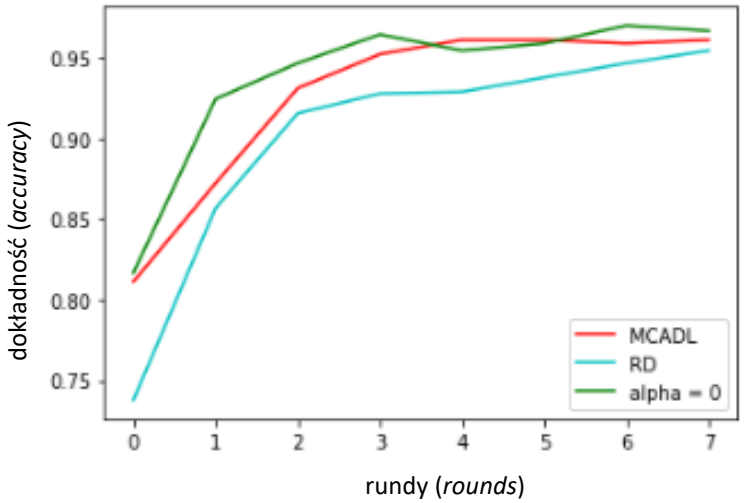
Na kilkadziesiąt eksperymentów wykonanych na bazie MNIST, niespodziewanie metoda MCADL w około 80% nie dawała najlepszego wyniku lub jej wynik był minimalnie lepszy, co przedstawiają przykładowe wykresy na rys. 13 – 16.

Na rys. 13 dokładność metody MCADL jest wysoka, ale minimalnie gorsza niż w metodzie losowej i w ostatnich rundach minimalnie lepsza niż zmodyfikowana metoda MCADL, w której waga alpha przyjmuje wartość „0", a zatem kryteria gęstości i podobieństwa (które pracują w oparciu o etykietowane próbki) mają niskie oddziaływanie.



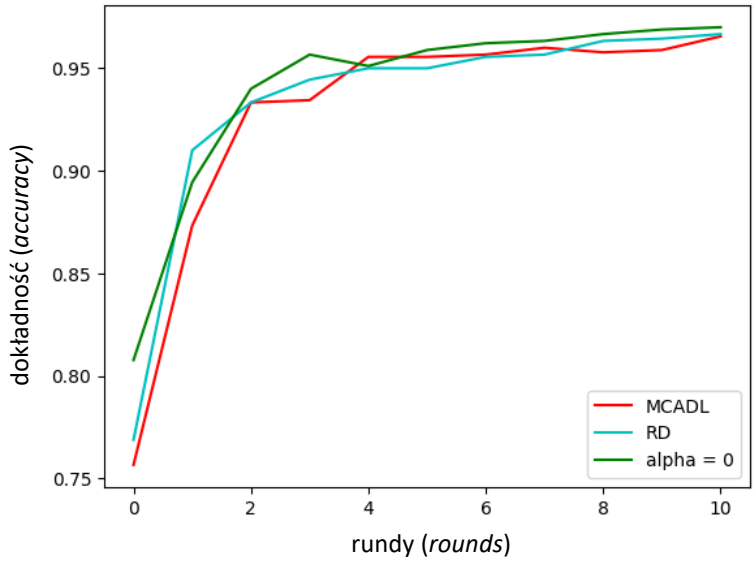
Rysunek 14 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz metody losowej (RL).

Na rys. 14 dokładność metody MCADL jest również wysoka, ale jej wynik w odniesieniu do metody losowej lub zmodyfikowanej metody MCADL, z wagą „0” dla kryteriów niepewności i gęstości wygląda podobnie, jak na rys. 13.



Rysunek 15 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz metody losowej (RD).

Na rys. 15, w zestawieniu z pozostałymi metodami, metoda MCADL zadziałała najbardziej stabilnie, gdyż jej przebieg pozycjonuje się od początku na wysokim poziomie i po osiągnięciu ponad 95% poziomu dokładności pozostaje płaski. Widać też, że trend jej wzrostu jest porównywalny do wyniku metody, w której waga dla kryteriów podobieństwa i gęstości przyjmuje wartość „0” oraz metody losowej.



Rysunek 16 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz metody losowej (RD)

Na rys. 16, w zestawieniu z pozostałymi metodami, metoda MCADL działa analogicznie do pozostałych, pozostając na wysokim poziomie, ale nie wyróżniając się zasadniczo w żaden sposób. Jak w większości przypadków pozostaje minimalnie gorsza niż pozostałe metody.

Podsumowując, metoda MCADL osiąga wysoką dokładność, ale nie jest najlepsza w porównaniu do innych metod. Istnieje możliwość zmodyfikowania metody poprzez zmianę wagi alpha dla kryteriów niepewności i gęstości, co może wpływać na wynik. Analiza funkcji straty dla różnych kryteriów oraz przeprowadzone eksperymenty wskazują, że istnieją różnice w skuteczności poszczególnych kryteriów w kontekście funkcji straty i wyników modelu.

Oprócz odtworzenia metody MCADL w środowisku *Tensorflow* (autorzy metody MCADL dokonali implementacji w *Tensorflow*), przeprowadzono własną implementację w *Pytorch*, której wyniki zostaną przedstawione w rozdziale III.

3. Charakterystyka sieci neuronowej

Sieć neuronowa to rodzaj modelu matematycznego lub algorytmu zbudowanego na podstawie inspiracji biologicznym działaniem mózgu. Jest to struktura składająca się z połączonych ze sobą sztucznych neuronów (lub węzłów), które przetwarzają dane wejściowe, przekazując sygnały przez wagi połączeń między nim. Neurony są zorganizowane w warstwy, które mogą być połączone w sposób sekwencyjny (warstwy jedna po drugiej) lub w bardziej skomplikowane struktury.

Każdy sztuczny neuron otrzymuje sygnały wejściowe, które są mnożone przez wagi (parametry sieci), a następnie sumowane. Do sumy może być również dodawany *bias*[11], a wynik jest przekazywany przez funkcję aktywacji. Funkcja aktywacji jest stosowana, aby wprowadzić nieliniowość do działania sieci neuronowej i umożliwić jej modelowanie bardziej złożonych relacji. Podczas procesu uczenia sieć neuronowa dostosowuje wagi i przesunięcia w celu minimalizacji funkcji straty. Jest to realizowane za pomocą algorytmów optymalizacji, takich jak propagacja wsteczna (ang. *backpropagation*), które aktualizują parametry sieci na podstawie gradientu funkcji straty.

Sieć neuronowa, na podstawie cyfrowej reprezentacji obrazu, dokonuje klasyfikacji obiektów, które się na nim znajdują. Wprowadza formy prostszej reprezentacji. Umożliwia maszynie zbudowanie własnej wiedzy na podstawie form uzyskanych dzięki podzieleniu obrazu

[11] *Bias* stanowi ważny element modelowania w sieciach neuronowych, umożliwiając modelom elastyczne dostosowywanie się do różnych danych i problemów, a także poprawę wydajności i skuteczności modelu. W uproszczeniu, bias określa, jak bardzo aktywacja neuronu powinna przesunąć się w kierunku pozytywnym lub negatywnym bez względu na wejścia. Jest to wartość dodawana do sumy ważonych wejść neuronu przed przepuszczeniem jej przez funkcję aktywacji.

na warstwy, w których każda zawiera inne odwzorowania. W warstwach ukrytych, w odróżnieniu od warstwy wejściowej, model sam określa, które pojęcia są użyteczne do wytłumaczenia związków w obserwowanych danych [31]. W procesie analizy, sieci odkrywają poszczególne cechy poprzez znalezienie wzorów między pikselami na rosnących poziomach abstrakcji, używając milionów drobnych obliczeń na każdym poziomie. Nowe obrazy są poddawane procesowi, który ma dopasować ich cechy do wyuczonych wzorców.

Najsłynniejsze architektury sieci powstały w drugiej dekadzie XXI wieku.
Jednakże jedną z pierwszych, które dały bardzo dobre wyniki była sieć *LeNet (1998)* zaprojektowana przez zespół naukowców z trzech uniwersytetów (ang. *University of Toronto, University of Montreal, New York University*) pod przewodnictwem *Yanna LeCuna*. Schemat uczenia się tej sieci oparty jest na gradiencie[12] i został zastosowany z sukcesem w automatycznym rozpoznaniu cyfr pisanych odręcznie. Sieć należy do kategorii małych i prostych. Składa się z 7 warstw: 3 warstw konwolucyjnych, 2 warstw uśredniających (ang. *subsumpling*) i 2 warstw w pełni połączonych (ang. *full connection*). Sieć *AlexNet (2012)* miała podobną do *LeNet* architekturę, ale była głębsza, z większą ilością filtrów w ramach poszczególnych warstw.
Ponadto stosowała *max pooling*, *dropout*, augmentację danych, aktywację ReLU, SGD z momentem. Autorzy *AlexNet* udowodnili, że sieć neuronowa składająca się tylko z 5 warstw konwolucyjnych i 3 w pełni połączonych może efektywnie i dokładnie klasyfikować obrazy.

Tabela 1 Wyniki działania sieci neuronowych [17]

SIEĆ	ROK	TOP-5 DOKŁADNOŚĆ	TOP-5 POZIOM BŁĘDU	LB. PARAMETRÓW
LeNet	1998	Nie dotyczy	Nie dotyczy	60 tys.
Alexnet	2012	84.70%	15,3%	62 mln
VGGNet	2014	92.30%	7.3%	138 mln
GoogLeNet	2014	93.30%	6.67%	6.4 mln
ResNet	2015	95.51%	3.6%	60.3 mln

Należy podkreślić, iż zróżnicowanie zbioru zdjęć i obiektów na których pracowała sieć było dużo większe niż wykorzystany przez *LeNet* zbiór ręcznie pisanych cyfr (MNIST)[13]. Trening sieci *AlexNet* został przeprowadzony z wykorzystaniem dwóch kart graficznych GTX 580 z pamięcią 3 GB. Paralelizacja wykorzystania GPU i trening rozproszony to techniki, które są do dziś często

[12] Metoda gradientu służy w sieciach neuronowych do znajdowania minimum funkcji, w celu dokonania zmian wag w taki sposób, by poziom błędu sieci się obniżał. Nachylenie wykresu w punkcie odpowiadającym aktualnym wartościom wag, dane jest przez gradient, czyli wektor pochodnych cząstkowych.
[13] *AlexNet* klasyfikowała na zbiorze 1.2 miliona obrazów treningowych, 50.000 obrazów walidacyjnych i 150.000 obrazów testowych [20, s. 85].

stosowane. *LeNet* była inspiracją również dla *GoogLeNet (2014)*, ale ta składa się z 22 warstw. Zredukowano w niej liczbę parametrów z 60 milionów (AlexNet) do 6,4 milionów.

GoogLeNet wprowadziła innowacyjne rozwiązanie w postaci modułów incepcyjnych. *ResNet* (2015) natomiast posiada połączenia rezydualne. Najbardziej obciążająca obliczeniowo jest sieć *VGGNet* (2014), gdyż składa się aż ze 138 mln parametrów. *AlexNet* i *ResNet*, obie mają około 60 milionów parametrów, ale różnica w ich dokładności w pierwszej piątce wynosi około 10%. Należy jednak zwrócić uwagę, iż trening *ResNet* wymaga wielu obliczeń, około 10 razy więcej niż w przypadku *AlexNet*.

Podsumowując, sieci takie jak *AlexNet, GoogLeNet, VGGNet i ResNet*, zazwyczaj osiągają wyższą skuteczność klasyfikacji w porównaniu do *LeNet*, która jest bardziej podstawową siecią. Sieci głębokie, takie jak *GoogLeNet, VGGNet i ResNet*, są bardziej złożone obliczeniowo i mają większą liczbę parametrów w porównaniu do *LeNet* i *AlexNe*t. Sieci te wymagają większych zasobów obliczeniowych i mocy obliczeniowej do treningu i testowania. Sieci takie jak *GoogLeNet* wprowadzają innowacyjne moduły *Inception*, które pozwalają na równoczesne przetwarzanie obrazu na różnych skalach. *ResNet* wprowadza połączenia skip, które umożliwiają przekazywanie informacji z jednej warstwy do innych, co pomaga w radzeniu sobie z problemem zanikającego gradientu i pozwala na zwiększenie efektywności treningu.

Tabela 2 Architektury zaprojektowane dla metody MCADL

Architektura CNN dla MNIST

Warstwa	Rodzaj	Input	Kernel	Stride	Output
dane	input	1 x 28 x 28	n/d	n/d	1 x 28 x 28
conv1	convolution	1 x 28 x 28	3 x 3	1	32 x 26 x 26
conv2	convolution	32 x 26 x 26	3 x 3	1	64 x 24 x 24
pool3	max pooling	64 x 24 x 24	2 x 2	2	64 x 12 x 12
fc4	fully connected	64 x 12 x 12	1 x 1	1	128 x 1 x 1
fc5	fully connected	128 x 1 x 1	1 x 1	1	10 x 1 x 1

Architektura CNN dla CIFAR-10

Warstwa	Rodzaj	Input	Kernel	Stride	Output
dane	input	3 x 32 x 32	n/d	n/d	3 x 32 x 32
conv1	convolution	3 x 32 x 32	3 x 3	1/0	32 x 30 x 30
pool2	max pooling	3 x 30 x 30	2 x 2	2/0	64 x 15 x 15
conv3	convolution	32 x 15 x 15	3 x 3		64 x 15 x 15
conv4	convolution	32 x 15 x 15	3 x 3	1/0	64 x 13 x 13
pool5	max pooling	64 x 13 x 23	2 x 2	2/0	64 x 6 x 6
fc6	fully connected	64 x 6 x 6	1 x 1	1/0	512 x 1 x 1
fc7	fully connected	512 x 1 x 1	1 x 1	1/0	10 x 1 x 1

Oczywistym jest, że analizując najbardziej znane architektury sieci neuronowych należy mieć na względzie, że skuteczność i wydajność danej sieci zależą od konkretnej implementacji, zbioru danych i zadania. W praktyce konieczne jest przeprowadzenie eksperymentów i dostosowanie sieci do konkretnych potrzeb, aby uzyskać optymalne wyniki. Mając to na względzie, w zakresie niniejszej pracy, do początkowych eksperymentów wykorzystano sieci zaprojektowane przez autorów MCADL (ich architektury zostały przedstawione w tabeli 2) do sprawdzenia tej metody na dwóch zbiorach: MNIST oraz CIFAR-10.

Natomiast z uwagi na niesatysfakcjonujący wynik (o czym piszą sami autorzy) dla sieci stworzonej dla CIFAR-10, docelowe rozwiązanie zostało zaimplementowane na zmienionej autorsko sieci, która umożliwiła zwiększenie poziomu dokładności w prowadzonych obliczeniach, co opisano w rozdziale III.

ROZDZIAŁ III
ANALIZA WIELOKRYTERIALNA

1. Adaptacyjne wyznaczanie rozwiązań efektywnych

1.1 Algorytmy optymalizacyjne w procesie decyzyjnym

Świat wielokryterialny jest dla człowieka naturalny. Większość problemów rozpatruje przez pryzmat różnych priorytetów, których określenie zależy od danej osoby lub organizacji, z których każda znajduje się w odmiennej sytuacji. Optymalizacja jest procesem, który porządkuje rzeczywistość i pomaga w podejmowaniu najlepszych decyzji.

Po wynalezieniu komputera i rozwoju technologii informatycznych, wiele problemów z dziedzin takich jak matematyka, inżynieria czy ekonomia stało się możliwych do rozwiązania z wykorzystaniem metod optymalizacyjnych, dzięki którym usprawniono wiele procesów i uzyskano lepsze wyniki w krótszym czasie. Jednym z pierwszych tego rodzaju zadań, przy wykorzystaniu komputera, było opracowanie metody optymalizacji kosztów produkcji i dystrybucji zaopatrzenia dla armii amerykańskiej podczas II Wojny Światowej, kiedy to powstała konieczność optymalizacji dostaw zaopatrzenia lotniskowców na Pacyfiku. *George Dantzig*[14] opracował wtedy algorytm sympleks, który jest najbardziej popularną metodą rozwiązywania problemów programowania liniowego – powstałej wtedy dziedziny matematyki i informatyki, która zajmuje się optymalizacją liniowych funkcji celu, z wykorzystaniem liniowych nierówności i równości jako ograniczeń. Algorytm sympleks działa na zasadzie przeszukiwania wierzchołków wielościanu ograniczeń, w celu znalezienia wierzchołka z najlepszym rozwiązaniem. Opracowanie tej metody programowania liniowego dało początek rozwojowi dziedziny Badań Operacyjnych. Współcześnie, zastosowanie narzędzi informatycznych, takich jak sztuczna inteligencja i uczenie się maszyn, pozwala na jeszcze bardziej zaawansowane rozwiązania i szybsze przetwarzanie danych [67].

Optymalizacja jest działaniem podejmowanym w celu polepszenia danego obiektu, procesu, sytuacji, która umożliwia stworzenie rozwiązania dającego wyniki lepsze od zastanych. W pracy prof. *Włodzimierza Ogryczaka* problem optymalizacyjny jest przedstawiany w kontekście podejmowania decyzji, których celem jest osiągnięcie oczekiwanego rezultatu. Optymalizacja w procesie wspomagania decyzji jest aktywnością, która może zakładać jedno lub wiele rozwiązań, wiążących się z rozważaniem jej wariantów

[14] Amerykański matematyk, twórca algorytmu sympleksowego, a także niezależnie programowania liniowego w kilka lat po rosyjskim ekonomiście i matematyku Leonidzie Kantorowiczu. *John J. O'Connor; Edmund F. Robertson: George Dantzig w MacTutor History of Mathematics archive*

przez człowieka. Najczęściej przyjmuje się w niej określone założenia i automatyzm w działaniu komputera. Oznacza to, że liczba zmiennych decyzyjnych może być dowolna, a optymalizacja będzie procesem ulepszania *x* zmiennych przy jednoczesnym procesie poszukiwania ekstremum funkcji.

W przypadku analizy obrazu prowadzonej w ośrodkach wojskowych wiadomo, że decyzję co do klasyfikacji obiektów nie tylko trzeba automatyzować, ale i realizować ten proces interaktywnie, w uzasadnionych przypadkach kierując do eksperta dziedzinowego. Wynika to z faktu, iż jeszcze kilka lat temu wskazywano, że analitycy poświęcają tylko 20% czasu na przeglądanie prawidłowych danych, podczas gdy 80% czasu poświęcali na poszukiwanie prawidłowych danych w ogóle [68], co pokazało jak duże obciążenie czasowe występuje w tym procesie przy osobowej obsłudze analizy zobrazowań i innych danych. I choć ta sytuacja niewątpliwie uległa poprawie to oczywiste jest, że interaktywne i zautomatyzowane systemy klasyfikacji w tym zakresie są koniecznością.

Nie zawsze jednak jest oczywiste, że podejmowanie decyzji powinno podlegać automatyzacji. Czasami pożądane jest tylko wspomaganie decyzji [69]. Przykładowo dzieje się tak wtedy kiedy decydent uzna, że z uwagi na dynamikę sytuacji lub zmienność uwarunkowań każdorazowo musi on wesprzeć proces decyzyjny swoją intuicją i wprowadzić własne kryterium w celu określenia optymalnego rozwiązania.

Nasuwa się w tym kontekście analogia, że proces uczenia się algorytmu *de facto* odzwierciedla typowy proces decyzyjny, w którym model rozpoznaje wzorce i po analizie zbioru podejmuje decyzję formułując odpowiedź przez zastosowanie odpowiedniej funkcji.

Większość klasycznych algorytmów optymalizacyjnych stosuje deterministyczną procedurę, która krok po kroku dociera do rozwiązania optymalnego realizując jednokierunkowe poszukiwanie najlepszego rozwiązania. Najlepsze rozwiązanie staje się nowym rozwiązaniem i procedura jest powtarzana określoną liczbę razy. Istnieje również grupa algorytmów ewolucyjnych, które posiadają zdolność łatwej adaptacji i mogą być stosowane przy rozwiązywaniu złożonych nieliniowych i wielowymiarowych problemów [70].

Dotychczas wypracowano wiele rodzajów algorytmów optymalizacyjnych, w tym między innymi [71]: algorytmy należące do grupy dokładnych, algorytmy należące do grupy heurystyk oraz algorytmy aproksymacyjne.

Algorytmy należące do grupy dokładnych, to między innymi:

a) programowanie dynamiczne (ang. *Dynamical Programming – DP*), w którym zakłada się, że problem jest ustrukturyzowany i dzięki optymalnym rozwiązaniom pod-problemów można wyznaczyć optymalne rozwiązanie problemu głównego;

b) przeszukiwanie wyczerpujące (ang. *Exhaustive Search - ES*), wymaga wygenerowania i sprawdzenia każdego rozwiązania dopuszczalnego.

Wśród algorytmów należących do grupy heurystyk, wyróżnia się:

a) heurystyczne specjalizowane – dla konkretnego problemu;
b) uniwersalne – metaheurystyki, w tym między innymi:
   - przeszukiwanie losowe (ang. *Random Search* - RS).
   - przeszukiwanie lokalne (ang. *Local Search – LS*), w którym istotna jest idea sąsiedztwa uwzględniająca parametr odległości i podobieństwa do „sąsiada". W tym zakresie więcej rozwiązań jest ocenianych niż akceptowanych. Dwie modyfikacje tego mechanizmu to: algorytm „zachłanny" (ang. *greedy*), który losowo „rzuca się" na wszystko, co znajduje się niedaleko, oraz „stromy" (ang. *steeper*), który poszukuje najlepszego rozwiązania.
   - przeszukiwanie tabu (ang. *Tabu Search* - TS) – oznaczające wprowadzenie zasady zakazu powrotu do miejsc ostatnio odwiedzanych, a zatem podjęcie decyzji o wyborze najlepszego spośród nie zakazanych ruchów nawet, jeżeli prowadzi do gorszego rozwiązania.
   - symulowane wyżarzanie (ang. *Simulation Annealing - SA*) – gdzie występuje parametr sterujący zwany *temperaturą*, który maleje w trakcie wykonywania algorytmu. Występuje w nim możliwość akceptowania rozwiązań gorszych niż aktualne, ale prawdopodobieństwo przyjęcia gorszego rozwiązania spada wraz ze spadkiem temperatury i wzrostem różnicy jakości obu rozwiązań [72].
   - Algorytm ewolucyjny (ang. *Evolutionary Algorithm - EO*), w którym stosowane są mechanizmy selekcji, reprodukcji i mutacji inspirowane przez biologiczny proces ewolucji w którym, podobnie jak w procesie biologicznym, algorytm ewolucyjny tworzy stopniowo coraz to lepsze rozwiązania [70].

W zakresie algorytmów aproksymacyjnych, dokonuje się oceny, o ile ich wynik jest gorszy od optimum gdyż koszt rozwiązania zwróconego przez algorytm aproksymacyjny jest nie większy (w przypadku problemu minimalizacyjnego) albo nie mniejszy (w przypadku problemu maksymalizacyjnego) od rozwiązania optymalnego pomnożonego przez pewną stałą.

Metody działania optymalizacji można podzielić na numeryczne (działające na systemach liczbowych) i kombinatoryczne, które działają na kombinacjach elementów. Problem optymalizacji może być sformułowany jako zadanie minimalizacji bądź maksymalizacji.

Dla systemu wspomagania decyzji istotne będzie zrozumienie ujęcia modelu w kategorii:

- jednokryterialności, oznaczającej, że algorytm uwzględnia jedną, skalarnie optymalizowaną funkcję celu (przy założeniu, że określono cel i przedmiot optymalizacji) lub;
- wielokryterialności, wskazującej na wielość optymalizowanych komponentów i rezultatów decyzji, co zostało wyjaśnione poniżej [1]. Tam, gdzie potrzebny jest system wspomagania decyzji w rozumieniu systemu komputerowego w przeważającym stopniu przedmiotem analiz zawsze będzie wiele kryteriów i uzyskiwanych w ślad za nimi rozwiązań, co stanowiło przedmiot prac, zgodnie z klasyfikacją przedstawioną w opracowaniu [1].

1.2 Optymalizacja jednokryterialna

W zastosowaniach technicznych poszukuje się efektywnego rozwiązania z obszaru tych dopuszczalnych. Ten proces prowadzi do maksymalizacji lub minimalizacji jednego celu, na przykład zysku, kosztów, czasu wykonania lub jakości. W zależności od celu, dla którego poszukiwany jest punkt optymalny, funkcja może mieć różne wartości maksymalne lub minimalne, a zatem różne punkty optymalne. Na przykład, jeśli celem jest maksymalizacja zysku firmy, to punktem optymalnym będzie wartość funkcji, która daje największy zysk. Natomiast, jeśli celem jest minimalizacja kosztów produkcji, to punktem optymalnym będzie wartość funkcji, która daje najniższe koszty.

W celu osiągnięcia optymalnego wyniku, proces optymalizacji jednokryterialnej zazwyczaj wymaga ustalenia wartości parametrów lub zmiennych decyzyjnych, które wpływają na kryterium optymalizacyjne. Następnie, używając odpowiedniej metody optymalizacyjnej, jak metoda gradientu lub zastosowanie algorytmu ewolucyjnego, próbuje się znaleźć wartości tych parametrów, które maksymalizują lub minimalizują wartość kryterium optymalizacyjnego.

Wynikiem optymalizacji jednokryterialnej jest zbiór rozwiązań optymalnych, zawierający rozwiązania zadania optymalizacji wielokryterialnej, w którym jednoznaczne w przestrzeni ocen rozwiązanie optymalne skalaryzacji jest rozwiązaniem efektywnym, zgodnie z wzorem nr 22 [73]:

$$\max \{ \min_{i=1,\dots,m} f_i(\mathrm{x}) \ : \mathrm{x} \in \mathrm{Q} \} \tag{22}$$

Rozwiązanie optymalne w zadaniu optymalizacji jednokryterialnej, gdzie poszukiwane jest tylko jedno optymalne rozwiązanie, jest równoważne z efektywnym rozwiązaniem

w przypadku optymalizacji wielokryterialnej, gdzie szukamy wielu rozwiązań optymalnych. Jednakże, w przypadku optymalizacji wielokryterialnej istnieje istotna różnica pomiędzy pojęciami rozwiązania optymalnego i efektywnego, ponieważ rozwiązania efektywne generują różne i nieporównywalne wektory ocen.

W celu formalizacji zadania optymalizacji wielokryterialnej, często wyznaczamy wszystkie rozwiązania efektywne. Jest to jednakże zadanie złożone i zwykle wymaga technik generowania rozwiązań efektywnych. Jednym ze sposobów na wyznaczenie pojedynczych rozwiązań efektywnych jest poszukiwanie wektorów najwyższych wartości w zbiorze ocen osiągalnych za pomocą pewnej spójnej i racjonalnej relacji preferencji. W tym celu można również stosować jednokryterialne skalaryzacje zadania. [73].

1.3 Analiza wielokryterialna

W odróżnieniu od modeli optymalizacji jednokryterialnej model decyzyjny optymalizacji wielokryterialnej nie precyzuje ściśle jednej koncepcji najlepszego rozwiązania. Zapis maksymalizacji w modelu wielokryterialnym oznacza jedynie, ze dla każdej pojedynczej oceny preferowana jest większa wartość. Nie mniej analiza wielokryterialna jest jedną z metod prowadzących do znalezienia rozwiązania efektywnego lub wszystkich rozwiązań efektywnych danego zagadnienia. Jej celem jest wyznaczenie całego zbioru rozwiązań efektywnych lub zbioru rozwiązań efektywnych generujących zbiór wszystkich niezdominowanych wektorów ocen [73]. Stanowią one podstawę do podjęcia ostatecznej decyzji.

Proces optymalizacji wielokryterialnej stanowi próbę znalezienia wektora zmiennych decyzyjnych:

$$x = [x_1, x_2,...,x_i] \tag{23}$$

który spełnia określone warunki:

$$g_i(x) \geq 0 \quad (i = 1... m),$$
$$h_i(x) = 0 \quad (i = 1 ... p)$$

i którego rozwiązania są oceniane według wektora funkcji celu, reprezentującej matematyczny opis danego kryterium nawet jeśli często pozostają w konflikcie miedzy sobą (różne rozwiązania efektywne generują różne i wzajemnie nieporównywalne wektory ocen [73]):

$$f(x) = (f_1(x), f_2(x),..., f_i(x)) \tag{24}$$

Trudność w analizie wielokryterialnej polega na znalezieniu optymalnego rozwiązania problemu decyzyjnego, które jest akceptowalne z punktu widzenia każdego kryterium, dlatego też zbiór rozwiązań efektywnych zadania wielokryterialnego stanowi jedynie podstawę do wyboru ostatecznego rozwiązania przez decydenta.

Rozwiązanie wielokryterialnych problemów decyzyjnych może być wspierane przez interaktywne systemy wspomagania decyzji. Istnieje rozwinięta metodologia interaktywnego wyznaczania efektywnych rozwiązań poprzez modelowanie racjonalnych preferencji. W przypadku otwartych systemów wspomagania decyzji, decydent nie jest zmuszony do stosowania ściśle określonego scenariusza analizy problemu decyzyjnego, a może modyfikować swoje preferencje w trakcie analizy, na podstawie poznawanej specyfiki problemu. Jądro metodologiczne (i obliczeniowe) takich systemów stanowi interaktywna technika analizy zbioru efektywnych rozwiązań, oparta na parametrycznych skalaryzacjach.

Zadanie optymalizacji wielokryterialnej może być zastąpione parametrycznym zadaniem optymalizacji jednokryterialnej, które polega na maksymalizacji funkcji s(v,y) dla y należącego do zbioru A, przy ustalonym wektorze parametrów sterujących v (wzór 25).

$$\max_{y} \{s(v, y) : y \in A\}, \quad v \in V \tag{25}$$

gdzie:

v – wektor parametrów sterujących,

s – parametryczna funkcja s: VxY→R, określająca dla każdej wartości parametrów sterujących v ∈ V funkcję skalaryzującą $s^v(y) = s(v,y)$.

Skalaryzację parametryczną definiujemy jako funkcję s(v,y), która zawsze reprezentuje racjonalną relację preferencji, niezależnie od wartości parametrów sterujących. Dzięki temu wyznaczane rozwiązania są niezdominowane, a skutkiem tego efektywne. Skalaryzacja parametryczna spełnia zasadę niezdominowania rozwiązań wtedy, gdy dla każdego wektora parametrów sterujących v, rozwiązanie optymalne skalarnego zadania jest niezdominowanym wektorem ocen dla oryginalnego zadania optymalizacji wielokryterialnej. [73].

Skalaryzacją zadania optymalizacji wielokryterialnej nazywamy zadanie optymalizacji jednokryterialnej

$$max\ \{s\ (f_1(x), f_2(x), \ldots\ldots, f_i(x)) : x \in Q\} \tag{26}$$

z funkcją skalaryzującą $s : R^i \rightarrow R$

W praktyce, do wyboru spośród wielu kryteriów można zastosować między innymi sumę ważoną (ważenie kryteriów w procesie decyzyjnym). Można również stworzyć system relacji i porządków, który wskaże zbiór rozwiązań optymalnych.

Suma ważona stanowi emanację zachowania decydenta, który przed podjęciem decyzji zazwyczaj, intuicyjnie waży kryteria wyboru.

$$\sum_i w_i \cdot x_i \tag{27}$$

W tym zakresie przypisywana jest waga danego kryterium, która powoduje, że w przestrzeni rozwiązań można określić, które ma charakter optymalny i jaki jest powód takiej oceny. W takiej procedurze każde rozwiązanie odzwierciedla sumę wag poszczególnych kryteriów. Przykładowo, gdyby się okazało, że środki na pozyskiwanie zdjęć są ograniczone i należy dokonać wyboru zdjęcia do analizy, można zdefiniować szereg kryteriów, które zostały przedstawione w tabeli 3.

Tabela 3 Przykładowe zestawienie wielu kryteriów

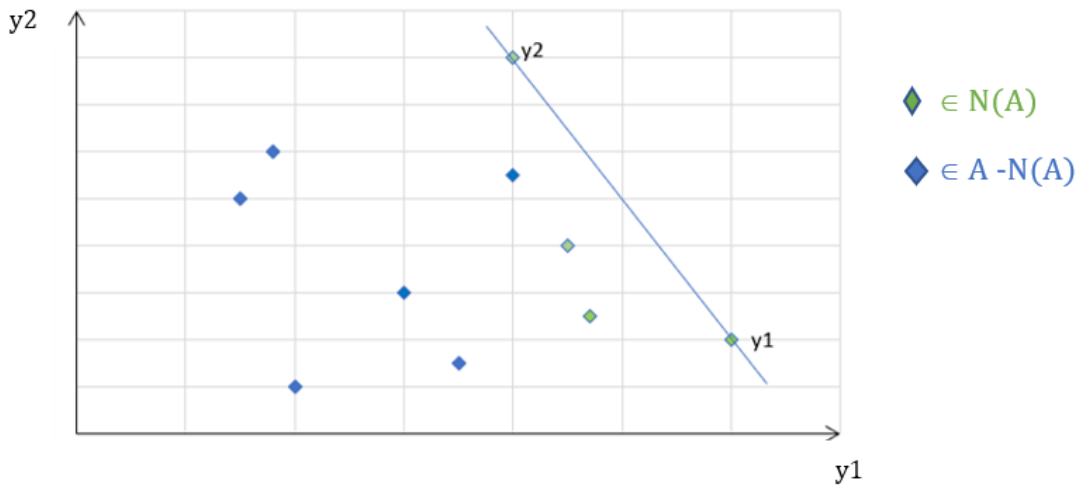
KRYTERIUM	MINIMALIZOWANE/ MAKSYMALIZOWANE	WAGA
Zasięg terytorialny zdjęcia	max	0,2
Czas pozyskania zdjęcia	min	0,1
Koszt pozyskania zdjęcia	min	0,4
Zdjęcie kolorowe	max	0,05
Bezpieczeństwo pozyskania zdjęcia	max	0,2
Rozdzielczość zdjęcia	min	0,05
	Suma ważona	1

Gdyby potraktować powyższy problem jednokryterialnie, można łatwo zdefiniować, które rozwiązanie jest najlepsze, bo wystarczy porównywać jedno z drugim odnosząc się do jednego poziomu, jednego wymiaru. Strzałki pokazują czy powinno zostać wybrane rozwiązanie w wersji maksymalnej danego kryterium czy minimalne (przykładowo im mniejsza cena, tym więcej zdjęć można pozyskać, więc racjonalnie patrząc, wiadomo, że zostanie wybrane rozwiązanie z najmniejszym kosztem per zdjęcie zaproponowanym przez oferenta). Natomiast traktując powyższy problem wielokryterialnie i definiując zakres rozwiązań niezdominowanych należy mieć świadomość, że są one możliwe tylko w określonej konfiguracji, bo teoretycznie tylko maksymalizacja jednego celu (zasięg terytorialny), a minimalizacja innego (np. kosztu), może spowodować, że zestaw rozwiązań będzie optymalny dla danego problemu. Jednocześnie istotnym jest wprowadzenie takiej normalizacji kryteriów, która w ogóle umożliwi dokonywanie podanego powyżej porównania dlatego też w skalaryzacji dokonywanej za pomocą ważonej sumy ocen, zazwyczaj przyjmuje się wagi

znormalizowane w skali 0-1, tak aby sumowały się do jedności. Ważona suma ocen wyraża średnią ważoną poszczególnych ocen.

Każdy decydent inaczej dobierze wagi dla osiągnięcia zakładanego przez siebie efektu. W zależności od celu pozyskiwania zobrazowania może być nastawiony przykładowo na zobrazowania satelitarne radarowe, które są wykonywane bez względu na porę doby i pogodę, co pozwala na stworzenie portfolio danych o zmianach na określonym obszarze, w czasie *t*, szczególnie jeśli chodzi o tereny krajów, których przestrzeń powietrzna jest zablokowana. Inny może być nastawiony na zdjęcia z bezzałogowych platform, które w bardziej ograniczonym zakresie terytorialnie, ale są możliwe do pozyskania sprawnie i bardziej dynamicznie niż satelitarne, często też nie wymagają zbyt wielu technik przetworzenia.

Natomiast, warto mieć na względzie, że uzyskanie rozwiązań efektywnych w drodze ważenia ocen nie jest możliwe do uzyskania dla przypadków optymalizowanych wielokryterialnie, zgodnie z poniższym rysunkiem:



Rysunek 17 Zbiór rozwiązań w oparciu o dane symulowane. Tylko dwa wektory niezdominowane y1 i y2 mogą być wyznaczone za pomocą maksymalizacji ważonej sumy ocen.

Podsumowując, w optymalizacji jednokryterialnej model decyzyjny precyzuje jedno najlepsze rozwiązanie, podczas gdy w optymalizacji wielokryterialnej określa zbiór rozwiązań, które są kompromisem między różnymi kryteriami. Analiza wielokryterialna ma na celu znalezienie rozwiązania efektywnego lub zbioru rozwiązań efektywnych, które generują zbiór niezdominowanych wektorów ocen. Zadanie optymalizacji wielokryterialnej polega na znalezieniu wektora zmiennych decyzyjnych, który spełnia określone warunki i jest oceniany według wektora funkcji celu.

Rozwiązanie wielokryterialnych problemów decyzyjnych może być wspierane przez interaktywne systemy wspomagania decyzji, które umożliwiają decydentowi modyfikowanie preferencji w trakcie analizy. Skalaryzacja parametryczna jest jedną z technik analizy zbioru efektywnych rozwiązań, która pozwala na wyznaczanie niezdominowanych rozwiązań. W praktyce, do wyboru spośród wielu kryteriów można zastosować sumę ważoną lub system relacji i porządków. Ważne jest uwzględnienie specyfiki problemu i celu decydenta przy doborze wag i kryteriów. Optymalne rozwiązania dla problemów wielokryterialnych znajdują rozwiązania efektywne, które uwzględniają różnorodne kryteria i niezależność od wartości parametrów sterujących.

1.4 Relacje dominacji i porządków

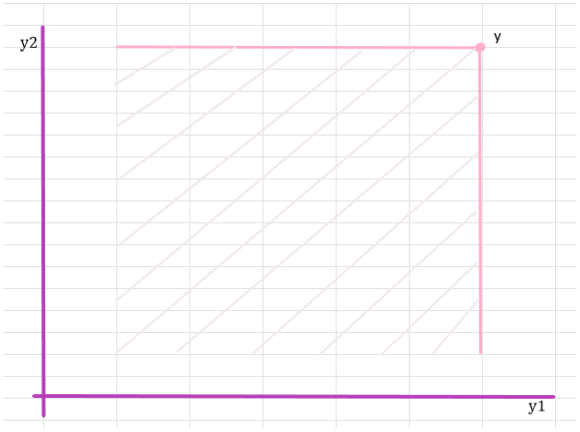
Relacja dominacji wielokryterialnej pozwala zidentyfikować, w dowolnym zbiorze rozwiązań ocenionych wieloma kryteriami, te rozwiązania, które są zdominowane wielokryterialnie i te, które tworzą front rozwiązań niezdominowanych, czyli *front Pareto*[15]. Użyta liczba mnoga wskazuje, że w procesie podejmowania decyzji, optymalność wektorowa nie dotyczy pojedynczego rozwiązania, ale całego ich zbioru. Oznacza ona również, że określenie rozwiązań wymaga znaczących nakładów obliczeniowych. Dzięki temu decydent może wybierać pomiędzy różnymi rozwiązaniami (Pareto-optymalnymi).

Relacja dominacji wielokryterialnej nie ma żadnych założeń co do istnienia wag. Zakłada się, że decydent będzie zawsze wybierał takie kryteria, które będą zgodne z jego preferencjami.

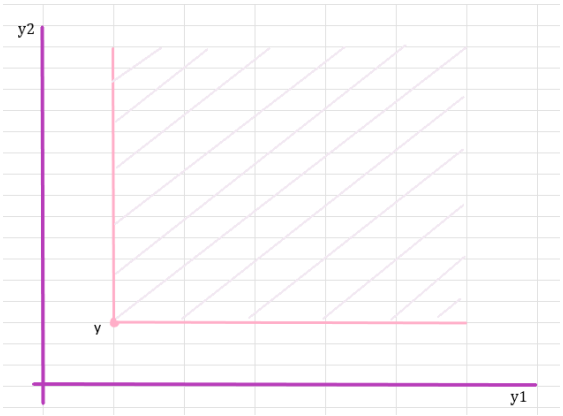
Dlatego też stwierdza się, że wektor ocen $y' \in Y$ (racjonalnie) dominuje $y'' \in Y$ wtedy i tylko wtedy, gdy $y' \succ y''$ dla wszystkich racjonalnych relacji preferencji. Racjonalność rozwiązania polega na założeniu, że rozwiązania wektora y' nie są gorsze od rozwiązań y'' na wielu kryteriach, a na jednym ściśle lepsze i dlatego racjonalny decydent preferuje zawsze wektor y'.

Jeśli nie można przyjąć żadnych założeń *a priori* dotyczących preferencji decydenta to zakłada się, że celem staje się znalezienie zbioru rozwiązań, które są optymalne w sensie optymalności Pareto.

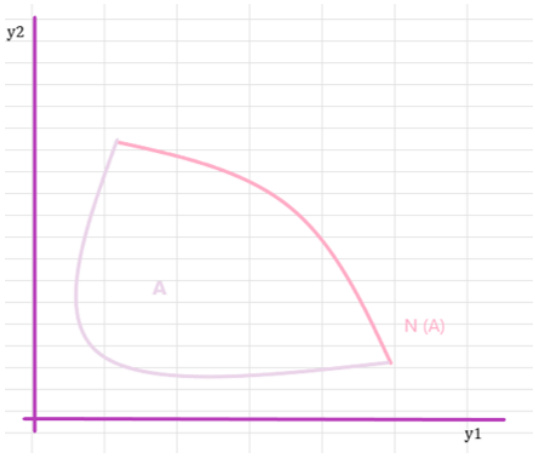
[15] Vilfredo Pareto rozszerzył zastosowania metod matematycznych w ekonomii oraz rozwinął pojęcie ogólnej równowagi ekonomicznej. Zajmował się też badaniami podziału dobrobytu. Stworzył pojęcie tzw. optymalności Pareto (lub inaczej – optimum w sensie Pareto), oznaczające sytuację gdy nie jest możliwa realokacja zasobów, powiększająca dobrobyt którejkolwiek jednostki bez jednoczesnego zmniejszenia dobrobytu innej jednostki. *The Non-Pareto Principle; Mea Culpa. W: Joseph Juran: Juran on Quality by Design. New York: Free Press, 1992, s. 68–71.*



Rysunek 18 Wektory dominujące



Rysunek 19 Wektory zdominowane



Rysunek 20 Wektory niezdominowane

Rysunek 21 Wektory niezdominowane

Dominacja w sensie Pareto definiuje częściowy porządek na zbiorze możliwych rozwiązań [74].

Niezdominowanie wektora ocen y ∈ A, będące istotą teorii Pareto, występuje gdy:

– dla każdego $y' \in$ A istnieje racjonalna relacja preferencji $\succeq$ taka, że nie zachodzi $y' \succ$ y

Racjonalne niezdominowanie wektora ocen y ∈ A występuje, gdy:

– nie istnieje $y' \in$ A taki, że y jest dominowany przez y'

Racjonalną relacją preferencji nazywamy relację preferencji, która jest zwrotna, przechodnia i ściśle monotoniczna [73].

Zagadnienie racjonalności zostało rozpatrzone w teorii decyzji zadowalających (ang. *satisficing decision making*) Herberta Simona[16], w ramach której wyróżniono trzy etapy procesu decyzyjnego:

[16] Herbert Simon - amerykański polihistor: ekonomista, informatyk, socjolog i psycholog, laureat nagrody Turinga (wraz z Allenem Newellem) w 1975. Trzy lata później otrzymał Nagrodę Banku Szwecji im. Alfreda Nobla w dziedzinie ekonomii za rozwój teorii zarządzania i organizacji. Za: *Simon Herbert Alexander, [w:] Encyklopedia PWN [online] [dostęp 2022-08-23]*

- definiowanie poziomów aspiracji dla poszczególnych rezultatów decyzji w sposób adaptacyjny i podczas procesu uczenia się.
- optymalizacja atrybutów towarzyszących podejmowaniu decyzji w sposób iteracyjny, przebiegający dynamicznie i w zależności od bieżących rezultatów procesu nauczania (poziom aspiracji może się zmienić).
- zakończenie procesu po znalezieniu zadowalającego rozwiązania, które co do zasady nie powinno odbiegać od definiowanych na bieżąco aspiracji [1].

W związku z potrzebą dokonywania przez system zmian funkcji wartości podczas procesu decyzyjnego, w sposób adaptacyjny i w zależności od przyjętego punktu aspiracji (modyfikacja może następować zarówno powyżej wskazanego poziomu aspiracji, jak i poniżej) można stwierdzić, że istotna jest tu prostota modelu funkcji wartości w celu maksymalnego uelastycznienia procesu. Taki system nazywany jest metodą quasi-zadowalającego podejmowania decyzji. Zakłada on, że maszyna otrzyma instrukcje w postaci punktów odniesienia, do których będzie dążyć, i które mogą zostać również przekroczone. Komputer może optymalizować przybliżoną wartość stosowanej funkcji wartości, znajdując rozwiązania nawet dla złożonych zadań optymalizacji. Biorąc jednakże pod uwagę, że taka funkcja może stanowić jedynie aproksymację opartą na wskazanych przez decydenta poziomach aspiracji, to należy podkreślić, że stosując tą metodę decydent musi zdefiniować między innymi poziomy odniesienia, kierunki optymalizacji czy inne komponenty, które algorytm powinien wziąć pod uwagę. Oznacza to, że stosowana funkcja nie jest funkcją celu, gdyż to określenie nie byłoby adekwatne, dlatego też w literaturze nazywana jest funkcją osiągnięcia [1].

2. Nowa metoda analizy wielokryterialnej

Problemem optymalizacyjnym przedmiotowej pracy jest znalezienie odpowiedzi na pytanie, jak dokonać wyboru próbek do treningu, które umożliwią modelowi sprawne nauczenie i w konsekwencji dokonanie dokładnej i efektywnej klasyfikacji obiektów na obrazie, w trybie *active learningu* i z wykorzystaniem punktów odniesienia.

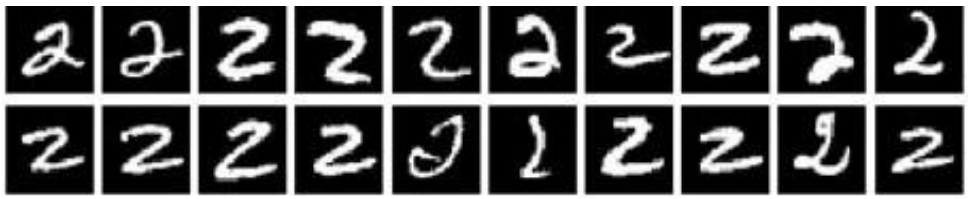
W celu stworzenia algorytmu optymalizacji, konieczne jest zdefiniowanie trzech składowych:

a) Reprezentacji rozwiązania (struktury, zbioru danych);
b) Metody modyfikacji rozwiązania lub generującej kolejne;
c) Funkcji oceny rozwiązania.

W niniejszym rozdziale opisano zaprojektowany algorytm optymalizujący dotychczasowe rozwiązanie, którego słabość została wykazana, a jednocześnie przez dokonanie znaczącej zmiany w postaci inicjalizacji algorytmu, zmiany mechanizmu treningu modelu oraz zaimplementowania metody *margin sampling* stanowiącej ostatni etap klasyfikacji oprowadzono do powstania nowej metody, zwanej dalej metodą z wykorzystaniem punktów odniesienia.

2.1. Zastosowane zbiory danych

Baza danych MNIST została opracowana przez zespół naukowców z trzech uniwersytetów (ang. *University of Toronto, University of Montreal, New York University*) pod przewodnictwem *Yanna LeCun'a*. Składa się z binarnych obrazów cyfr pisma ręcznego i obejmuje zestaw treningowy zawierający 60 000 obrazów oraz zestaw testowy zawierający 10 000 próbek. Przykładowy zestaw danych zawierający cyfrę „2" został przedstawiony na rysunku 22. W zbiorze MNIST cyfry zostały znormalizowane pod względem rozmiaru i wyśrodkowane na obrazie o stałym rozmiarze. Jest to podzbiór większej bazy danych formularzy i znaków opublikowanych przez *National Institute of Standards and Technology* (NIST).

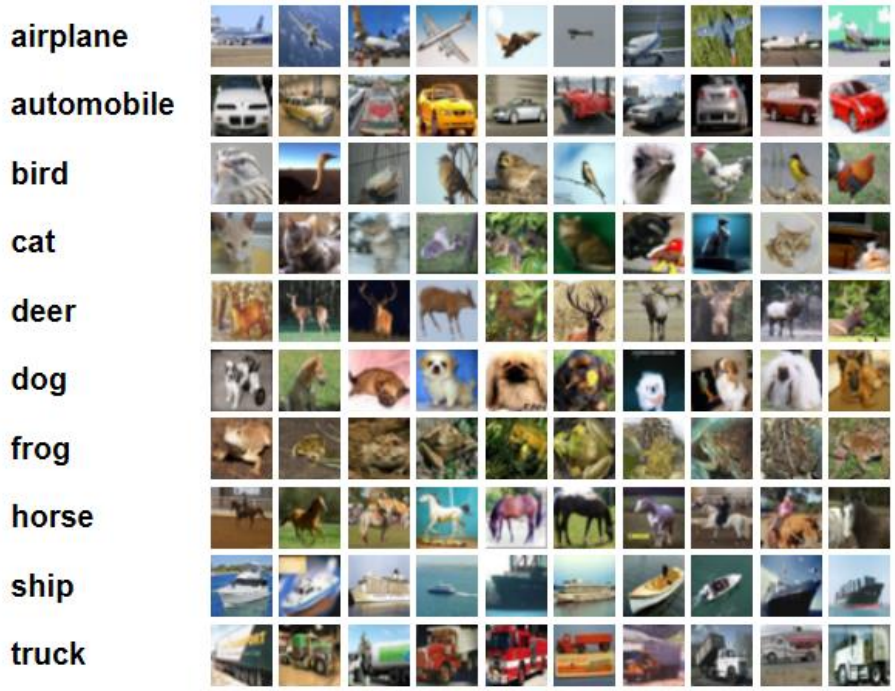


Rysunek 22 Przykładowy zestaw danych MNIST. Na podstawie: [75]

Struktura danych w bazie MNIST jest trójwymiarowa gdyż jest tablicą (ang. *N-dimmentional array*), w której dwa wymiary (28 x 28) oznaczają wymiary zdjęć. Trzeci wymiar wskazuje liczbę zdjęć (algorytm wykorzystuje 50 000 zdjęć w zbiorze treningowym i 10 000 zdjęć w zbiorze testowym), czyli 28 x 28 x 50000. W celu wprowadzenia tych tablic do modelu dane zostały przekształcone na tensory[17], które umożliwiają przeprowadzanie multiprocessingu z silnikiem GPU.

W zbiorze CIFAR-10 struktura danych wygląda podobnie. Zbiór danych CIFAR-10 został opracowany przez *A. Krizhevsky'ego, V. Naira i G. Hintona*[18]. Jak sama nazwa sugeruje zawiera 10 różnych klas obrazów w trzech kanałach barw, uwzględniających następujące obiekty: samolot, samochód, ptak, kot, jeleń, pies, żaba, koń, statek oraz ciężarówka. Zostały przedstawione na rysunku 23.

[17] Tensory są formułą danych powszechnie wykorzystywaną w *deep learningu*.



Rysunek 23 Przykładowy zestaw danych CIFAR-10. Na podstawie [76]

Baza zawiera 60000 obrazów, w tym 50000 obrazów treningowych i 10000 obrazów testowych [77]. Wszystkie zdjęcia mają rozmiar 32×32.

2.2. Zastosowane sieci neuronowe

W sieci pracującej na bazie MNIST wykorzystano metodę *mini-batch gradient descent* [78] do nauki parametrów, a do przyspieszenia zbieżności sieci użyto programu *Adam* [79].

Tabela 4 Architektura CNN dla zbioru danych MNIST

Architektura CNN dla MNIST					
Warstwa	Rodzaj	Input	Kernel	Stride	Output
dane	input	1 x 28 x 28	n/d	n/d	1 x 28 x 28
conv1	convolution	16 x 28 x 28	3 x 3	1	16 x 28 x 28
pool2	max pooling	16 x 14 x 14	2 x 2	2	16 x 14 x 14
conv3	convolution	32 x 14 x 14	3 x 3	1	32 x 14 x 14
pool4	max pooling	32 x 14 x 14	2 x 2	2	32 x 7 x 7
conv5	convolution	32 x 7 x 7	3 x 3	1	64 x 7 x7
pool6	max pooling	64 x 7 x7	2 x 2	2	64 x 3 x 3
fc7	fully connected	64 x 3 x 3	1 x 1	1	32 x 1 x 1
fc8	fully connected	32 x 1 x 1	1 x 1	1	10 x 1 x 1

W pierwszej fazie eksperymentów, sieć neuronowa nie została zmieniona z uwagi na chęć wskazania, że opracowana metoda optymalizacji algorytmu zmieniła przebieg treningu, a nie inne czynniki. Natomiast po realizacji eksperymentów wykazujących, że metoda MCADL działa niewystarczająco zastosowano punkty odniesienia i sieć została dostosowana i zmieniona zgodnie ze schematem przedstawionym w tabeli 4.

Sieć składa się z warstw konwolucyjnych (*Conv2d*), funkcji aktywacji *ReLU*, warstw normalizacji (BatchNorm2d), warstw *MaxPooling* oraz warstw w pełni połączonych (*Linear*). Pierwsza warstwa konwolucyjna ma 16 filtrów o rozmiarze 3x3 piksele. Wynikowa mapa cech ma wymiar 16x28x28. Wynik przekazywany jest do funkcji aktywacji *ReLU*, która wykonuje nieliniową operację na każdym elemencie wyniku. Następnie wynik przekazywany jest do warstwy *MaxPooling*, która redukuje wymiar mapy cech z 28x28 do 14x14.
W kolejnych warstwach wykonywane są analogiczne operacje. Normalizacja pomaga w przyspieszeniu uczenia oraz poprawie ogólnej wydajności sieci. Ostatnia warstwa konwolucyjna ma 64 filtry o rozmiarze 3x3 piksele, a wynik przekazywany jest do funkcji aktywacji *ReLU*. Następnie wynik przekazywany jest do warstwy *MaxPooling*, która redukuje wymiar mapy cech z 7x7 do 3x3.

Kolejna warstwa *Flatten* służy do spłaszczenia wyniku z warstwy konwolucyjnej, tak aby można było przekazać go do dwóch warstw w pełni połączonych (*Linear*) z funkcją aktywacji *ReLU*, Ostatnia warstwa *Softmax* informuje o poziomie prawdopodobieństwa przynależności do 10 klas. W sumie sieć ma 42,154 parametrów do trenowania, a rozmiar danych wejściowych to 28x28 pikseli. Przekształcenia wynikające z propagacji wymagają pamięci na poziomie 0,59 MB.

Pierwsze eksperymenty nowej metody, przeprowadzane na sieci zaproponowanej przez naukowców chińskich wykazały lepsze wyniki (dokładność wskazywana w artykule źródłowym wynosi między 55-60%). Dodatkowo jednak, w celu osiągnięcia efektów bliższych do tych uzyskiwanych na bazie MNIST zdecydowano o zmianie sieci.

Tabela 5 Architektura sieci dla bazy CIFAR - 10

Architektura CNN dla CIFAR-10					
Warstwa	Rodzaj	Input	Kernel	Stride	Output
dane	input	3 x 32 x 32	n/d	n/d	3 x 32 x 32
conv1	convolution	3 x 32 x 32	3 x 3	1	32 x 32 x 32
conv2	convolution	32 x 32 x 32	3 x 3	1	32 x 32 x 32
pool3	max pooling	32 x 32 x 32	2 x 2	2	32 x 16 x 16
conv4	convolution	32 x 32 x 32	3 x 3	1	64 x 16 x 16
conv5	convolution	64 x 16 x 16	3 x 3	1	64 x 16 x 16
pool6	max pooling	64 x 16 x 16	2 x 2	2	64 x 8 x 8
conv7	convolution	64 x 8 x 8	3 x 3	1	128 x 8 x 8
conv8	convolution	128 x 8 x 8	3 x 3	1	128 x 8 x 8
pool9	max pooling	128 x 8 x 8	2 x 2	2	128 x 4 x 4
fc10	fully connected	128 x 4 x 4	1 x 1	1	1024 x 1 x 1
fc11	fully connected	1024 x 1 x 1	1 x 1	1	10 x 1 x 1

Analiza publikacji wskazujących na architektury sieci dające wyższe parametry działania sieci na bazie CIFAR-10 przekonuje do wykorzystania następującej architektury przedstawionej w tabeli 6.

Początkowe wyniki osiągane w eksperymentach wskazywały na zbyt duże dopasowanie modelu. Algorytm przygotowany do rozpoznawania w miarę jednorodnych dziesięciu klas na zdjęciach czarno białych koncentrował się w sposób nieadekwatny do rozpoznawania zróżnicowanych klas na zdjęciach kolorowych. Biorąc to pod uwagę, zdecydowano o wprowadzeniu zmian do struktury modelu. Klasyfikacja obrazu może przebiegać znacznie efektywniej jeśli jest wykonywana z wykorzystaniem sieci neuronowej, w której zostaje zwiększona liczba warstw. Powszechnie wiadome jest również, iż wysoki poziom poprawności klasyfikacji przy miernym poziomie klasyfikacji na zbiorze walidacyjnym oznacza, że należy wprowadzić regularyzację modelu.

Sieć zaprojektowana dla metody MCADL (Tabela nr 2) oraz sieć zaprojektowana dla metody będącej przedmiotem niniejszej pracy (Tabela nr 5) są właściwe do klasyfikacji obrazów na zbiorze danych CIFAR-10. Główną różnicą między nimi jest liczba warstw i konfiguracja filtrów konwolucyjnych oraz operacji poolingowych. Pierwsza sieć zawiera 2 warstwy konwolucyjne i 2 warstwy w pełni połączone, natomiast druga sieć składa się z 4 warstw konwolucyjnych i 2 warstw w pełni połączonych. Ponadto, w pierwszej sieci stosowane są mniejsze filtry (3x3) w pierwszej warstwie konwolucyjnej i maksymalne *pooling* (2x2) w drugiej warstwie *poolingowej*. W drugiej sieci stosowane są większe filtry (3x3) w pierwszych dwóch warstwach konwolucyjnych i większe rozmiary *pooling* (2x2) w trzeciej warstwie *poolingowej*.

Ostatecznie, druga sieć ma większą liczbę parametrów do wytrenowania i potencjalnie może osiągnąć lepsze wyniki w klasyfikacji niż pierwsza sieć, co potwierdzają osiągnięte wyniki.

Zagadnienie, które wymaga również poruszenia analizując dane w kontekście baz źródłowych to parametry przekazywane do modelu. Tabela 6 przedstawia początkowy zakres zbioru *N_ini*, oraz liczbę *N* reprezentującą liczbę wybranych próbek, dostarczanych do etykietowania w rundzie *R*.

Tabela 6 Parametry przekazywane do modelu

	MNIST	CIFAR-10
N	128	200
N_ini	100	2000
Rounds	10	30-35

Podsumowując powyższe rozważania należy mieć na uwadze, że istnieje zawsze konieczność dostosowania sieci neuronowej do konkretnego zadania, po analizie różnych architektur sieci. Wyniki klasyfikacji zazwyczaj ulegają poprawie po zwiększeniu liczby warstw i uwzględnieniu odpowiednich parametrów przekazywanych do modelu.

2.3. Wprowadzenie nowej metody inicjalizacji i analiza koszt-efekt

Pierwszym krokiem w pracy algorytmu był wybór puli inicjalizującej, która stała się początkowym zbiorem, na którym uczył się model. W celu zmniejszenia przypadkowości w doborze próbek do treningu, zdecydowano, by pierwsza pula była wybierana z wykorzystaniem połączonych metod k-średnich i analizy składowych głównych (ang. *Principal Component Analysis - PCA*), stanowiąc krok inicjujący w optymalizacji całego algorytmu. Oznacza to, że z jednej strony nastąpiło klastrowanie danych wprowadzające od razu wstępną ich agregację, a jednocześnie dokonywana była zmiana struktury danych i zmniejszenie ich wymiaru przez dokonanie transformacji wejściowego wektora atrybutów w wektor o mniejszej wymiarowości z wykorzystaniem jednej z najbardziej popularnych metod w tym zakresie, czyli PCA. Jest ona podstawową techniką ekstrakcji cech w przypadku posiadania nieetykietowanych próbek, wykorzystującą pojęcie odległości między próbkami w danej przestrzeni cech i zakładającą, że zmienne objaśniające są liniowymi kombinacjami ukrytych czynników.

Zastosowany sposób wyboru puli inicjalizującej metodą łączoną *k-średnich* i *PCA* nie wpłynął znacząco na wynik algorytmu chociaż warto podkreślić, że jego implementacja w większości wykonanych eksperymentów przyniosła lepszy wynik, niż rozpoczęcie algorytmu metodą losową. Na przedstawionych w pracy wykresach przedstawiono przykłady obliczeń z wyszczególnieniem różnic rezultatów osiągniętych na bazie MNIST z wykorzystaniem inicjalizacji losowej oraz inicjalizacji PCA- *k-means* stanowiącej novum w tym rozwiązaniu.

2.4. Nowa metoda klasyfikacji obrazu z punktami odniesienia

2.4.1. Strategia wyboru punktów odniesienia

Jedną z technik, która umożliwia implementację systemu wspomagania decyzji jest metoda punktu odniesienia – MPO (ang. *reference point method)*, bazująca na parametrycznej skalaryzacji maksiminowej;

$$\max \{ \min f_i(x) \quad : x \in Q\} \tag{28}$$

uwzględniającej funkcje osiągniecia dążące do poziomów aspiracji a_n.

Zaprojektowana, w ramach niniejszej pracy nowa metoda, opiera się o założenie, że właśnie punkty odniesienia uwzględniające poziomy aspiracji dla każdego kryterium dadzą lepsze wyniki niż ważenie kryteriów. Stosowanie punktów odniesienia w klasyfikacji ma zalety wynikające z jej cech: obiektywizmu, porównywalności, optymalizacji oraz wsparciu w procesie ustalenia granic między klasami. W zależności od wskazanych poziomów aspiracji przesuwany jest początek układu współrzędnych w przestrzeni ocen do wektora poziomów aspiracji [73]. Metoda punktu odniesienia nie traktuje wektora aspiracji jako bezwzględnego celu a jedynie jako punkt odniesienia.

Punkty odniesienia są iteracyjnie obliczane w oparciu o funkcję maksiminowa, przedstawioną wzorem 29 i definiującą zbiór rozwiązań.

$$\max_{x \in X} \min_{1 \le i \le m} (q_i - \bar{q}_i) + \frac{\varepsilon}{m} \sum_{i=1}^{m} (q_i - \bar{q}_i) \tag{29}$$

gdzie:

x - zbiór X, którym jesteśmy zainteresowani. Funkcja maksymalizuje wartość funkcji dla x należącego do tego zbioru.

X - przestrzeń, w której znajduje się zbiór x.

m - liczba kryteriów, dla których szukana jest minimalna wartość. Jest to liczba od 1 do *m*, gdzie *m* to całkowita liczba kryteriów.

q_i - wartość *i*-tego kryterium dla konkretnego elementu x.

$\bar{q}_i$ - punkt odniesienia (średnia wartość) dla *i*-tego kryterium. Jest to wartość, do której następuje dążenie, w celu minimalizacji różnicy między $q_i - \bar{q}_i$.

ε - dodatnia wartość niewielka, która jest dodana w celu uniknięcia dzielenia przez zero i reguluje wpływ różnicy między $q_i - \bar{q}_i$ na wynik funkcji.

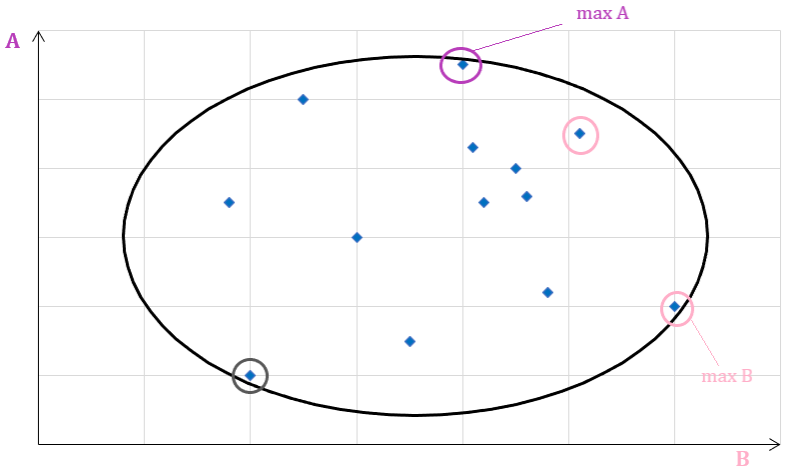
$\sum_{i=1}^{m} (q_i - \bar{q}_i)$ – suma różnic między wartościami $q_i - \bar{q}_i$ dla wszystkich kryteriów

Motywacją dla takiego wyznaczenia punktów odniesienia był fakt, iż w przypadku optymalizacji wielokryterialnej, funkcja maksiminowa jest jednym z możliwych sposobów podejścia do problemu wyboru najlepszego rozwiązania spośród zbioru potencjalnych rozwiązań, które mogą mieć sprzeczne cele. Polega na maksymalizacji minimalnej wartości ze zbioru minimalnych wartości dla każdego z kryteriów. Oznacza to, że poszukiwane rozwiązanie, będzie miało najwyższą minimalną wartość spośród minimalnych wartości dla każdego z kryteriów. Funkcja maksiminowa pozwala na transparentne określenie punktów

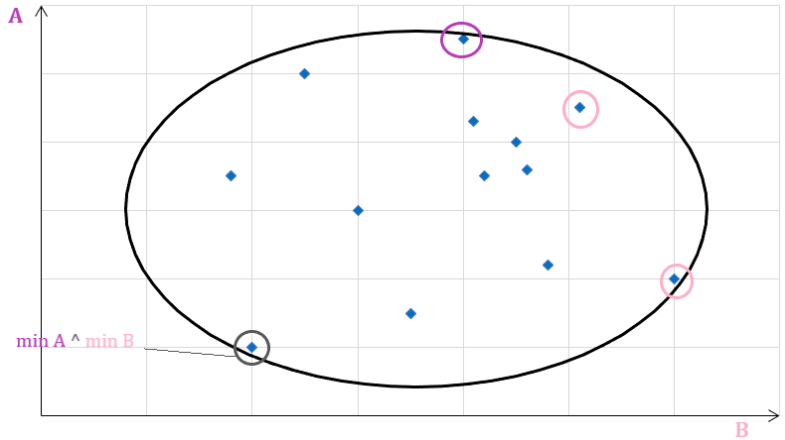
odniesienia na podstawie matematycznego modelu. Jest to obiektywny i powtarzalny sposób definiowania punktów odniesienia, co przyczynia się do większej przejrzystości procesu optymalizacji wielokryterialnej.

Mając na względzie charakter kryteriów dążących do minimalizacji ich wartości, na rys. 25 przedstawiono punkt *min* (A ∧ B), który odzwierciedla wybór rozwiązania na najniższym poziomie biorąc pod uwagę najmniejsze wartości z istniejącego zbioru.

Algorytm zaimplementowany w ramach niniejszej pracy, uwzględniający więcej niż jedno kryterium wyboru próbki, kieruje się kryteriami opisanymi w rozdziale II: podobieństwem, gęstością, niepewnością modelu, oraz etykietami próbek (ang. *label based*). Dwa pierwsze z wymienionych kryteriów są powiązane z danymi, a dwa kolejne z działaniem modelu.



Rysunek 24 Punkty o maksymalnych wartościach dla kryterium A i kryterium B.



Rysunek 25 Punkt o minimalnych wartościach kryterium A i kryterium B.

Istotne jest określenie relacji między nimi, gdyż kryterium podobieństwa i gęstości jest ważne szczególnie na początku treningu modelu, kiedy to dane i związane z nimi kryteria, podlegają nauczaniu przez model.

START

→ Wybór puli inicjalizującej

→ Przygotowanie danych treningowych i testowych na podstawie puli inicjalizującej

→ Trenowanie sieci neuronowej na przygotowanych danych treningowych z wykorzystaniem *active learningu*

→ Wybór przykładów uczących na podstawie czterech kryteriów: gęstości, podobieństwa, niepewności i opartej na etykietach, z których każda pracuje z punktem odniesienia

→ Dodanie wybranych przykładów do puli uczącej sieć neuronową

→ Aktualizacja wag sieci neuronowej na podstawie nowej puli uczącej

→ Testowanie modelu na danych testowych

→ Ocena działania modelu na zbiorze walidacyjnym

KONIEC

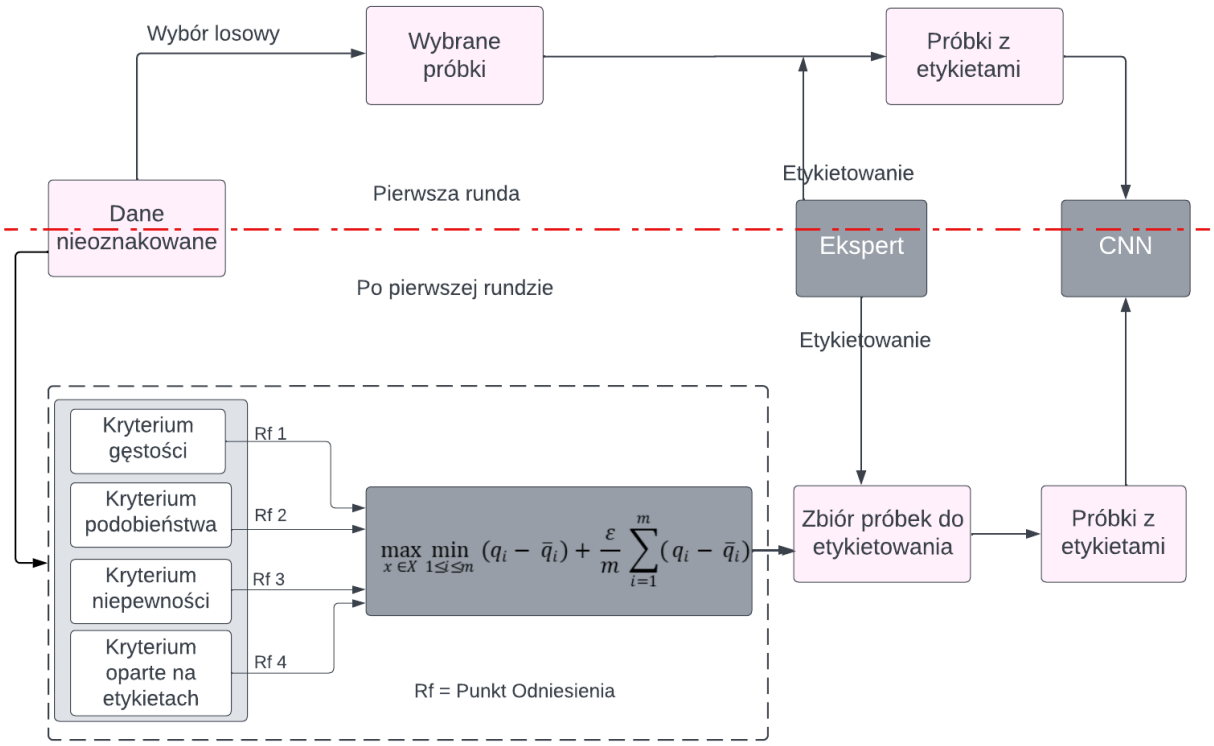
Rysunek 26 Sekwencja działań algorytmu analizy wielokryterialnej.

Schemat przedstawiony na rys. 26 odzwierciedla trening sieci neuronowej z wykorzystaniem *active learningu* i czterech kryteriów wyboru próbek, dzięki którym jest w stanie nauczyć się rozpoznawać obiekty na zdjęciach w sposób bardziej efektywny i dokładny. Zgodnie z przedstawionym na rys. 27 schematem, po wybraniu nowych przykładów uczących i zaktualizowaniu wag sieci neuronowej, algorytm testuje wyuczony model na danych testowych i ocenia jego skuteczność. Zgodnie z przedstawioną wcześniej charakterystyką zakres każdego z kryteriów jest wyrażony w przedziale 0-1.

Metoda punktu odniesienia uwzględnia poziomy aspiracji (punkty odniesienia), które w bieżącym rozwiązaniu zostały określone, w punkcie startowym:

- dla bazy MNIST: w eksperymencie ε wszystkie na poziomie „0”, w eksperymencie ϕ wszystkie na poziomie „1”, w eksperymencie γ kryteria gęstości i podobieństwa operujące na danych z etykietami na 0,1[19], 0,15 natomiast kryteria niepewności i oparte na etykietach operujące na danych nieoznakowanych na 0,9 i 0,8.
- dla bazy CIFAR10: w eksperymencie γ kryteria gęstości i podobieństwa operujące na danych z etykietami na poziomie0,1 i 0,15 natomiast kryteria niepewności i oparte na etykietach operujące na danych nieoznakowanych na poziomie 0,9 i 0,8.

[19] Zastosowano notację w formacie użytym w języku programowania (*Python*), dla zachowania zgodności z umieszczonymi w pracy wynikami obliczeń.



Rysunek 27 Przebieg procesu działania nowej metody uwzględniającej punkty odniesienia. Opracowanie własne.

Reasumując przedstawione powyżej informacje warto podkreślić, iż nowa metoda nie traktuje wektora aspiracji jako bezwzględnego celu, ale jako punkt odniesienia. Poziomy aspiracji są określane na początku procesu. W zależności od wskazanych poziomów aspiracji, początek układu współrzędnych w przestrzeni ocen jest przesuwany. Przedstawione rysunki ilustrują działanie opisywanych metod i algorytmów.

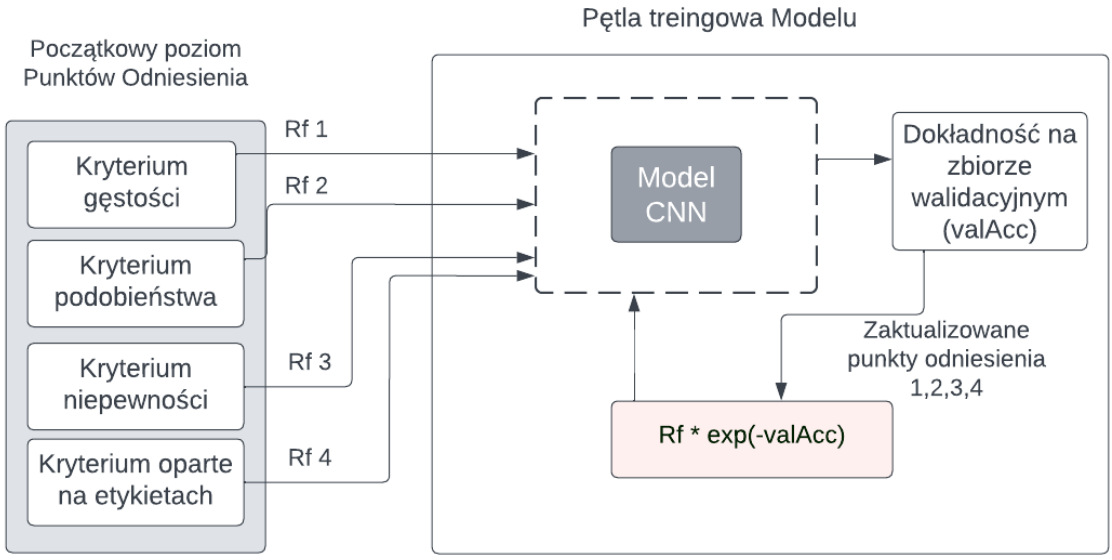
2.4.2. Powiązanie funkcji oceny rozwiązania z iteracyjną zmianą punktów odniesienia

Do oceny przedmiotowego rozwiązania została wybrana metryka dokładności (ang. *accuracy)*, którą opisano w rozdziale I. Poza standardowym zastosowaniem tej funkcji do oceny w algorytmach metody MCADL oraz nowej metody z zastosowaniem punktów odniesienia, dokładność pełni ważną funkcję, sprzęgającą cały mechanizm zastosowany w algorytmach. W metodzie MCADL w miarę wzrostu *accuracy* (*Acc*) maleje waga α, a wraz z nią wykorzystanie kryteriów gęstości i podobieństwa, zgodnie z wzorem:

$$\alpha = \alpha_{ini}\, e^{-Acc^t} \tag{30}$$

Natomiast w nowej metodzie, stosującej punkty odniesienia, dokładność jest powiązana z każdym z kryteriów, których wartość jest ustawiana w celu zwiększenia poziomu tej metryki,

co zostało przedstawione na rys. 28 Mechanizm implementacji punktów odniesienia w niniejszej metodzie można zdefiniować w następujący sposób: wartości referencyjne są zmniejszane w funkcji aktualizującej parametry przez pomnożenie ich przez wykładnik ujemnej dokładności na zbiorze walidacyjnym (*valAcc*). Gdy wartość *self.ref* nie jest *None*, to następuje odniesienie do zewnętrznego tensora, który wymaga aktualizacji. Pomnożenie go przez *torch.exp* (*-torch.tensor(valAcc))* zmniejsza wartość *self.ref* o wielkość proporcjonalną do ujemnej dokładności na zbiorze walidacyjnym.



Rysunek 28 Schemat iteracyjnego doboru punktów odniesienia w powiązaniu z poziomem dokładności. Opracowanie własne

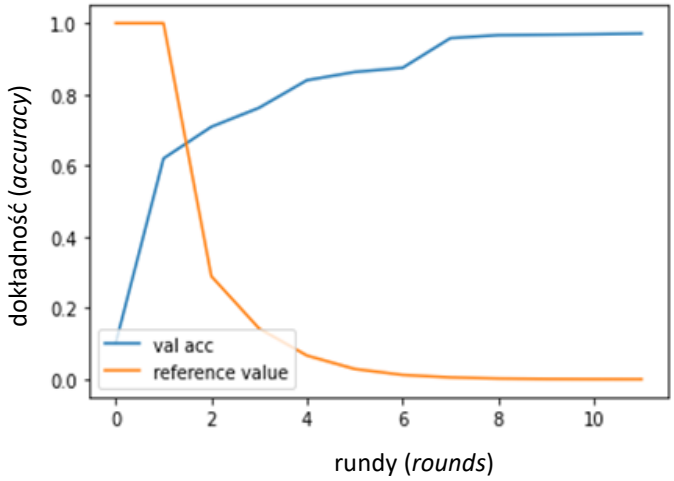
Ten rodzaj rozkładu jest często używany w algorytmach uczenia maszynowego, aby zmniejszyć wpływ informacji z przeszłości, gdy nowe informacje stają się dostępne. Poprzez zmniejszenie wartości *self.ref* w czasie, algorytm staje się bardziej wrażliwy na ostatnie zmiany w danych i mniej podatny na wpływ starszych informacji.

Jak wykazały eksperymenty, w miarę wzrostu poziomu *accuracy,* wartość kryteriów malała. Mechanizm uzależnienia wartości kryteriów od poziomu dokładności pozwolił na zwiększenie wydajności każdej klasy, co było automatycznie weryfikowane pomiędzy rundą *t* a (*t-1*) na zbiorze walidacyjnym. W miarę poprawy wydajności, algorytm wybierał próbki z klas o niskiej wydajności w celu zrównoważenia wydajności pomiędzy klasami.

Założeniem dla konstrukcji informatycznego systemu wsparcia decyzji jest podanie systemowi wartości parametrów sterujących dla każdego niezdominowanego wektora ocen. W celu zdefiniowania najlepszych parametrów wykorzystuje się techniki analizy uwzględniające parametryczne skalaryzacje, które powinny między innymi być zupełne i efektywne obliczeniowo. Ponadto parametry sterujące mogą być wyznaczane przez decydenta

w formie wartości ocen. Jeśli dla danego zagadnienia wskazane przez decydenta *poziomy aspiracji* dla poszczególnych ocen są osiągane przez wartości ocen uznaje się, że dany proces decyzyjny przebiegł w sposób zadowalający. W tym przypadku decydent koncentruje się tylko na tych kryteriach, które nie osiągnęły poziomu aspiracji, nie doskonaląc już tych wartości ocen, które wskazany poziom osiągnęły. W modelu *quasi-zadowalającym* decydent, pomimo osiągnięcia przez wartości ocen poziomów aspiracji próbuje, w miarę możliwości, zwiększyć poziom doskonałości i dokonać poprawy ocen.

Mając na względzie, że celem optymalizacji wielokryterialnej jest znalezienie zbioru rozwiązań, w przebiegu eksperymentów, w pierwszym etapie rozpoczęto od przeszukiwania przez algorytm danych zaczynając od skrajnych poziomów referencji dla wszystkich kryteriów 0 i 1.

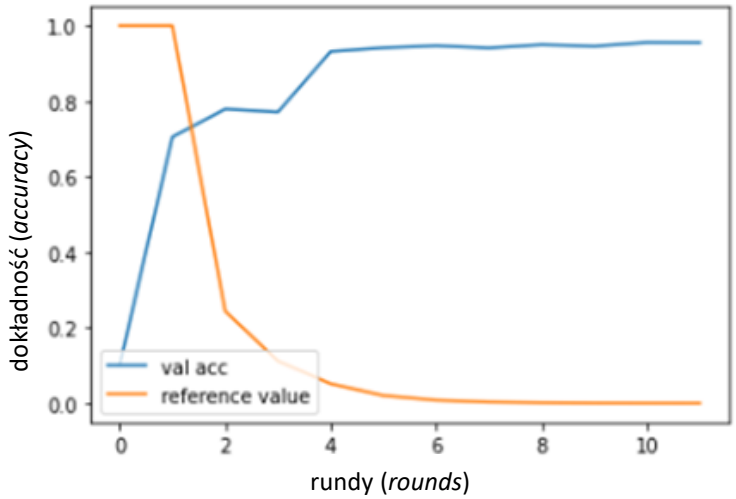


Rysunek 29 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej

Rysunki 29 i 30 przedstawiają przebieg procesu w którym punkty odniesienia zdefiniowano na poziomie 1. Oznacza to, że działanie czterech kryteriów zostało odzwierciedlone krzywą oznaczoną jako *reference value* (kolor pomarańczowy). Widać, że każde z kryteriów „startujące" od punktu odniesienia „1.0" dąży do „0.0". W miarę obniżania się poziomu wartości punktu odniesienia, krzywa oznaczona, jako *val acc* (kolorem niebieskim) oznaczająca dokładność algorytmu - rosła.

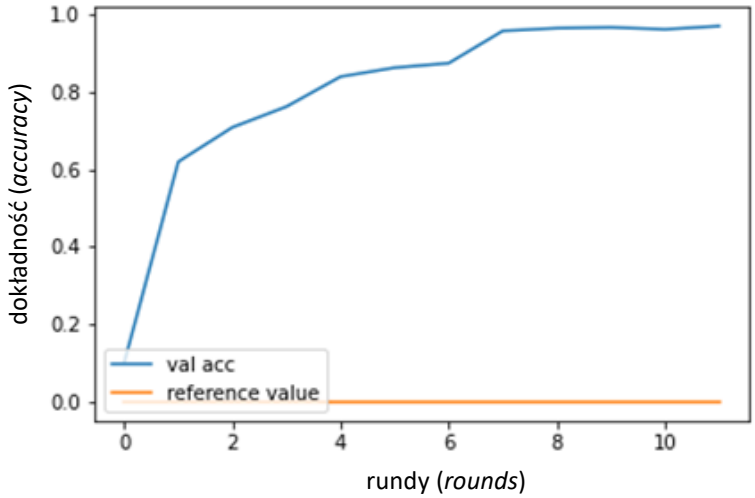
Rys. 29 przedstawia wynik algorytmu inicjalizowanego metodą *PCA-k-means*, wprowadzoną w niniejszej pracy. Metoda *PCA-k-means* została przedstawiona w rozdziale III, punkt 2.3. Przykładowo, dla tego wariantu dokładność wyniosła 0,9985 dla zbioru treningowego oraz 0,9753 dla zbioru walidacyjnego.

Dla porównania na rys. 30 przedstawiono wykres przebiegu działania algorytmu zainicjalizowanego metodą losową, którego dokładność wyniosła 0,9977 dla zbioru treningowego i 0, 9725 dla zbioru walidacyjnego. Można więc stwierdzić, iż wprowadzona metoda inicjalizacji nie wpłynęła znacząco na wyniki, w przypadku przyjęcia dla wszystkich kryteriów poziomu odniesienia „1".



Rysunek 30 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means

Inaczej wygląda przebieg krzywej odzwierciedlającej działanie kryteriów, których wartość odniesienia jest wyznaczona na poziomie „0".



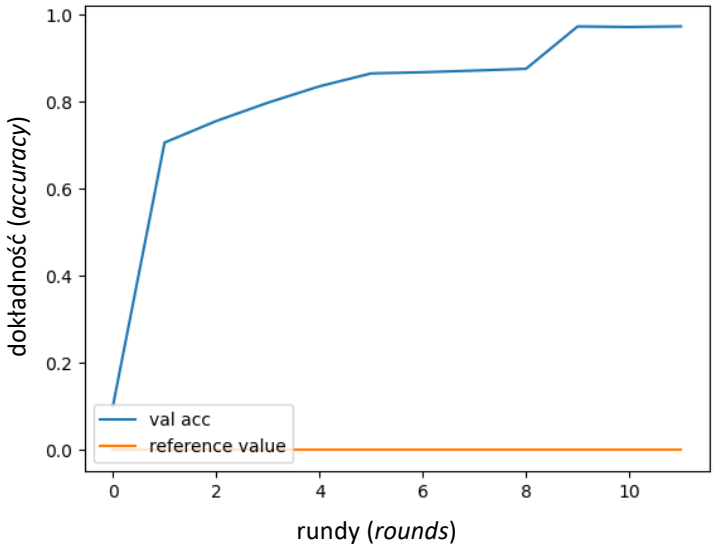
Rysunek 31 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej

Pomimo, iż poziom odniesienia pozostaje niezmieniony, co zostało odzwierciedlone na krzywej oznaczonej, jako *reference value*, algorytm pracuje w sposób powodujący wzrost jego dokładności, oznaczonej jako *val acc*, kolorem niebieskim. W takim wariancie przykładowo eksperymenty wykazały, iż dla inicjalizacji losowej dokładność wyniosła,

dla zbioru treningowego 0,9915 i 0,9657 dla zbioru walidacyjnego, co zostało przedstawione na rysunku 31.

Dla porównania na rys. 32 przedstawiono wykres przebiegu działania algorytmu zainicjalizowanego metodą *PCA-k-means*, gdzie dokładność wyniosła 0,9942, a dla zbioru walidacyjnego 0,9703.

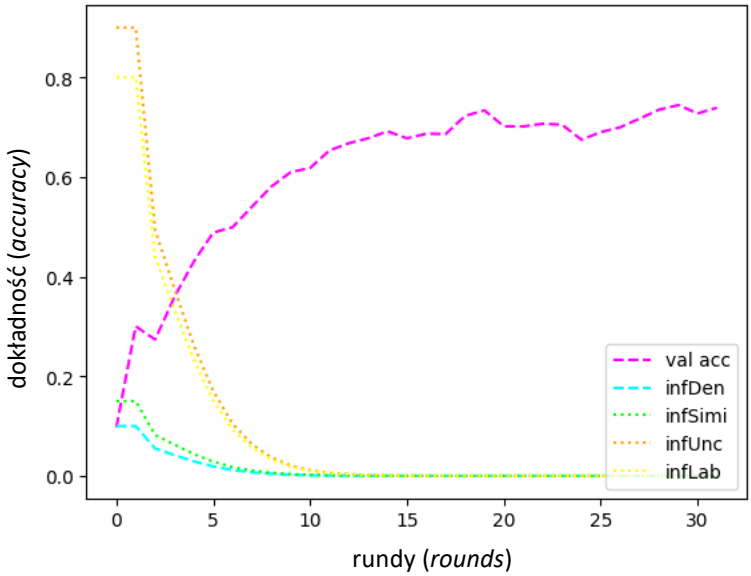
Na bazie MNIST już na poziomie 10 rundy algorytm osiągał dokładność ponad 90%, a poziom odniesienia był bliski *0*, co jest widoczne na rysunkach 29-32.



Rysunek 32 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means

Zarówno w eksperymentach ε (poziom aspiracji „0") oraz ϕ (poziom aspiracji „1"),wyniki funkcji oceny, czyli *accuracy,* przedstawiały się porównywalnie. Poziom wszystkich punktów referencji malał w miarę wzrostu poziomu dokładności algorytmu.

Badania skrajnych wartości punktów odniesienia (0 i 1) wykazały, iż algorytm dążył do zera, kiedy rosła dokładność na zbiorze walidacyjnym. Mając to na względzie, w przypadku realizacji eksperymentu γ, na sieci CIFAR-10, poziom punktów odniesienia zróżnicowano i dla kryteriów opartych o dane z etykietami, czyli dla podobieństwa i gęstości przyjęto poziomy bliskie zeru (podobieństwo: 0,1 i gęstość: 0,15). Dla kryterium niepewności przyjęto punkt odniesienia 0,9, a dla kryterium opartego na etykietach na poziomie 0,8.

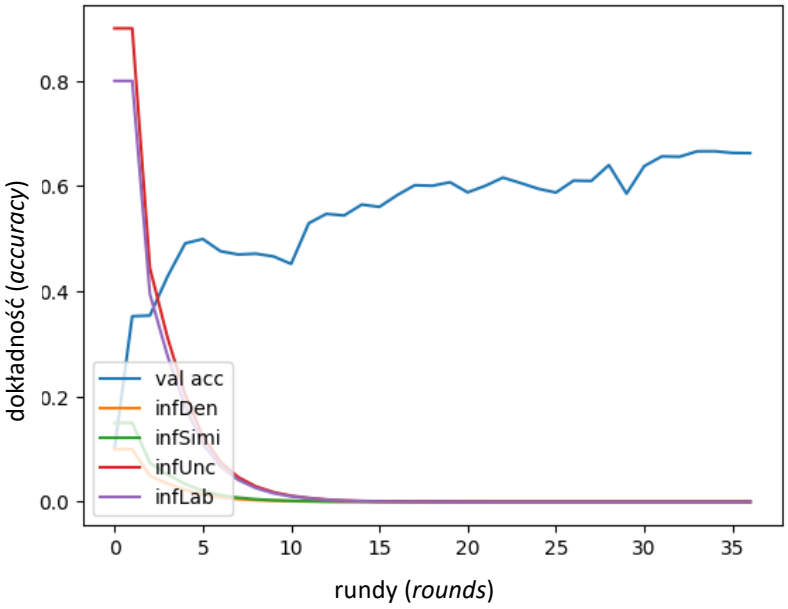


Rysunek 33 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8).

Na rysunku 33 widać, iż poszczególne kryteria (gęstość oznaczona, jako infDen i kolorem turkusowym, podobieństwo oznaczone, jako infSimi i kolorem zielonym, niepewność oznaczona, jako infUnc i kolorem pomarańczowym, kryterium oparte na etykietach oznaczone, jako infLab i kolorem żółtym) powiązane z oceną dokładności w każdej rundzie, dążą do zera, żeby dokładność mogła rosnąć. Podobnie mechanizm przedstawiał się we wszystkich innych eksperymentach, których wyniki zostały przedstawione na rysunkach 34 – 36.

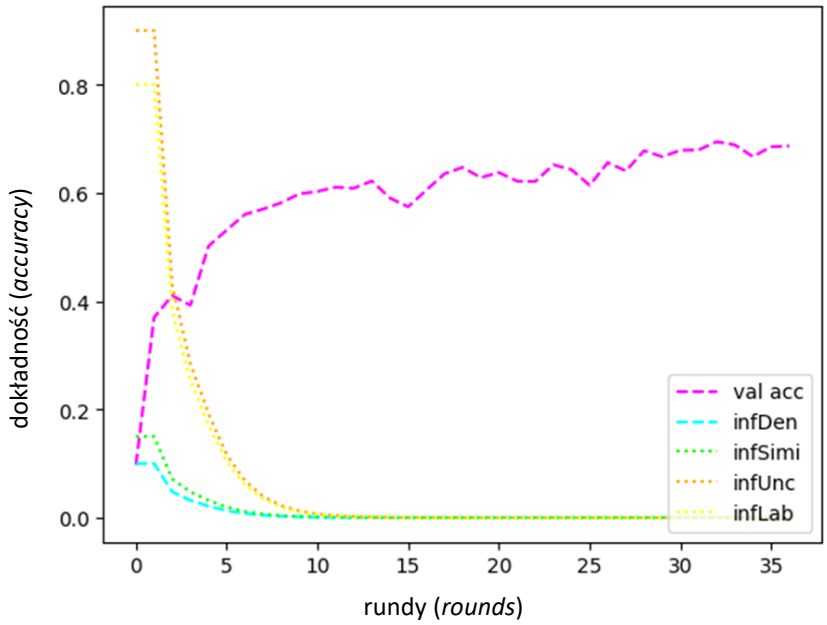
W przypadku wyników przedstawionych na rysunku 33 dokładność dla zbioru treningowego wyniosła 0,8495, a dla zbioru walidacyjnego 0,7367. Nawet jeśli wynik na zbiorze walidacyjnym był wysoki to uzyskana wartość oznacza, że algorytm miał problem z generalizacją. Rozpiętość pomiędzy wynikami na dwóch zbirach była zbyt duża.

Inaczej rezultat przedstawiał się dla inicjalizacji metodą *PCA-k-means*, na sieci CIFAR-10, który można zobaczyć na rysunku 34. Dokładność dla zbioru treningowego wyniosła 0,6991, a dla zbioru walidacyjnego 0,6637. Krzywa oznaczona na wykresie, jako *val acc* i kolorem różowym odzwierciedla poziom dokładności na zbiorze walidacyjnym. Oznacza to, że poziom uzyskanej dokładności nie osiągnął wysokiego poziomu, ale trening przebiegł w sposób umożliwiający uzyskanie proporcjonalnie wysokiej dokładności na zbiorze walidacyjnym. Wyniki przedstawione w pracy pokazują, że metoda inicjalizacji PCA-k-means nie przyczyniła się znacząco do osiągania wyższych poziomów dokładności, ale lepiej porządkuje przebieg nauczania przez algorytm, gdyż wyniki są w większości przypadków lepiej zsynchronizowane w relacji zbiór treningowy i zbiór walidacyjny.



Rysunek 34 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8).

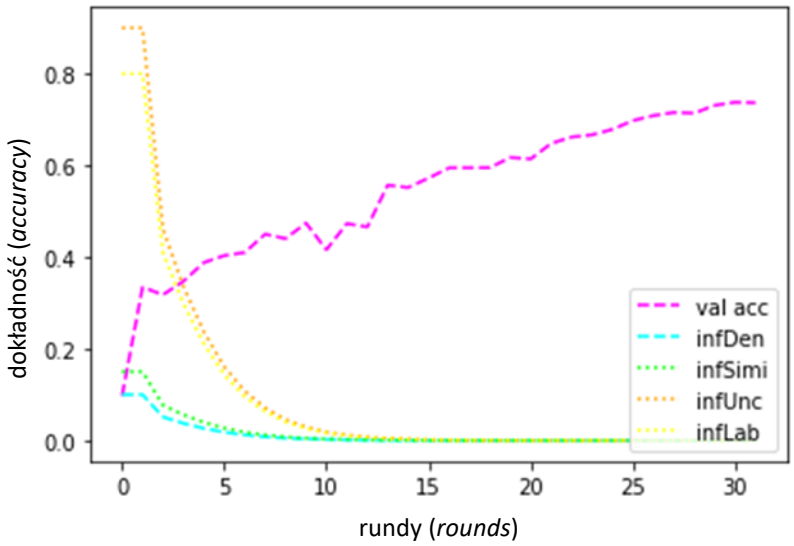
Na rysunku 35 ponownie przedstawiono przebieg działania algorytmu zainicjowanego metodą losową. Jego wynik jeszcze raz osiągnął wyższy poziom i kształtował się dla zbioru treningowego na poziomie 0,8745, natomiast dla zbioru walidacyjnego na poziomie 0,6869.



Rysunek 35 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8).

Na rysunku 36 przedstawiono jeden z najlepszych wyników osiągniętych nową metodą na sieci CIFAR-10. Dokładność dla zbioru treningowego wyniosła 0,7641, a dla zbioru walidacyjnego

0,7609.Krzywa oznaczona na wykresie, jako *val acc* i kolorem różowym odzwierciedla poziom dokładności na zbiorze walidacyjnym .



Rysunek 36 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8).

Należy zauważyć, że wyniki działania algorytmu z jednej strony wykazały, że metoda MCADL, zarówno z zastosowaniem ważenia, jak i punktów odniesienia daje najlepsze wyniki na zbiorze danych MNIST. Natomiast dla zbioru CIFAR-10, wyniki nowej metody nie osiągnęły poziomu dokładności na zbiorze walidacyjnym przekraczającego 0,8. Należy jednocześnie zaznaczyć, że nowa metoda pozwoliła na otrzymanie rezultatów przewyższających te uzyskane przez naukowców chińskich. Warto dla porównania wskazać, że oryginalna metoda MCADL, na zbiorze CIFAR-10 w najwyższym wymiarze osiągnęła poziom 0,595 [2]

Jednocześnie, pomimo zrealizowania eksperymentów na różnych architekturach sieci neuronowych implementacja zarówno MCADL, jak i nowej metody prezentowała rozbieżność między zbiorem treningowym, a walidacyjnym, co świadczy o nadmiernym dopasowaniu modelu. To spowodowało, że zdecydowano o kolejnej innowacji i w procesie klasyfikacji dodano etap pozwalający modelowi na osiągnięcie lepszych wyników. Zaimplementowano metodę *Margin Sampling* [80].

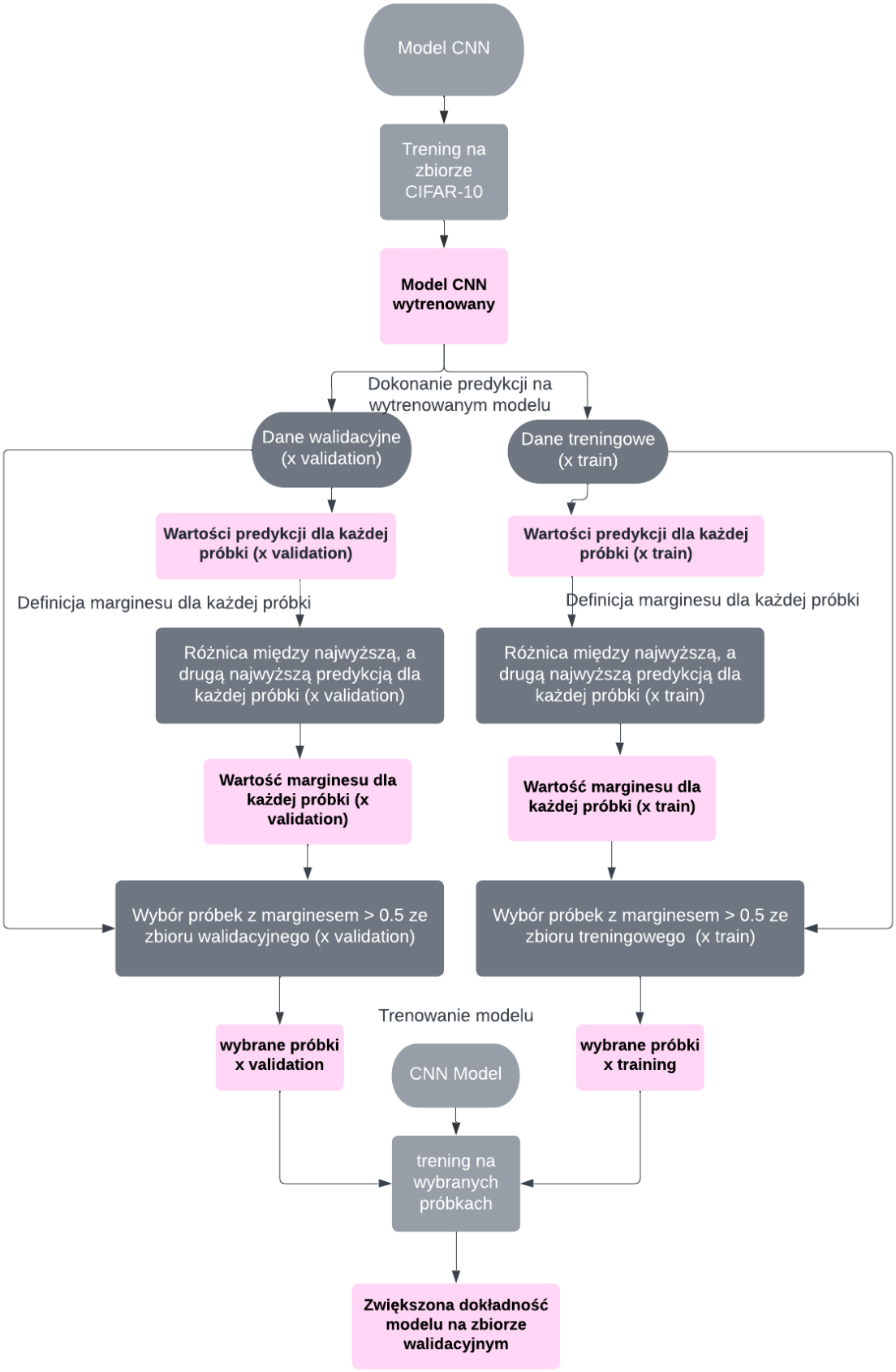
2.4.3. Nowe zakończenie algorytmu metodą *margin sampling* dla danych zbioru CIFAR-10

Metoda *margin sampling*, została wybrana z jednej strony z uwagi na prostotę działania, a z drugiej mając na względzie jej właściwości. Metoda poprawia jakość modelu klasyfikacyjnego poprzez selekcję próbek, dla których model jest mniej pewny w swoich predykcjach. Próbki te są bardziej skomplikowane i często znajdują się blisko granicy decyzyjnej, dlatego dokładniejsze ich zrozumienie może przynieść lepsze wyniki.

Ponadto szukając sposobu na wsparcie generalizacji w modelu wybrano *margin sampling*, gdyż przyczynia się do redukcji zbytniego dopasowywania się modelu do określonych cech. Metoda faworyzuje bowiem próbki trudne do sklasyfikowania, co pomaga uniknąć nadmiernej złożoności modelu. Metoda koncentrując się na próbkach znajdujących się wokół granicy decyzyjnej pozwala modelowi na bardziej precyzyjne nauczenie się różnic między klasami w trudnych obszarach, co z kolei przekłada się na lepszą zdolność klasyfikacji. Pomaga również w eliminacji próbek zakłócających, które mogą utrudniać nauczenie się modelu. Wybierając próbki bliskie granicy decyzyjnej, które są ważniejsze dla klasyfikacji, metoda ta pomaga w ograniczeniu wpływu próbek odstających i danych szumowych. Metoda umożliwia bardziej zrozumienie, dlaczego model dokonuje określonych predykcji.

Mając na względzie powyższe opracowano algorytm, który w pierwszym etapie pracuje na wytrenowanym modelu, zarówno metodą MCADL, jak i nową metodą z wykorzystaniem punktów odniesienia (w obu formułach, w celach porównawczych), a następnie przekazuje predykcje, co do zidentyfikowanych klas, do metody *margin sampling.* Na rys. 37 przedstawiono diagram działania nowej metody po dodaniu *margin sampling* w drugim etapie działania algorytmu.

Po wytrenowaniu modelu (na schemacie oznaczone, jako „model CNN wytrenowany”), dla każdej próbki przewidziana jest określona wartość. Z podanych predykcji wybierana jest ta próbka, której wartość jest największa oraz druga co do wielkości. Różnica między nimi wskazuje na margines pomiędzy jedną klasa i drugą, do której model przyporządkował dany obiekt. Taki sam proces odbywa się na zbiorze walidacyjnym. Następnie ze zbioru treningowego i walidacyjnego wybierane są te wszystkie instancje, które posiadają margines > 0,5, co oznacza, że znajdują się najbliżej granicy decyzyjnej modelu i tym samym stanowią dla niego największy problem w procesie uczenia się. Zdefiniowane w ten sposób pule instancji (treningowa i walidacyjna) podlegają ponownemu treningowi w ramach modelu, który był już wykorzystany na początku procesu klasyfikacji.

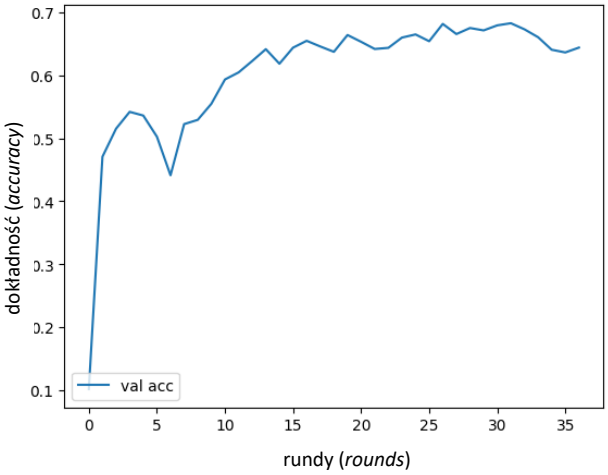


Rysunek 37 Diagram działania nowej metody z zaimplementowaną margin sampling, stanowiącą ostatni etap klasyfikacji.

Następuje ponowna inicjalizacja i trening z wykorzystaniem wcześniej przefiltrowanych danych oraz nadpisanie wyników. Skuteczność modelu została oceniona przy użyciu danych walidacyjnych (oznaczonych na schemacie, jako *x validation*) i treningowych (oznaczonych na schemacie, jako *x train*). Tryb *active learningu* czerpie tylko z tej puli, która stała się priorytetem dla modelu. W rezultacie, poprawa klasyfikacji pomiędzy opisanymi etapami procesu jest widoczna, co przedstawiono na przykładowych wynikach na rys. 38 – 41. Jednakże podkreślenia wymaga, iż dla wszystkich zrealizowanych eksperymentów model działa gorzej w oparciu o metodę MCADL, niż w ramach nowej metody, wykorzystującej punkty odniesienia.

Tabela 7 Wyniki działania modelu MCADL przed wyodrębnieniem puli próbek z marginesem kierującym do ponownego treningu

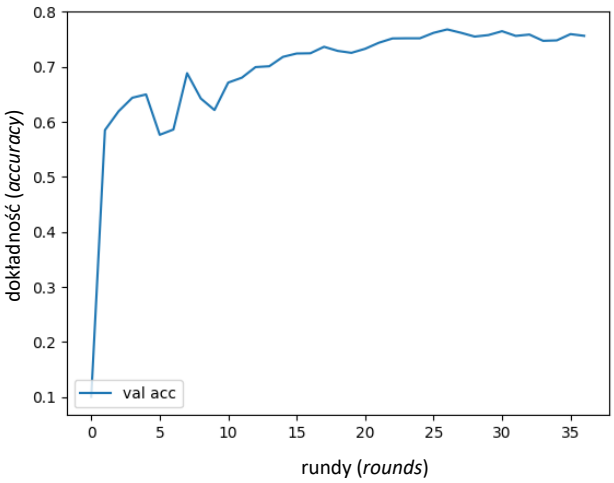
```
Round 23. Train acc=0.6909, Val acc=0.6649
Round 24. Train acc=0.6937, Val acc=0.6541
Round 25. Train acc=0.6966, Val acc=0.6816
Round 26. Train acc=0.6977, Val acc=0.6655
Round 27. Train acc=0.6940, Val acc=0.6751
Round 28. Train acc=0.6991, Val acc=0.6713
Round 29. Train acc=0.7002, Val acc=0.6793
Round 30. Train acc=0.7053, Val acc=0.6827
Round 31. Train acc=0.7067, Val acc=0.6730
Round 32. Train acc=0.7032, Val acc=0.6605
Round 33. Train acc=0.7137, Val acc=0.6406
Round 34. Train acc=0.7060, Val acc=0.6363
Round 35. Train acc=0.7116, Val acc=0.6440
```



Rysunek 38 Wykres działania modelu przed wyodrębnieniem puli próbek z marginesem kierującym do ponownego treningu

Tabela 8 Wyniki działania modelu MCADL po treningu z wykorzystaniem próbek z puli marginesu

```
Round 23. Train acc=0.7569, Val acc=0.7520
Round 24. Train acc=0.7658, Val acc=0.7619
Round 25. Train acc=0.7646, Val acc=0.7681
Round 26. Train acc=0.7660, Val acc=0.7620
Round 27. Train acc=0.7614, Val acc=0.7551
Round 28. Train acc=0.7617, Val acc=0.7578
Round 29. Train acc=0.7591, Val acc=0.7648
Round 30. Train acc=0.7643, Val acc=0.7563
Round 31. Train acc=0.7722, Val acc=0.7587
Round 32. Train acc=0.7711, Val acc=0.7474
Round 33. Train acc=0.7696, Val acc=0.7482
Round 34. Train acc=0.7756, Val acc=0.7596
Round 35. Train acc=0.7722, Val acc=0.7564
```



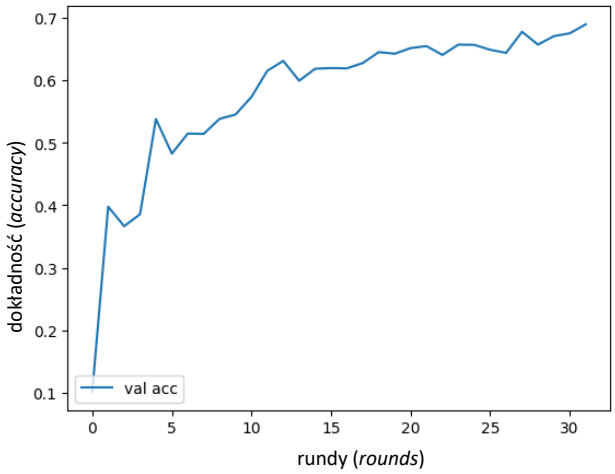
Rysunek 39 Wyniki działania modelu po treningu z wykorzystaniem próbek z puli marginesu

Tabela 7 oraz towarzyszący jej rysunek 38 przedstawiają wynik działania algorytmu MCADL, przed wyodrębnieniem puli próbek z marginesem. Dokładność na zbiorze walidacyjnym wyniosła 0,6440. Po dodaniu etapu w postaci metody *margin sampling* poprawie uległa zarówno dokładność, która osiągnęła wartość 0,7564, jak i generalizacja modelu. Widać, iż różnica pomiędzy wynikiem na zbiorze treningowym, a walidacyjnym posiada właściwa proporcję.

Należy jednak wskazać, iż nowa metoda, opierająca się o punkty odniesienia uzyskała lepszy rezultat. W przykładowej tabeli 9 i rysunku 40 widać, że wynik jest bardziej zrównoważony. To oznacza, że trening przebiegł z właściwym poziomem generalizacji i na zbiorze walidacyjnym osiągnął wyższy poziom niż metodą MCADL.

Tabela 9 Wyniki działania nowej metody przed wyodrębnieniem puli próbek z marginesem kierującym do ponownego treningu

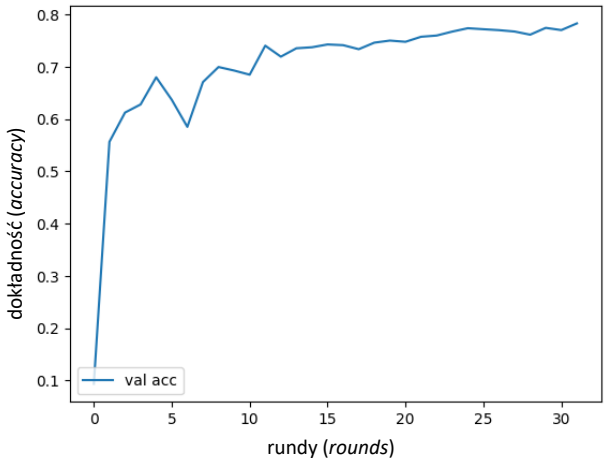
```
Round 16. Train acc=0.6827, Val acc=0.6275
Round 17. Train acc=0.6883, Val acc=0.6449
Round 18. Train acc=0.6929, Val acc=0.6423
Round 19. Train acc=0.6843, Val acc=0.6513
Round 20. Train acc=0.6947, Val acc=0.6545
Round 21. Train acc=0.6894, Val acc=0.6404
Round 22. Train acc=0.6976, Val acc=0.6569
Round 23. Train acc=0.6974, Val acc=0.6565
Round 24. Train acc=0.6910, Val acc=0.6486
Round 25. Train acc=0.6994, Val acc=0.6436
Round 26. Train acc=0.6943, Val acc=0.6774
Round 27. Train acc=0.6968, Val acc=0.6569
Round 28. Train acc=0.6999, Val acc=0.6704
Round 29. Train acc=0.6951, Val acc=0.6750
```



Rysunek 40 Wykres działania modelu przed wyodrębnieniem puli próbek z marginesem kierującym do ponownego treningu

Tabela 10 Wyniki działania nowej metody po treningu z wykorzystaniem próbek z puli marginesu

```
Round 17. Train acc=0.7772, Val acc=0.7461
Round 18. Train acc=0.7739, Val acc=0.7501
Round 19. Train acc=0.7737, Val acc=0.7477
Round 20. Train acc=0.7721, Val acc=0.7574
Round 21. Train acc=0.7767, Val acc=0.7597
Round 22. Train acc=0.7765, Val acc=0.7672
Round 23. Train acc=0.7780, Val acc=0.7737
Round 24. Train acc=0.7821, Val acc=0.7718
Round 25. Train acc=0.7802, Val acc=0.7700
Round 26. Train acc=0.7733, Val acc=0.7674
Round 27. Train acc=0.7800, Val acc=0.7613
Round 28. Train acc=0.7790, Val acc=0.7744
Round 29. Train acc=0.7848, Val acc=0.7701
```



Rysunek 41 Wyniki działania modelu po treningu z wykorzystaniem próbek z puli marginesu

Tabela 10 i rysunek 41 wskazują, iż nowa metoda, z punktami odniesienia, po dodaniu kolejnego etapu w postaci metody *margin sampling* osiągnęła najlepszy wynik, w ramach którego dokładność na zbiorze treningowym wyniosła 0,7848, a na zbiorze walidacyjnym 0,7701.

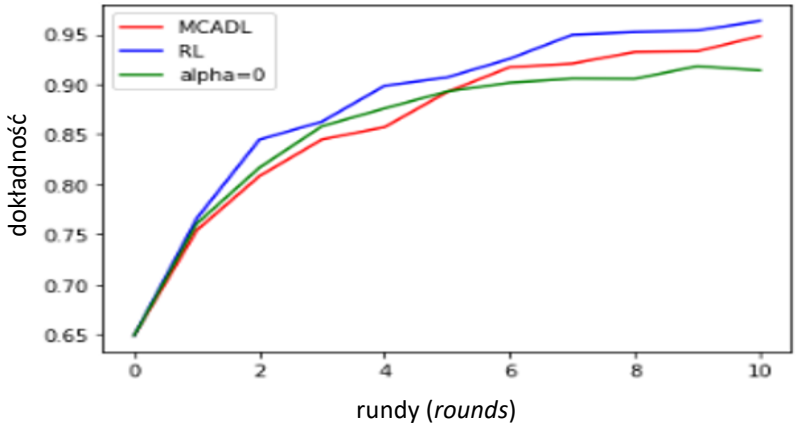
Wybór i trenowanie modelu na próbkach z większym marginesem pomaga w dostosowaniu modelu do trudniejszych przypadków i poprawie jego ogólnej skuteczności. Poprzez trenowanie na wybranych próbkach, spodziewano się zwiększenia dokładności modelu na zbiorze walidacyjnym przez jeszcze lepsze dopasowanie modelu do danych i lepszą generalizuję na nowe próbki spoza zbioru treningowego. Efekt został osiągnięty, co przedstawiono w niniejszej pracy.

Skuteczność zastosowanego podejścia zależy zawsze od specyfiki danych, problemu, a także innych czynników, ale podkreślenia wymaga fakt, iż w niniejszej pracy została potwierdzona. Dlatego warto eksperymentować i oceniać, jak dana technika wpływa na wyniki modelu.

ROZDZIAŁ IV
PRZEDSTAWIENIE WYNIKÓW PRAC I OBSZARU WDROŻENIA

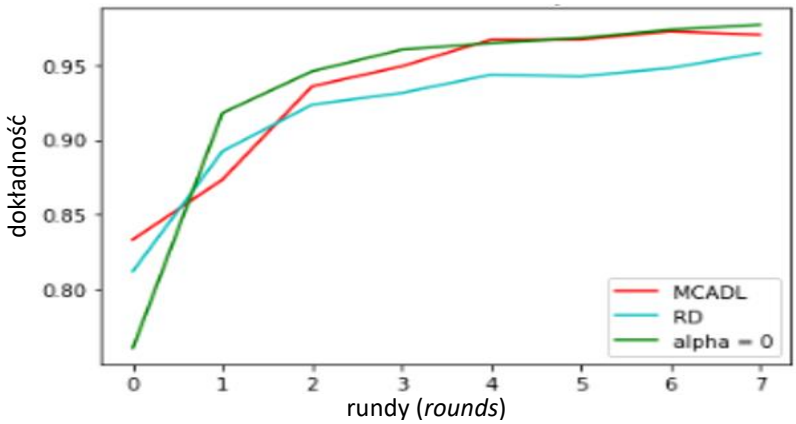
1. Przebieg prac i ich wyniki

Opisując zestawienie przebiegu prac należy wskazać, iż początkowym ich rezultatem był przegląd literaturowy, który pozwolił na wyodrębnienie z wielu innych metod klasyfikacji obrazu metodę MCADL, do dalszej analizy i zbadania. Najpierw dokonano implementacji własnej metody MCADL w technologii *Tensorflow* w celu sprawdzenia jej niezawodności oraz natury i charakteru poszczególnych kryteriów, które były badane. Stwierdzono niską (1/10) skuteczność metody MCADL.



Rysunek 42 Wyniki działania metody MCADL, w porównaniu z metodą losową (RL) oraz metodą z założeniem wagi α na poziomie „0".

W zdecydowanej większości eksperymentów, dokładność klasyfikacji w odniesieniu do metody losowej lub z wykorzystaniem wagi $\alpha = 0$ dawała lepsze lub co najmniej porównywalne wyniki, co zostało przedstawione w rozdziale III na rysunkach 13 - 16 oraz w rozdziale IV, na rysunkach 42 i 43.

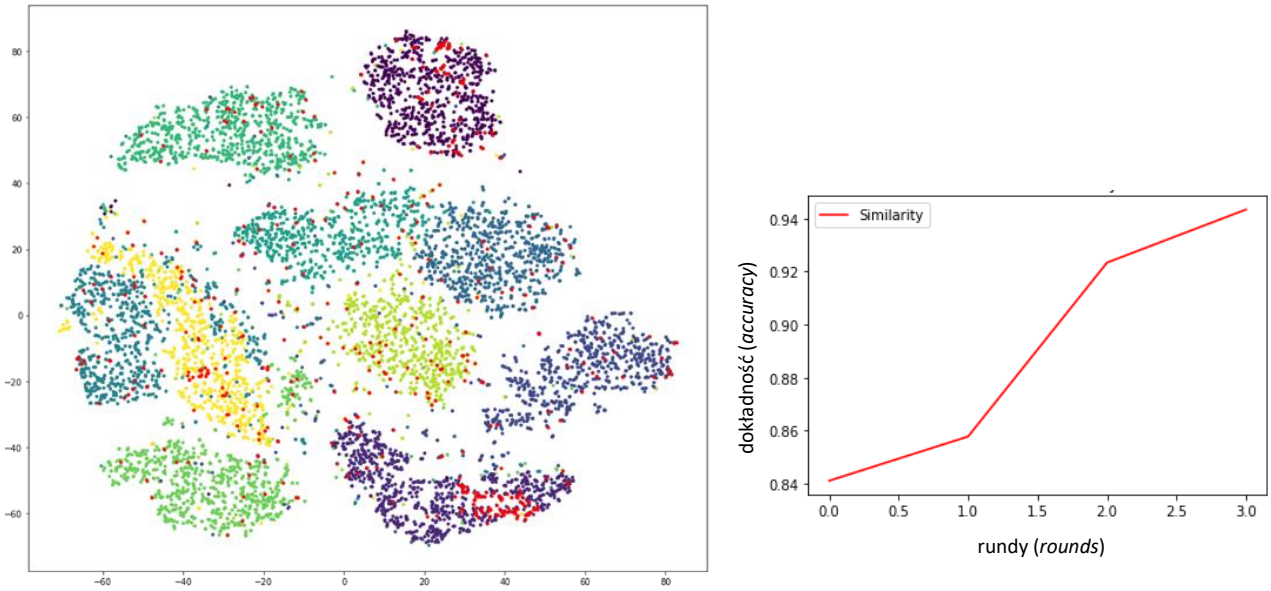


Rysunek 43 Wyniki działania metody MCADL, w kontekście metody losowej (RL) oraz metody z założeniem wagi α na poziomie „0".

Działanie metody MCADL, odzwierciedlone na rysunkach 42 i 43 czerwoną krzywą wskazuje, iż dokładność klasyfikacji w jej zakresie posiadała wysoki poziom na zbiorze MNIST, natomiast w zestawieniu z zaimplementowaną metodą losową oraz metodą, w ramach której waga α (wzmacniająca w metodzie MCADL kryterium podobieństwa i gęstości) jest równa „0" uzyskała poziom minimalnie lepszy lub minimalnie gorszy, ale nigdy nie przewyższyła obydwu metod w sposób systematyczny i przejrzysty.

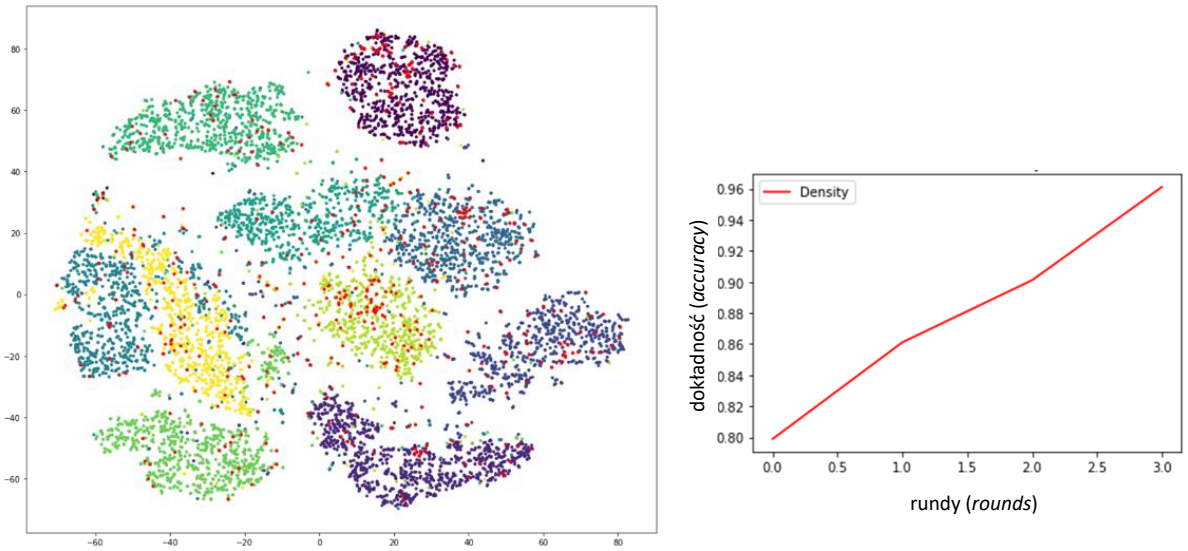
Chcąc wprowadzić znaczącą modyfikację algorytmu MCADL w postaci zaimplementowania punktów odniesienia w miejsce wag, w kolejnym kroku przeprowadzono analizę ukierunkowaną na zbadanie zachowania się poszczególnych kryteriów w celu znalezienia wzorca pozwalającego na zdefiniowanie ich poziomów referencji.

W tym zakresie dokonano wizualizacji interaktywnego (plik gif, t-sne) rozmieszczenia próbek w ramach danego kryterium i osiąganego poziomu dokładności danego kryterium. Wyniki tego procesu przedstawiono na rysunkach 44 - 47.



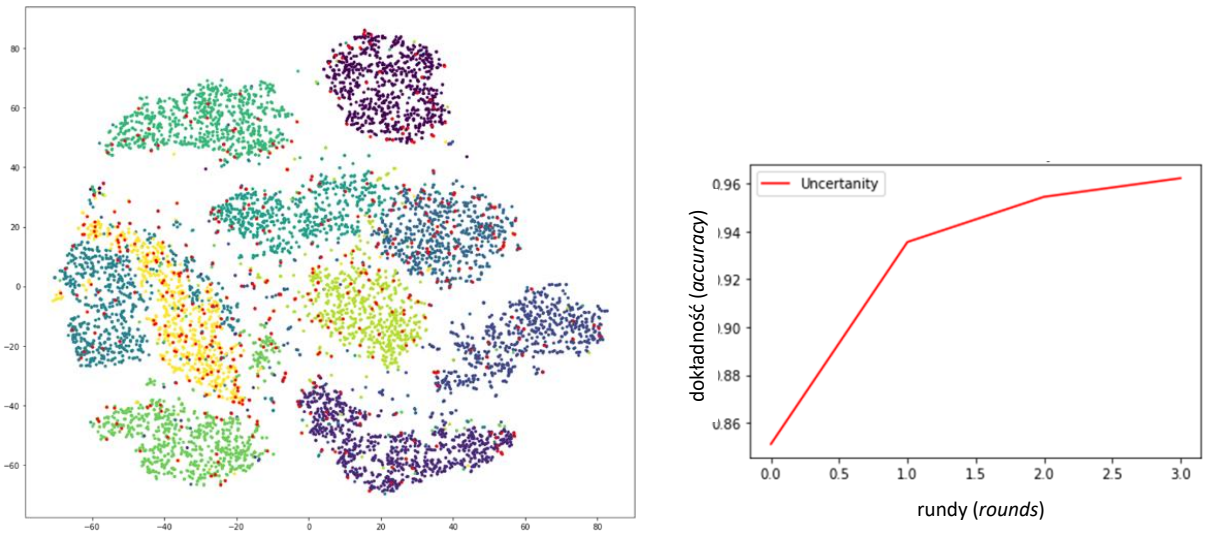
Rysunek 44 Wybór próbek według kryterium podobieństwa (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu.

Na rysunku 44, po lewej stronie wykres przedstawia rozmieszczenie 10 klas (próbek z etykietami) i umiejscowienie na nich próbek (oznaczonych, jako czerwone kropki) pobieranych przez algorytm zgodnie z kryterium podobieństwa. Widać, że najwięcej zostało pobranych z klasy oznaczonej kolorem ciemno-fioletowym. Dokładność działania tego kryterium została przedstawiona na wykresie po prawej stronie i wskazuje, że 94% poziom został osiągnięty w trzeciej rundzie.



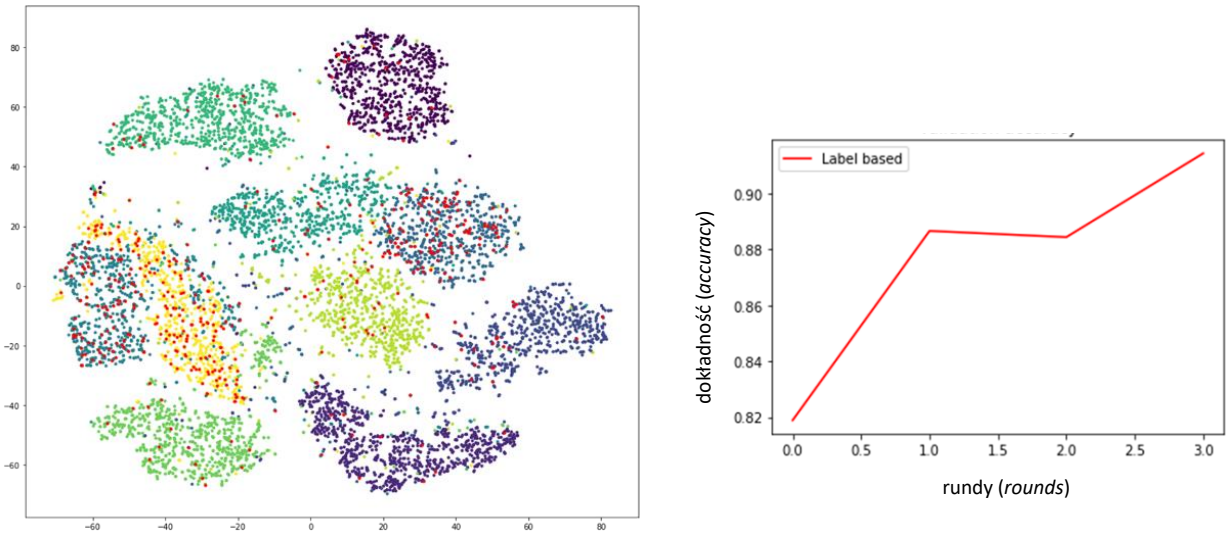
Rysunek 45 Wybór próbek według kryterium gęstości (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu.

Na rysunku 45, po lewej stronie odzwierciedlono pobieranie próbek przez algorytm według kryterium gęstości. Model ponownie zdecydował o pobraniu największej puli z klasy oznaczonej kolorem ciemno-fioletowym. Dokładność działania kryterium gęstości została przedstawiona na wykresie po prawej stronie i wskazuje, że w trzeciej rundzie dokładność sięga już 96%.



Rysunek 46 Wybór próbek wg kryterium niepewności (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu.

Na rysunku 46, po lewej stronie odzwierciedlono pobieranie próbek przez algorytm według kryterium niepewności. Widać, że rozłożenie pobierania próbek jest bardziej równomierne i rozkłada się podobnie we wszystkich klasach. Dokładność działania kryterium niepewności została przedstawiona na wykresie po prawej stronie i wskazuje, że w trzeciej rundzie sięga już 96%.



Rysunek 47 Wybór próbek wg kryterium opartego na etykietach (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu.

W odniesieniu do działania kryterium opartego na etykietach można stwierdzić, że są trzy klasy podlegające jego „szczególnemu zainteresowaniu", oznaczone na rysunku 47 po lewej stronie kolorami turkusowym, niebieskim i żółtym. Dokładność osiąga poziom ponad 90% w trzeciej rundzie, ale wzrost dokładności przebiega w sposób mniej równy niż w przypadku pozostałych kryteriów.

Analiza wykresów i wizualizacji przedstawionych na rysunkach 44 - 47 ukazuje różne zachowania poszczególnych kryteriów w trakcie działania algorytmu. Każde kryterium ma swoje specyficzne cechy i wpływ na proces wyboru próbek przez algorytm. Ważne jest zrozumienie tych różnic i odpowiednie dostosowanie parametrów algorytmu oraz definiowanie punktów odniesienia dla poszczególnych kryteriów, aby poprawić jego skuteczność i efektywność w procesie uczenia się. Biorąc pod uwagę uzyskane w tym kroku wyniki należy stwierdzić, że nie uzyskano wskazówek pozwalających na jednoznaczne określenie poziomów odniesienia do których algorytm powinien dążyć.

W kolejnym kroku dokonano wyodrębnienia każdego kryterium i zbadania jego zachowania względem funkcji straty. Wyniki tego procesu przedstawiono w rozdziale II, na rysunku 13. Przeprowadzona analiza nie pozwoliła na zdefiniowanie wzorca, który mógłby posłużyć do dalszej zmiany algorytmu. Nie znaleziono uzasadnienia do wykluczenia któregokolwiek z kryteriów.

Następnie zaimplementowano metodę MCADL we framework'u *Pytorch*. W nowym kodzie przeprowadzono drugą turę eksperymentów i dokonano zasadniczych zmian w algorytmie:

a) W zakresie sposobu inicjalizacji (oprócz metody losowego doboru puli wyjściowej zastosowano *PCA – k-means*).
b) Wprowadzono mechanizm zastępujący ważenie kryteriów punktami odniesienia wyznaczonymi funkcją maksiminową.
c) Dla danych ze zbioru CIFAR-10, który jest bardziej złożony niż dane ze zbioru MNIST, dodano na końcowym etapie treningu metodę *margin sampling*.

W zakresie zmiany sposobu inicjalizacji z losowej na *PCA-k-means* warto wskazać, że wysiłek obliczeniowy okazał się większy niż w wyniku zastosowania inicjalizacji losowej. Nie zawsze też inicjalizacja *PCA-k-means* dawała znacząco lepsze rezultaty, aczkolwiek tak skonstruowana metoda wykazała większą stabilność treningu oraz właściwą generalizację modelu.

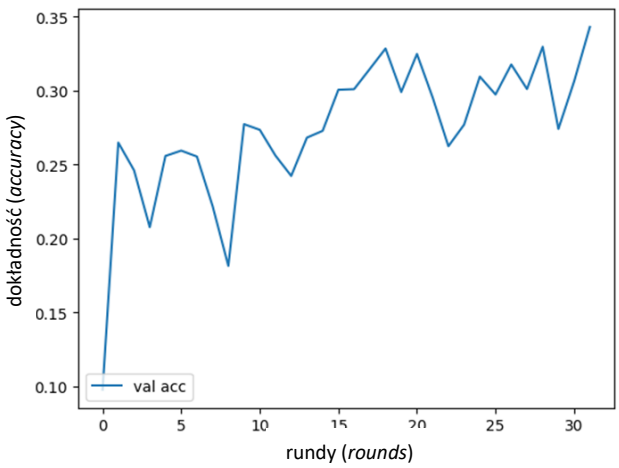
Zastosowane punkty odniesienia w trakcie działania nowego algorytmu dążyły do poziomu bliskiego „0”. Taki trend powodował, że dokładność rosła, a model uczył się lepiej. Dokonanie wyboru poziomów odniesienia w powiązaniu z poziomem dokładności zostało przeprowadzone dzięki zastosowaniu funkcji maksiminowej, o której napisano w rozdziale III.

Wykresy na rysunkach 48 - 51 przedstawiają poziom dokładności zastosowanych metod wielokryterialnych.

Na rysunku 48 i w tabeli 11 przedstawiono wynik metody MCADL.

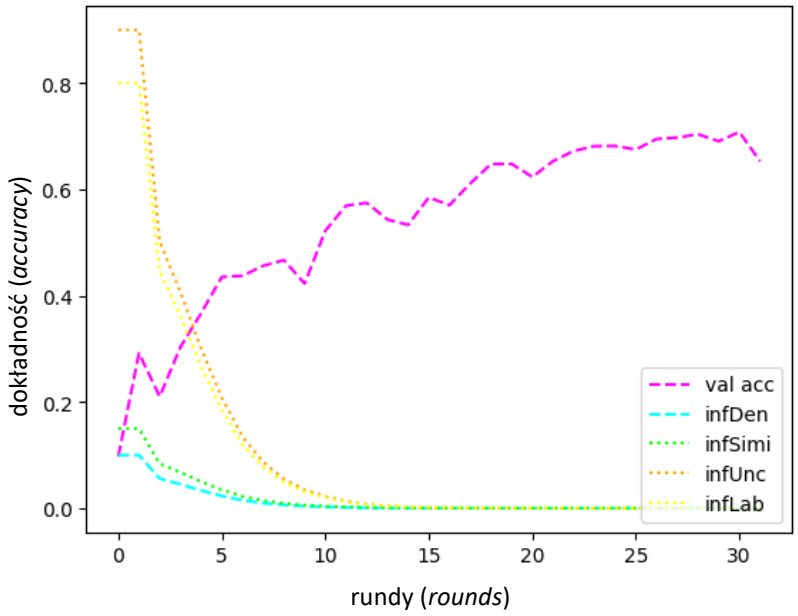
Tabela 11 Wyniki metody MCADL

```
Round 11. Train acc=0.3029, Val acc=0.2423
Round 12. Train acc=0.3195, Val acc=0.2682
Round 13. Train acc=0.2795, Val acc=0.2728
Round 14. Train acc=0.3261, Val acc=0.3006
Round 15. Train acc=0.3317, Val acc=0.3010
Round 16. Train acc=0.3305, Val acc=0.3147
Round 17. Train acc=0.3355, Val acc=0.3285
Round 18. Train acc=0.2966, Val acc=0.2991
Round 19. Train acc=0.3184, Val acc=0.3248
Round 20. Train acc=0.3159, Val acc=0.2953
Round 21. Train acc=0.3090, Val acc=0.2624
Round 22. Train acc=0.3360, Val acc=0.2770
Round 23. Train acc=0.3030, Val acc=0.3095
Round 24. Train acc=0.3392, Val acc=0.2974
Round 25. Train acc=0.3500, Val acc=0.3177
Round 26. Train acc=0.3296, Val acc=0.3011
Round 27. Train acc=0.3485, Val acc=0.3297
Round 28. Train acc=0.3248, Val acc=0.2741
Round 29. Train acc=0.3249, Val acc=0.3063
Round 30. Train acc=0.3418, Val acc=0.3431
```



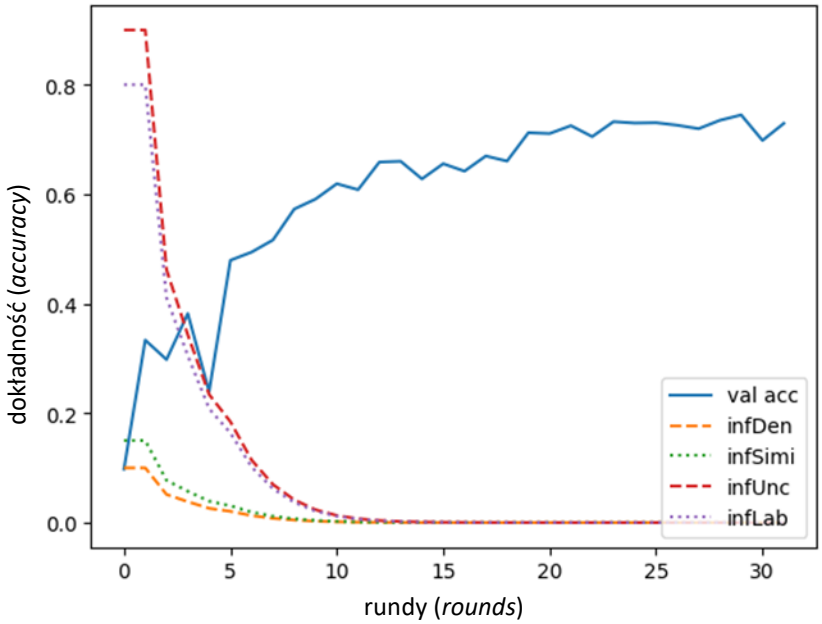
Rysunek 48 Wykres przedstawiający wyniki działania oryginalnej metody (MCADL)

Na rysunku 49 przedstawiono wynik działania nowej metody, inicjalizowanej losowo.



Rysunek 49 Wykres wyników nowej metody z punktami odniesienia (inicjalizacja losowa)

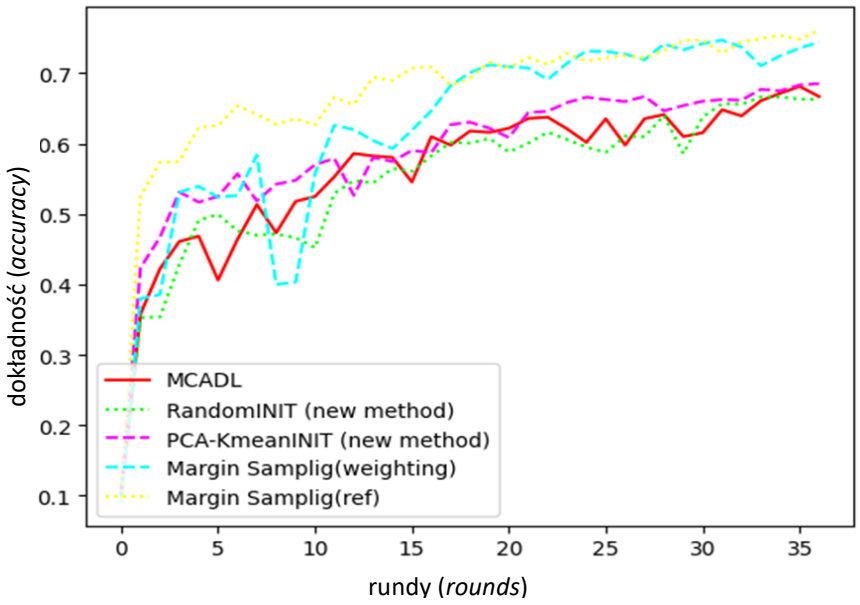
Na rysunku 50 przedstawiono wynik działania nowej metody, inicjalizowanej *PCA-k-means*.



Rysunek 50 Wykres wyników nowej metody z punktami odniesienia (inicjalizacja PCA – k-means)

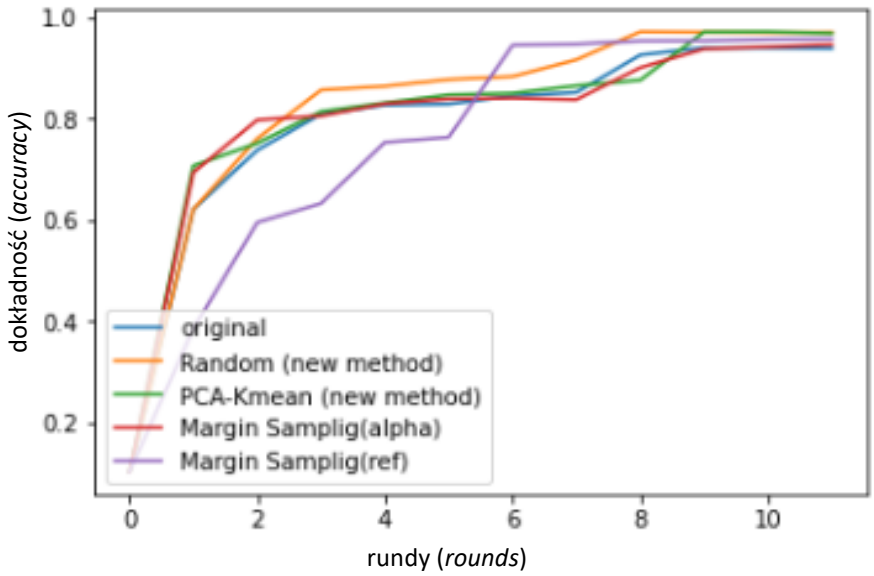
Metody wykorzystujące punkty odniesienia, w większości zrealizowanych eksperymentów, dały najlepsze wyniki. Zarówno w wymiarze nowej metody wielokryterialnej z punktami odniesienia, jak i po dodaniu etapu *margin sampling* z punktami odniesienia dokładność osiągała najwyższe poziomy i poprawiła działanie klasyfikacji na zbiorze CIFAR-10, co przedstawiają przykładowe wykresy zestawiające zaimplementowane metody

na rysunkach 51 - 55. W przeprowadzonych eksperymentach agregujących działanie algorytmu zaimplementowanymi metodami widać, że metoda MCADL (oznaczona, jako MCADL lub *original*) osiąga najgorsze, lub prawie najgorsze wyniki.



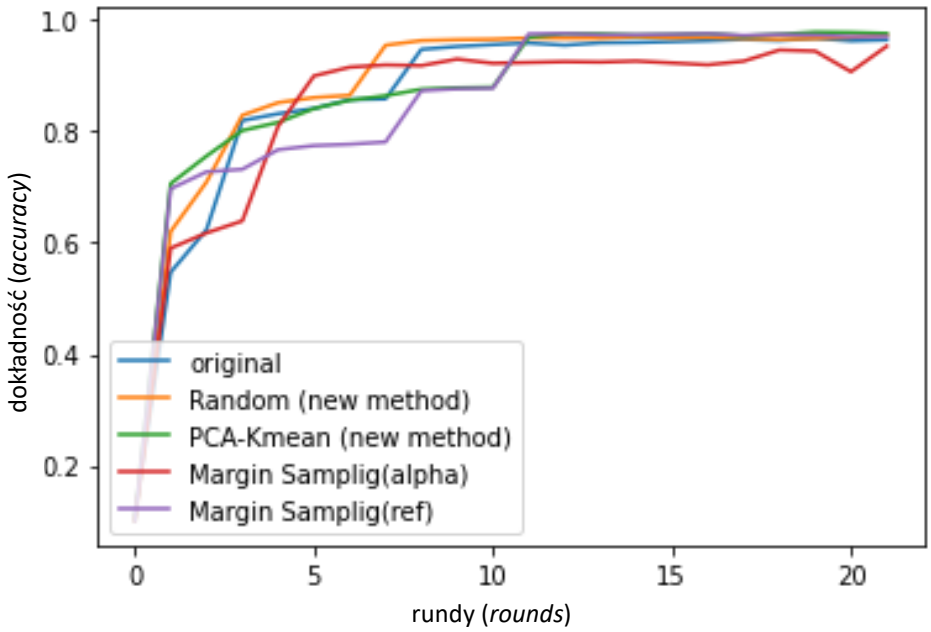
Rysunek 51 Wyniki działania metody MCADL, nowej metody (ang. new method) z inicjalizacją losową oraz inicjalizacją PCA – k-means, oraz z uwzględnieniem metody margin sampling.

Na rysunku 51 najlepszy rezultat osiągnął algorytm *margin sampling* z punktami odniesienia (krzywa oznaczona, jako Margin Sampling(ref) i kolorem żółtym), który czerpał z nowej metody z punktami odniesienia. Metoda MCADL uzyskała gorszy wynik, ale w przykładzie widać, że nowa metoda zainicjalizowana losowo nie osiągnęła lepszego rezultatu.

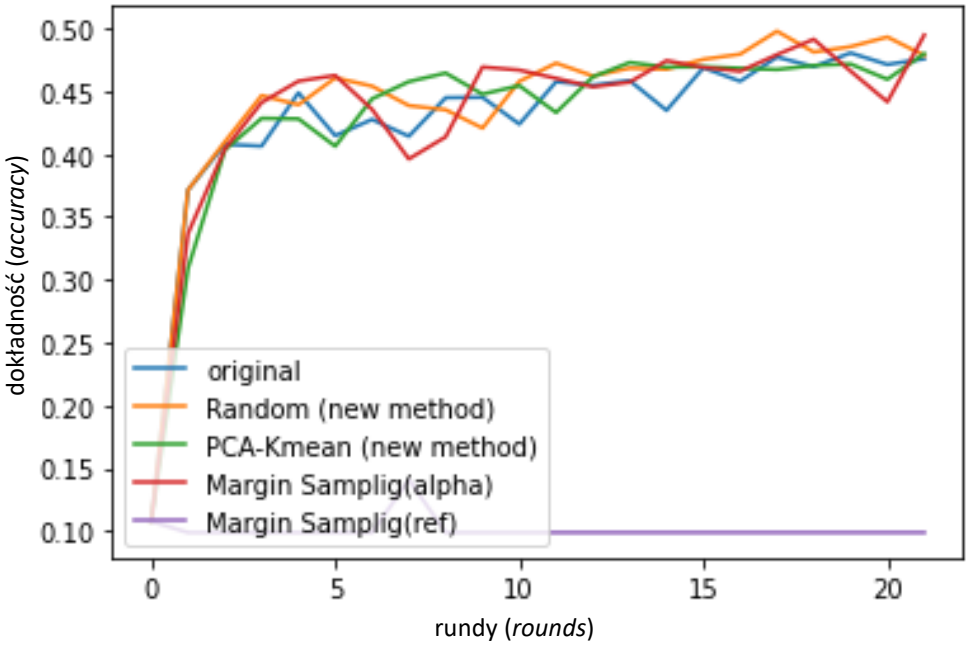


Rysunek 52 Wyniki działania nowej metody (ang. new method) w kontekście metody MCADL, oraz dodanej metody margin sampling zastosowanej z uwzględnieniem wag oraz metody margin sampling z zastosowaniem punktów odniesienia, gdzie oś pionowa wskazuje na poziom dokładności, a oś pozioma na liczbę rund, na bazie MNIST

Na rysunku 52 najlepszy rezultat osiągnęła nowa metoda, zarówno inicjalizowana losowo, jak i metodą *PCA-k-means*, która na poziomie 9 rundy osiągnęła dokładność na jednakowym poziomie. Bardzo zbliżony poziom został uzyskany przez metodę *margin sampling* bazującą na punktach odniesienia.



Rysunek 53 Wyniki działania nowej metody (ang. new method) w kontekście metody MCADL, oraz dodanej metody margin sampling zastosowanej z uwzględnieniem wag oraz metody margin sampling z zastosowaniem punktów odniesienia, gdzie oś pionowa wskazuje na poziom dokładności, a oś pozioma na liczbę rund, na bazie MNIST



Rysunek 54 Wyniki działania nowej metody (ang. new method) w kontekście metody MCADL, oraz dodanej metody margin sampling zastosowanej z uwzględnieniem wag oraz metody margin sampling z zastosowaniem punktów odniesienia, gdzie oś pionowa wskazuje na poziom dokładności, a oś pozioma na liczbę rund, na bazie MNIST

Mając na względzie, iż w odniesieniu do bazy CIFAR-10, dokładność na zbiorze walidacyjnym, nie przekraczyła poziomu 80% można więc stwierdzić, że założenia matematyczne dla sformułowania czterech kryteriów wymagają dalszych prac, gdyż algorytm osiąga znaczaco lepsze rezultaty dla bazy czarno-białej niż dla kolorowej.

2. Rozpoznanie wojskowe

2.1. Rys historyczny

Skuteczne rozpoznanie [81] jest kluczowym warunkiem prowadzenia każdego rodzaju działań wojennych. Informacyjne przygotowanie pola walki, (IPB, ang. *intelligence preparation of the battlefield)* jest systematycznym i ciągłym (także w trakcie operacji) procesem zbierania i analizowania informacji na temat zagrożeń oraz środowiska w specyficznym rejonie geograficznym. Powodzenie misji zależy od prawidłowej analizy dostępnych informacji na etapie planowania. Obecnie metody ich zbierania zmieniły się dzięki szybkiej dostępności informacji bojowych o wysokiej jakości i wiarygodności, pochodzących z różnych czujników i źródeł [15].

Literatura dotycząca systemów rozpoznania pola walki jest obszerna. Ich definicja zależy od wielu czynników, w tym: kontekstu, w jakim są prezentowane dane; celu, jakiemu służą systemy; rodzaju sił zbrojnych czy instytucji, która kieruje jego rozwojem. Jednym z istotnych wyznaczników organizacji systemu rozpoznania jest rodzaj zagrożenia - również w tym zakresie obszar definicyjny będzie zróżnicowany. Przez stulecia termin *rozpoznanie*, używany w dziedzinie wojskowości, rozpatrywany był głównie w kontekście działalności człowieka.

Pierwsze opisy działań zwiadowczych znajdujemy w księgach Starego Przymierza. Służby wywiadowcze były integralną częścią sił zbrojnych od starożytności. Monarchie absolutne XVII i XVIII wieku przywiązywały wagę do terminowego rozpoznania zamiarów potencjalnych przeciwników [82]. W czasie wojny francusko – austriackiej w 1794 roku pioniersko użyto balonów na potrzeby wykonania obserwacji. Był to początek wykorzystania przestrzeni powietrznej do celów wojskowych [83]. Jednak pierwsze, formalne komórki wywiadowcze powstały w XIX wieku, niemal równocześnie w Niemczech i Francji.

Wagę i znaczenie systemów rozpoznawczych dla XX wieku w sposób uniwersalny zaprezentował oficer Cesarskiej Armii Rosyjskiej - Aleksander Iwanowicz Kuk – który w 1921 roku stwierdził, że zwycięstwo danego państwa zależy przede wszystkim od [84]:

- „*znajomości planu wojennego prawdopodobnego przeciwnika (przeciwników) przez dane państwo oraz stopnia faktycznej skuteczności jego realizacji;*

– *utrzymania w tajemnicy wszystkiego, co dane państwo wymyśliło i zrealizowało w swoim planie wojennym*".

Przełom w rozwoju obszaru rozpoznania przyszedł wraz z pierwszym konfliktem zbrojnym o zasięgu globalnym. Pojawiły się nowe techniki: łączność radiowa i telefoniczna; nowe możliwości dla praktyk rozpoznawczych: fotografia lotnicza (choć prowadzenie rozpoznania z powietrza, datuje się już od konfliktu włosko-tureckiego w Libii w 1911 r.), wojska desantowe. Jednym z najważniejszych wynalazków związanych z dziedziną wywiadu były maszyny do szyfrowania informacji – w tym najbardziej znana Enigma. Złamanie systemu jej funkcjonowania przez polskich matematyków i przekazanie tej wiedzy aliantom miało znaczący wpływ na losy II wojny światowej. Niebagatelne znaczenie dla rozwoju systemów rozpoznania okresu wojennego miało również uruchomienie stacji radiolokacyjnych, które umożliwiły koordynację sił powietrznych i przyczyniły się znacząco do wygranych aliantów (jak Bitwa o Anglię). Niemcy włączyli radary do obrony przeciwlotniczej już w 1940 roku. Rosja również wyciągnęła wnioski i najważniejsze posterunki polowe zostały wyposażone w stacje radiolokacyjne [83].

Wraz z rozwojem technologii, wojskowe systemy rozpoznawcze były doskonalsze, a ich poszczególne elementy coraz bardziej wyspecjalizowane. Obecnie coraz częstsze wynoszenie i wykorzystywanie satelitów obserwacyjnych, radarowych i zwiadowczych oraz zdynamizowanie rozwoju rynku bezzałogowych statków powietrznych spowodowało, że rozpoznanie pola walki w oparciu o analizę obrazu stało się jedną z najpowszechniejszych i najskuteczniejszych metod rozpoznania.

2.2. Przetwarzanie obrazu na rzecz wojskowych systemów rozpoznania

Współczesny, dynamiczny rozwój technologiczny wymaga szczegółowego spojrzenia na zakres systemów rozpoznania. NATO nie posiada autonomicznych sił i środków w obszarze systemów wywiadowczych (ang. *ISR - Intelligence, Surveillance and Reconnaissance*) dlatego podczas prowadzenia operacji wykorzystuje się zarówno wydzielone, jak i narodowe zdolności ISR. Logika tego obszaru została przedstawiona w Sojuszniczej Wspólnej Doktrynie Wywiadu, Kontrwywiadu i Bezpieczeństwa (ang. *Allied Joint Doctrine for Intelligence, Counterintelligence and Security*) i ujęta trzy-zakresowo, jako wywiad, obserwacja i rozpoznanie.

Wywiad definiuje się jako *"(...) działania wynikające z bezpośredniego zbierania i przetwarzania informacji (...)*" [85]. Wyróżnia się kilkanaście rodzajów wywiadu wojskowego, a wśród nich przedstawione w tabeli 12.

Tabela 12 Lista rodzajów wywiadu

HUMINT	Ang. *Human Intelligence* W tej dziedzinie, mimo dominacji technologicznej we współczesnym świecie, niezwykle istotna jest rola człowieka. „Konflikty zbrojne w Iraku i Afganistanie w znaczący sposób zmieniły podejście do prowadzenia rozpoznania operacyjnego. Tam najważniejszym elementem rozpoznania był człowiek i jego środowisko" [86].
OSINT [87]	Ang. *Open Source Intelligence*, tzw. biały wywiad. Informacje są pozyskiwane z publicznie dostępnych źródeł: serwisów społecznościowych, specjalizowanych (serwisy mapowe) i dedykowanych (serwisy udostępniające narzędzia szpiegowskie za opłatą), zdjęcia, video itp. Prowadzenie działań wywiadowczych w tym zakresie nazywane jest też rozpoznaniem pasywnym.
SIGINT	Ang. *Signal Intelligence* – wywiad sygnałowy. Opiera się na analizie fal elektromagnetycznych oraz sygnałów pochodzących z systemów komunikacji (Ang. *Communication Intelligence*), radarowych lub innych. W ramach SIGINT rozróżnia się dwie podkategorie COMINT i ELINT.
COMINT	Ang. *Communication Intelligence* – analiza różnych kanałów komunikacji: radiowych, telefonicznych, satelitarnych, smsowych, w ramach której badaniu podlegają m.in. częstotliwości, nadajniki, czas trwania sygnału.
ELINT	Ang. *Electronic Signals Intelligence* – obejmuje analizę sygnału elektronicznego, który nie jest rozmową lub tekstem (zarezerwowane dla COMINT). Ma szczególne zastosowanie w zakresie Walki Radio-Elektronicznej (WRE), kiedy to koncentruje się na lokalizowaniu konkretnych celów ELINT. Uwzględnia w dużej części analizę telemetryczną polegającą na przechwytywaniu, przetwarzaniu i raportowaniu obcych telemetrii.
GEOINT	Ang. *Geospatial Intelligence* [88] - wywiad geoprzestrzenny. Polega na wykorzystaniu oraz analizie obrazu i informacji geoprzestrzennej do opisu, oceny i wizualizacji cech fizycznych, a także lokalizacji różnego rodzaju działalności na Ziemi (np. elektrowni jądrowych czy baz terrorystów). Wynikiem działań ISR i fuzji danych jest stworzenie wielowarstwowej informacji geoprzestrzennej.
IMINT	Ang. *Image Intelligence*- analiza obrazu. Zgodnie z najnowszymi ustaleniami literaturowymi, stanowi integralną część GEOINT [89]. Uwzględnia badania m.in. obrazów elektrooptycznych, podczerwonych, radarowych i wideo.
MASINT [90]	Ang. *Measurement and Signature Intelligence* Wywiad pomiarowo - badawczy. Obejmuje analizę wielu rodzajów danych w różnych typach środowisk. Zgodnie, z poniższym:

	ACINT	Ang. *Acoustical Intelligence* – skupia się przede wszystkim na badaniu sygnałów podmorskich pochodzących zarówno z łodzi podwodnych, jak i innych obiektów ulokowanych pod wodą.
	RADINT	Ang. *Radar Intelligence* – rozpoznanie radiolokacyjne, radiotechniczne.
	RINT	Ang. *Unintentional Radiation Intelligence* Polega na badaniu informacji o niezamierzonej radiacji pochodzącej z różnego rodzaju elektronicznych i elektrycznych obiektów.
	CBNINT	Ang. *Chemical and Biological Intelligence* Obejmuje prowadzenie zarówno tradycyjnych analiz chemicznych, jak i materiałów biologicznych, w tym przeprowadzanie zaawansowanych badań w laboratoriach mikrobiologicznych.
	DEWINT	Ang. *Directed Energy Weapons Intelligence* Wywiad skierowany na badanie broni wiązkowej, różnych aspektów energii kierowanej.
	NUCINT	Ang. *Nuclear Intelligence* Polega m.in. na monitorowaniu testów jądrowych oraz analizie emisji radioaktywnych próbek.
	EMPINT	Ang. *Electromagnetic Pulse Intelligence* Badanie impulsu elektromagnetycznego. Oprócz piorunów i wyładowań statycznych, impulsy mogą być generowane przez radar lub broń, stworzoną do niszczenia sprzętu elektronicznego.
	ELECTRO-OPTINT	Ang. *Electro-optical Intelligence* – polega na optycznej analizie spektrum elektromagnetycznego od ultrafioletu (0,01 mikrometra) do dalekiej podczerwieni (1000 mikrometrów).
	LASINT	Ang. *Laser Intelligence* Podkategoria wywiadu opto-elektronicznego, w ramach której podejmowane są działania na rzecz zbadania sygnałów pochodzących z systemów laserowych.
	MATE-RIALS INTELLI GENCE	Polega na badaniu różnorodnych materiałów: tradycyjnych lub innowacyjnych. W przypadku tych ostatnich coraz powszechniej używa się dedykowanego oprogramowania, które pozwala na zdefiniowanie materiału, a także jego/ich łączenie. Analizie podlega kształt materiału, surowce, z których jest wykonany lub miejsce produkcji.
	IRINT	Ang. *Infrared Intelligence* Obejmuje gromadzenie i analizowanie danych pochodzących z zakresu podczerwieni.

Źródło: Opracowanie własne na podstawie danych *Federation of American Scientists (FAS).*

Wywiad odgrywa kluczową rolę we wspieraniu dowódców w podejmowaniu decyzji w całym spektrum operacji wojskowych. Skuteczność działań wywiadowczych polegających na pozyskiwaniu informacji o zasobach i ruchach przeciwnika zależy od czasu pozyskania i wiarygodności danych [91]. W trakcie konfliktu zbrojnego szczególnie istotne jest,

by informacje wywiadowcze były przekazywane w czasie rzeczywistym. Dowódcy wykorzystują je do przewidywania, wizualizacji i zrozumienia sytuacji operacyjnej. Bezpieczeństwo, właściwy zakres i precyzja danych jest niezbędna dla funkcjonowania procesu prowadzenia operacji wojskowych i zarządzania systemem walki.

W zależności od poziomu działań wojennych, wsparcie wywiadowcze powinno być ukierunkowane na poziom strategiczny, operacyjny lub taktyczny. Aby zapewnić dowódcom pełne zrozumienie sytuacji, oprócz rozpoznania i obserwacji nowych celów lub pojawiających się wysoce prawdopodobnych zagrożeń, analitycy wywiadu muszą również brać pod uwagę i łączyć inne istotne aspekty sytuacji operacyjnej, takie jak czynniki socjokulturowe.

Obserwacja jest definiowana jako "*(...) systematyczne śledzenie przestrzeni powietrznej, powierzchni lub obszaru pod powierzchnią, miejsc, osób lub rzeczy za pomocą środków wizualnych, podsłuchowych, elektronicznych, fotograficznych lub innych*" [85]. Obserwacja ma charakter stabilnego nadzoru, stałego i systematycznego śledzenia, niezależnie od tego, czy dotyczy celu odległego i jest prowadzona z wykorzystaniem wywiadu optoelektronicznego, czy też celu bliskiego, gdzie wykorzystywany jest wywiad sygnałowy. Obserwacja może być również prowadzona przez człowieka, który w określonym czasie i we właściwie dobrany sposób śledzi cel.

Rozpoznanie definiuje się jako *"(...) misję podjętą w celu uzyskania informacji o działaniach lub zasobach przeciwnika (...) lub zabezpieczenia danych dotyczących meteorologicznych, hydrograficznych lub geograficznych cech danego obszaru*" [85].
Rozpoznanie należy rozumieć, jako konkretną misję skoncentrowaną na zwiadzie terenowym (z wykorzystaniem np. *GEOINT, IMINT*) lub/i rozpoznaniu siłowym (z wykorzystaniem wszystkich rodzajów wywiadu, które pozwalają na zidentyfikowanie sprzętu, technologii, infrastruktury i innych zasobów wykorzystywanych przez przeciwnika). Rola systemu rozpoznania rośnie, ponieważ poziom technologiczny narzędzi wykorzystywanych do analizy zasobów militarnych i taktyki przeciwnika jest coraz bardziej wymagający.

W obszarze rozpoznania wojskowego wyniki analizy obrazu zapewniają wsparcie procesów decyzyjnych. Identyfikują obszary zainteresowania, dostarczając informacje decydentowi i wskazując, na czym należy skupić uwagę. Wojna w Iraku w 1991 roku unaoczniła znaczenie posiadania właściwej technologii dla procesów rozpoznawczych, kiedy to siły sojusznicze dysponowały zintegrowaną informacją pochodzącą z rozpoznania obrazowego, elektronicznego i osobowego, praktycznie w czasie rzeczywistym, podczas gdy zasoby irackie umożliwiały nanoszenie na mapy informacji przesyłanych analogowo o położeniu wojsk [92]. Z kolei patrząc na to zagadnienie trzydzieści lat później należy mieć

świadomość istniejącego ryzyka, gdyż dostęp i pozyskanie wysokiej jakości zdjęć i filmów jest współcześnie możliwe z poziomu tanich urządzeń kompaktowych, takich jak telefony komórkowe. Zwiększyła się również liczba ogólnodostępnych i darmowych narzędzi, które pozwalają na modyfikację obrazu. To oznacza, że w kolejnych latach poziom możliwości obróbki zdjęć może być na tyle istotny, że będzie pozwalał na zamianę obrazu i przesyłanie fałszywych danych.

Odrębną kwestią występującą w obszarze klasyfikacji jest jakość samego obrazu, od której wiele zależy (wiarygodność klasyfikacji obiektów wojskowych może mieć krytyczne znaczenie, szczególnie na obszarach toczących się konfliktów). Nawet jeśli parametry taktyczne i techniczne sensorów stosowanych na polu walki są względnie stabilne, jakość obrazu może być obniżona przykładowo przez flary boczne, nieprzejrzystość atmosfery, szumy własne fotodetektorów itp. i wprowadzać do procesu klasyfikacji tzw. niepewność aleatoryczną[20]. W opracowaniu [4] badacze wskazują również na występowanie w procesie klasyfikacji obrazów niepewności epistemicznej, która występuje nawet wśród wykwalifikowanych interpretatorów. Błędy poznawcze (ang. *cognitive bias*) popełniane są przez człowieka nieświadomie i przejawiają się w zniekształconym postrzeganiu niektórych elementów obrazu, nieuzasadnionych przesunięciach regresyjnych w oszacowaniach, nieuzasadnionym wyrównywaniu prawdopodobieństw itp.

Pomimo rosnącego zapotrzebowania na automatyzację procesów rozpoznawczych sztuczna inteligencja (ang. *artificial intelligence - AI[21])* nie stanowi jeszcze podstawowego elementu prowadzenia analizy obrazowej, gdyż obiekty zidentyfikowane w ramach działań algorytmów nadal muszą być objęte oceną człowieka. Zmniejszenie stronniczości w mechanizmach sztucznej inteligencji jest trudne i opiera się na wielokrotnej weryfikacji modeli, ich ciągłej aktualizacji i zwiększaniu dokładności. Należy mieć również na uwadze fakt, że pole walki i przegrupowania sił mogą zmieniać się na tyle dynamicznie, że ograniczenia *AI,* jak brak bieżącego kontekstu i wiedzy o najnowszych wydarzeniach, nie pozwolą na właściwą analizę i interpretację wyników.

Współcześnie największym wyzwaniem dla analizy obrazu nie jest zdefiniowanie obserwowanego obiektu, ale właściwe sklasyfikowanie zdarzenia, które pozwoli na

[20] Istotnym problemem w analizach ryzyka jest rozróżnienie pomiędzy niepewnością aleatoryczną (probabilistyczną) oraz epistemiczną (wynikającą z braku precyzji lub braku informacji)

[21] Zgodnie z Rekomendacją Rady OECD ds. Sztucznej Inteligencji z 2019 roku „System AI to system oparty na maszynie (ang. *machine based system*), który może, dla określonego zestawu celów zdefiniowanych przez człowieka, przewidywać, rekomendować lub podejmować decyzje wpływające na środowisko rzeczywiste lub wirtualne. Systemy AI są zaprojektowane do działania na różnych poziomach autonomii". Za: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

kompleksową ocenę sytuacji. Z jednej strony, bardziej zaawansowana analiza powinna ujawnić przykładowo czy grupa ludzi wokół obiektu to osoby cywilne czy wojskowi i czy obiekt zmienił położenie czy też należy do krajobrazu na stałe. W tym celu wykorzystywana jest inteligencja rozszerzona (ang. *augmented intelligence*) stanowiąca połączenie *AI* i analizy prowadzonej przez człowieka. Pozwala to skupić się na istotnych zdarzeniach i pogłębić analizę o nowe, nieopisane jeszcze w systemach dane (jak warunki atmosferyczne lub stan obiektów). Szereg publikacji włącza do analizy obrazu tak zwaną informację kontekstową (przykładowo [93] i [94]).

Informacje zebrane z rozpoznania obrazowego są przekazywane na odpowiedni szczebel dowodzenia. Muszą być pewne i wiarygodne. Nie jest to jeszcze możliwe przy wykorzystaniu sztucznej inteligencji jako jedynego narzędzia. Z tego powodu - niezależnie od postępu technologicznego – czynnik ludzki będzie w dalszym ciągu integralnym elementem prowadzenia obrazowego rozpoznania wojskowego. Na obecną chwilę jest mało prawdopodobne, by uczenie maszynowe, w pełni zastąpiło ludzi w podejmowaniu decyzji. Sztuczna inteligencja pomaga w automatyzacji procesów rozpoznawczych i choć nadal jest mało użyteczna w praktyce, to na pewno jej udział się zwiększy [92].

Analizując obszar analizy obrazu warto odnieść się do koncepcji *Coalition Shared Data* (CSD), czyli koncepcji i wdrożenia elastycznej architektury NATO umożliwiającej wymianę danych w określonym standardzie, w celu wsparcia wszystkich poziomów dowodzenia. Tylko w zakresie rozpoznania obrazowego, gdzie występuje duża różnorodność źródeł informacji, konieczne było opracowanie szeregu standardów, takich jak STANAG 7023 (dotyczący formatu danych obrazów pierwotnych), STANAG 4545 (dotyczący formatu danych obrazów wtórnych), STANAG 4607 (dotyczący formatu danych GMTI (ang. *Ground Moving Target Indicator*)) czy STANAG 4609 (dotyczący formatu danych wizyjnych uzyskiwanych z sensorów elektro-optycznych i podczerwieni (ang. *Electro-Optical / Infrared*). Świadomość problemów związanych z zapewnieniem interoperacyjności w rozpoznawaniu obrazowym doprowadziła do opracowania standardu STANAG 4559 (*NATO Standard ISR Library Interface - NSIL*), w którym zdefiniowano interfejs umożliwiający dostęp w koalicji środowiskowej do wszystkich bibliotek danych *ISR* oraz narodowych baz danych, w których przechowywane są produkty powstałe w wyniku rozpoznawania obrazów [95].

Komercyjną implementacją standardu STANAG 4559, jest projekt dotyczący systemu przechowywania i rozpowszechniania zasobów wywiadu, obserwacji i rozpoznania o nazwie *Coalition Shared Data server*. W ramach tego projektu rozwijana jest seria systemów do kompilacji informacji z wielu różnych źródeł w różnych formatach (klipy wideo, zdjęcia,

radary itp.), dostarczających analitykom wywiadu niezbędnych narzędzi do wymiany informacji ISR [95].

Integracja z serwerem CSD stanowi wyzwanie dla polskich rozwiązań. Klauzula tajności NATO oznacza, że polskie systemy muszą być budowane z uwzględnieniem tego poziomu bezpieczeństwa informacji.

2.3. System rozpoznania w SZ RP

W Polsce jednostką wojskową odpowiedzialną za zarządzanie całym podsystemem rozpoznania obrazowego, zapewniającym zdolność do przetwarzania i analizy danych obrazowych oraz prowadzenia kompleksowych ocen środowiska bezpieczeństwa, przy wykorzystaniu danych obrazowych pozyskiwanych z różnych systemów rozpoznawczych jest Ośrodek Rozpoznania Obrazowego (ORO) w Białobrzegach.

W Polsce, jednostki rozpoznawcze ulokowane zostały w większości we wschodniej części kraju.

Rysunek 55 Jednostki rozpoznawcze – stan na początek 2023 roku. Opracowanie własne. Grafika ORP Nawigator: https://pl.wikipedia.org/wiki/ORP_Nawigator. Grafika ORP Hydrograf: https://pl.wikipedia.org/wiki/ORP_Hydrograf.

Ponadto w ramach podsystem rozpoznania obrazowego (IMINT) polskich sił powietrznych wykorzystywane są samoloty F-16 z zasobnikiem AN/ASD-14 systemu DB-110 operujące z 10. ELT w składzie 32 Bazy Lotnictwa Taktycznego w Łasku. Zasobniki rozpoznawcze DB-

110 współpracują z dwoma naziemnymi zestawami odbioru i analizy zdobytych danych w czasie rzeczywistym, jednym stacjonarnym w Łasku oraz jednym mobilnym. W coraz mniejszym stopniu (z uwagi na przestarzałą konstrukcję oraz zużycie sprzętu) wykorzystywane są samoloty rozpoznawcze starszej generacji SU-22 z zasobnikiem KKR-1. W ostatnich latach coraz większego znaczenia w systemie rozpoznania nabiera wykorzystywanie bezzałogowych systemów powietrznych (UAS), operujących głównie z 12. Bazy Bezzałogowych Statków Powietrznych w Mirosławcu.

Podczas operacji stabilizacyjnej w Iraku Polski kontyngent był wspierany *„(...) przez kontyngenty wojskowe z innych państw koalicji. W zakresie prowadzonej operacji ujawniły się braki polskiej armii, szczególnie w zakresie rozpoznania osobowego, a także niedocenianego rozpoznania patrolowego. Potencjał rozpoznawczy dywizji ulegał ciągłemu zmniejszeniu podczas kolejnych zmian polskiego kontyngentu wojskowego. (...) Można stwierdzić, że posiadany potencjał rozpoznawczy był zdecydowanie za mały w stosunku do ilości zadań stawianych przed systemem rozpoznania*" [96].

Inaczej wyglądała sytuacja w trakcie misji w Afganistanie. Polski kontyngent brał udział w działaniach stabilizacyjnych, wśród których najważniejsze było rozpoznanie i patrolowanie. Większe wykorzystanie bezzałogowych statków powietrznych na poziomie dowodzenia taktycznego i operacyjnego wymagało nowych możliwości pozwalających na sprawne i dokładne pozyskiwanie oraz przetwarzanie danych obrazowych. Dzięki temu wzrosło zrozumienie konieczności wykorzystania w misjach wojskowych obszaru ISR.

Obecnie w procesie planowania i prowadzenia operacji istotną kwestią jest spełnienie wymagań stawianych Dowództwu Operacyjnemu Rodzajów Sił Zbrojnych oraz Dowództwom innych komponentów - jednostek zależnych. Informacje pozyskiwane między innymi z ISR lub instytucji współdziałających są niezbędne do planowania na poziomie operacyjno-strategicznym oraz podczas realizacji operacji. Biorąc to pod uwagę, najważniejsze dla procesu decyzyjnego jest dostęp we właściwym czasie do właściwych informacji.

Nadmiar danych i faktów generowanych z wielu źródeł, w tym przez instytucje i agendy współdziałające z wojskiem, może utrudniać ich terminowe przetwarzanie. Z tego powodu kluczowe znaczenie ma możliwość znalezienia i dostarczenia ważnych informacji w pożądanym czasie [97]. W tym celu budowany jest zintegrowany system gromadzenia, przetwarzania i wymiany danych/informacji. Jego opracowanie jest jednak bardzo trudne ze względu na specyfikę systemów rozpoznania (rozpoznanie na poziomie patroli, pododdziałów, artylerii, sił powietrznych, rozpoznanie bliskie i dalekie itp.) oraz rozproszoną architekturę systemów.

Znaczenie i konieczność wdrożeń ISR w Siłach Zbrojnych RP znalazło swoje odzwierciedlenie w Planie Modernizacji Technicznej, w którym przewidziano następujące systemy i przedsięwzięcia:

a. System informatyczny do gromadzenia, analizy i dystrybucji informacji ze wszystkich elementów ISTAR (rozpoznania patrolowego, dalekiego zasięgu, elektronicznego, obrazowego i osobowego) – kryptonim SOWA. Jego zadaniem będzie przyjmowanie i dystrybucja wszystkich wiadomości rozpoznawczych mogących mieć istotne znaczenie dla prowadzonych działań oraz wsparcie informacyjne dowództw w zakresie zapewnienia zdolności bojowej i bezpieczeństwa wojsk z wykorzystaniem zautomatyzowanych systemów dowodzenia,
b. Zautomatyzowany system zbierania, przetwarzania i dystrybucji wiadomości rozpoznawczych otrzymywanych z elementów rozpoznania dalekiego zasięgu – kryptonim PAJĄK,
c. Lekkie opancerzone pojazdy rozpoznawcze – kryptonim KLESZCZ,
d. Pojazdy rozpoznawcze dla jednostek rozpoznania dalekiego zasięgu – kryptonim ŻMIJA,
e. Mobilne bezzałogowe pojazdy rozpoznawcze (MBPR) – kryptonim TARANTULA,
f. Zestawy bezzałogowych systemów powietrznych klasy mini (BSP klasy MINI NeoX 2) – kryptonim WIZJER,
g. Systemy Bezzałogowych Statków Powietrznych klasy taktycznej krótkiego zasięgu – kryptonim ORLIK.

Obecnie polskie Siły Zbrojne muszą się mierzyć z problemami, które już wcześniej zostały zidentyfikowane w procesie analiz danych rozpoznawczych przez inne armie, zwłaszcza w USA. W 2017 roku gen. *Jack Shanahan,* dyrektor ds. wywiadu obronnego w Biurze Podsekretarza Obrony ds. Wywiadu USA podał, że Pentagon zbiera codziennie 22 terabajty danych [98]. *Strategia Danych Departamentu Obrony Stanów Zjednoczonych* (ang. *DoD Data Strategy*) stanowiąca kluczowy element programu Cyfrowej Modernizacji Departamentu (będący uszczegółowieniem Narodowej Strategii Obrony USA) w znamienny sposób pozycjonuje algorytmy sztucznej inteligencji i dane przygotowane do ich wykorzystania, przyznając im wysoką wartość szkoleniową, a z czasem status „najcenniejszych aktywów cyfrowych" [99]. Strategia wprowadza pojęcie „ery wojny algorytmicznej" [99], w której należy doskonale zabezpieczyć zbiory danych wykorzystywanych do tworzenia algorytmów pozwalających na efektywne zarządzanie zasobami cyfrowymi. Ma to krytyczne znaczenie,

w miarę włączania sztucznej inteligencji do funkcjonowania armii w trakcie konfliktu zbrojnego.

Główne problemy, z jakimi boryka się obecnie wojsko, dotyczą dostępności coraz większej ilości danych z czujników pochodzących z integralnych źródeł, takich jak bezzałogowe statki powietrzne (UAV) i inne zasoby narodowe. Zwykła całodzienna misja UAV może dostarczyć do 10 terabajtów danych, z których tylko około 5% jest analizowane, a reszta przechowywana. Analitycy są ograniczeni prędkością pobierania danych w zależności od ich lokalizacji. Nieoznakowane dane prowadzą do pobierania podobnych danych z innych źródeł, aby potwierdzić swoje wnioski. W wielu przypadkach łącza komunikacyjne są współdzielone lub mogą nie być stale dostępne, co zwiększa opóźnienia w analizie. Zapewnienie kompleksowej świadomości sytuacyjnej jest uzależnione od dokładności i integracji danych otrzymywanych z wielu rodzajów czujników oraz źródeł wywiadowczych. Ze względów bezpieczeństwa dane ISR pochodzące z różnych źródeł są przechowywane w różnych miejscach, z różnymi poziomami dostępu, co prowadzi do niekompletnych analiz. Pojedyncza domena sieciowa zapewniająca dostęp do danych na wielu poziomach klasyfikacji bezpieczeństwa nie jest jeszcze dostępna [15].

Wyżej wymienione uwarunkowania powodują, że z jednej strony coraz trudniej odpowiedzieć na współczesne wyzwania związane z analizą obrazu, jej bezpieczeństwem wykonania i jednoczesnym tempem obliczeń, poprawnością identyfikacji obiektów, a tym samym terminowym dostarczeniem najbardziej potrzebnej i najlepszej jakości informacji na odpowiedni poziom dowódczy. Z drugiej jednak tworzą przestrzeń dla coraz większej liczby algorytmów, które wymagają ciągłego doskonalenia i dostosowania do zmieniającej się rzeczywistości.

2.4. Wdrożenie

Opracowanie algorytmu w ramach niniejszej pracy jest wzbogaceniem oferty Grupy Kapitałowej PGZ, a w szczególności oferty jej spółki Ośrodka Badawczo – Rozwojowego Centrum Techniki Morskiej (OBR CTM) biorącego udział od 2015 roku w postępowaniu na dostawę Systemu Analiz Obrazowych (SAO) o metodę klasyfikacji obrazów, która jako dodatkowy komponent zostałaby przekazana do Sił Zbrojnych RP.

W związku z unieważnieniem przedmiotowego postępowania w 2022 roku, postanowiono, by wiedzę i doświadczenie zdobyte w trakcie przygotowania do jego realizacji wykorzystać w kolejnym przedsięwzięciu pt. „Bałtyk Cyfrowy”. Rozpoczęto prace w zakresie budowy demonstratora sieciocentrycznego modułowego systemu wsparcia procesów informacyjno-decyzyjnych w operacjach i działaniach taktycznych, prowadzonych przez dowództwa, sztaby,

a także oddziały i pododdziały wchodzące w skład lub realizujące zadania na rzecz komponentu morskiego SZ RP, jako elementu wsparcia wielodomenowego pola walki.

Obecnie do wspierania procesu dowodzenia i użycia sił komponentu morskiego wykorzystywane są dedykowane systemy tj. ZSyD MW RP ŁEBA, MCCIS, LINK – 11/16 oraz funkcjonujące bazy danych takie jak baza danych obiektów podwodnych (MWDC), czy bazy danych rozpoznania, które posiadają specyficzne ograniczenia. Taka konfiguracja wpływa na możliwość efektywnego budowania i utrzymania aktualnego jednolitego obrazu sytuacyjnego. Proponowany w ramach projektu rozwój technologii wymaga wdrożenia technik konsolidacji, uogólniania i udostępniania danych pochodzących z różnych źródeł. Klasyfikacja obiektów stanowi ważny komponent zakresu przedmiotowego projektu.

Rozwój powyższych technologii przyczynia się do zwiększenia funkcjonalności systemu. W tym zakresie trwają prace wdrożeniowe mające na celu wykorzystanie rozwiązania autorki pracy do poszerzenia bazy algorytmów realizujących jeden z celów naukowych projektu: „*wsparcia procesów rozpoznawania obiektów lub zjawisk mające na celu określenie ich położenia, parametrów kinematycznych, określanie właściwych cech i charakterystyk pozwalających na identyfikację obiektów lub zjawisk*”, jak również wdrożenia wiedzy zgromadzonej podczas doktoratu do „*budowy bazy danych pozyskiwanych z rozpoznania obrazowego, w tym danych pochodzących z mobilnych i stacjonarnych układów sensorycznych oraz rozpoznania radioelektronicznego, a w perspektywie długofalowej przygotowanie do wykorzystania danych pochodzących z satelitarnych systemów rozpoznawczych*”. Badania i opracowanie metod przedstawionych w niniejszej pracy doktorskiej stanowią właściwą podbudowę teoretyczną i algorytmiczną do rozwoju technologii rozpoznania, co wraz z pozostałymi komponentami projektowanego systemu może przyczynić się do poprawy zdolności do dowodzenia, rozpoznania, a także zdolności w obszarze przetrwania i zapewnienia bezpieczeństwa państwa.

Należy mieć na względzie, że sytuacja geopolityczna oraz zwiększone zaangażowanie zespołów inżynierskich Polskiej Grupy Zbrojeniowej (PGZ) w odpowiadanie na szybkie zapotrzebowanie Sił Zbrojnych RP powodują, że całkowite wdrożenie rozwiązania autorki w zakresie nowego projektu, jakim jest „Bałtyk Cyfrowy”, zostało przesunięte w czasie. Natomiast zgodnie ze stanowiskiem spółki, zespół ds. analizy obrazowej (opracowujący bazę obiektów wojskowych), prowadzi prace konsultacyjne i wdrożeniowe, w odniesieniu do wypracowanego w niniejszym doktoracie rozwiązania. Prace te wpisują się w „Priorytetowe kierunki badań w resorcie obrony narodowej na lata 2017-2026” (Załącznik do decyzji nr 235/DNiSzW Ministra Obrony Narodowej z dnia 26 czerwca 2019 r.).

WNIOSKI

Największym osiągnięciem przedmiotowej pracy jest opracowanie nowej metody klasyfikacji obiektów na obrazie, w wyniku dokonania optymalizacji algorytmu w sposób umożliwiający usunięcie ważenia kryteriów i zastąpienie ich metodą stosującą punkty odniesienia uwzględniające poziomy aspiracji, które są definiowane w oparciu o funkcję maksiminową.

W wielokryterialnej metodzie klasyfikacji dokonano połączenia czterech kryteriów, agregując je w dwóch grupach. W pierwszej grupie znalazły się kryteria gęstości i podobieństwa. Ich połączenie pomaga wieloaspektowo, pozwala na uwzględnienie w klasyfikacji zarówno rozkładu danych, jak i podobieństwa między nimi, co prowadzi do bardziej kompleksowej oceny i lepszych rezultatów w wielu analizach danych. Umożliwia między innymi dokonywanie pełniejszej oceny danych, wykrycie anomalii, dokonanie klasyfikacji i zgrupowanie danych, redukcję wymiarowości. W drugiej grupie zestawiono kryterium niepewności i oparte na etykietach. Ich połączenie może przynieść korzyści w zakresie efektywnego wykorzystania danych oznaczonych, redukcji błędów klasyfikacji, zarządzania niepewnością i selekcji przykładów do dalszej analizy. W przedmiotowej metodzie metryka oceny, którą jest dokładność, została powiązana z każdym z kryteriów, których wartość jest ustalana iteracyjnie, w celu zwiększenia poziomu dokładności.

W celu zdefiniowania algorytmu optymalizacji zdefiniowano:

1. Reprezentację rozwiązania - w celu osiągnięcia efektu porównania nowej metody z metodą MCADL wykorzystano bazy MNIST i CIFAR-10, w których struktura danych jest trójwymiarowa i są one przekształcone na tensory w celu przeprowadzenia multiprocessingu z silnikiem GPU.
2. Metodę modyfikacji rozwiązania lub generowania kolejnych – zaimplementowano metodę wykorzystującą punkty odniesienia, zdefiniowane przez zastosowanie funkcji maksiminowej, jako poziomy aspiracji. Punkty odniesienia zostały zdefiniowane dla każdego kryterium, a następnie iteracyjnie ich wartość była zmieniana w zależności od wzrostu *accuracy*.
3. Funkcję oceny rozwiązania - do oceny skuteczności przedmiotowych rozwiązań wykorzystano metrykę dokładności, która jest kluczowa dla obu metod wielokryterialnych. W metodzie MCADL, dokładność jest powiązana z wagą alfa i beta, które są zmniejszane wraz z jej wzrostem. W kilkudziesięciu eksperymentach zbadano wyniki działania algorytmu z wykorzystaniem inicjalizacji losowej oraz inicjalizacji

PCA-k-means. Eksperymenty wykazały, że w miarę wzrostu poziomu dokładności, wartość kryteriów malała.

W pierwszej fazie eksperymentów, dokonanej na architekturach sieci neuronowych opracowanych dla metody MCADL, wykazano niską skuteczność metody. Na kilkadziesiąt eksperymentów wykonanych na bazie MNIST, metoda MCADL w około 80% nie dawała najlepszego wyniku lub jej wynik był lepszy minimalnie. Mając to na względzie, w drugiej fazie eksperymentów podjęto próbę dokonania szeregu zmian:

a) Zaprojektowano nowe architektury sieci neuronowych.
b) Wprowadzono nowy sposób inicjalizacji algorytmu.
c) Co najważniejsze, zastąpiono mechanizm ważenia kryteriów mechanizmem ich iteracyjnego dostosowywania do poziomów odniesienia (aspiracji). W tym zakresie na początku wykonano próby odnosząc wszystkie cztery kryteria do poziomu 0, a następnie do poziomu 1. Z uwagi na wyniki analizy zachowywania się poszczególnych kryteriów w kolejnym kroku założono, że dwa pierwsze punkty odniesienia powinny być ustawione blisko poziomu zerowego: gęstość (0,1) i podobieństwo (0,15), a dwa kolejne blisko poziomu 1: niepewność (0,9), kryterium oparte na etykietach (0,8). Dodatkowo należy podkreślić, że największy nacisk został położony na eksperymenty w zakresie bazy CIFAR-10 z uwagi na chęć lepszego odzwierciedlenia zróżnicowania obiektów na obrazach, analogiczne do tego, które ma miejsce w środowisku wojskowym.
d) W ramach eksperymentów i w związku z potrzebą polepszenia wyników dla danych pochodzących ze zbioru CIFAR-10 zbudowano algorytm uwzględniający metodę wynikającą z połączenia *margin sampling* i nowej metody uwzględniającej punkty odniesienia. *Margin sampling* przynosi korzyści poprzez poprawę jakości modelu, redukcję *overfittingu*, skupienie się na obszarach trudnych, ograniczenie zakłóceń w danych oraz zwiększenie interpretowalności modelu.

   W celach porównawczych algorytm zaimplementowano w wersji uwzględniającej ważenie kryteriów oraz w wersji z punktami odniesienia. Połączenie tych dwóch metod dało najlepsze wyniki w skali przeprowadzonych eksperymentów, w tym najwyższe wskaźniki walidacyjne.

Ostatecznie metoda w pierwszej kolejności wybiera pulę inicjalizującą z wykorzystaniem klastrowania danych za pomocą *k-średnich* i analizy składowych głównych. To pozwala na zmniejszenie przypadkowości w doborze próbek do treningu oraz zmniejszenie

wymiarowości danych. Zastosowanie tej metody nie wpłynęło znacząco na wynik algorytmu, ale w większości eksperymentów przyniosło lepsze wyniki niż inicjalizacja losowa.

Metody wykorzystujące punkty odniesienia, w większości zrealizowanych eksperymentów, dały najlepsze wyniki. Zarówno w wymiarze nowej metody wielokryterialnej z punktami odniesienia, jak i *margin sampling* z punktami odniesienia, dokładność osiągnęła w większości eksperymentów najwyższe poziomy. W zakresie zmiany sposobu inicjalizacji z losowej na *PCA - k-means* warto zauważyć, że złożoność obliczeniowa jest większa niż w wyniku zastosowania inicjalizacji losowej, natomiast treningi z wykorzystaniem *PCA - k-means* mają bardziej stabilny charakter niż te realizowane z inicjalizacją losową.

Reasumując, praca nie ogranicza się do wymiaru naukowego, ale jej efekty są dedykowane i będą przydatne w militarnym obszarze zastosowań. Zaproponowana metoda klasyfikacji obrazu, która w następstwie dokonanej optymalizacji spełnia wymóg niezawodności oraz sprawności realizowanych obliczeń przy jednoczesnym utrzymaniu lepszego poziomu dokładności, jest realizacją założonego celu pracy.

BIBLIOGRAFIA

[1] A. Wierzbicki, Teoria i Praktyka Wspomagania Decyzji, p. 27.

[2] J. Yuan, X. Hou, Y. Xiao, D. Cao, W. Guan i L. Nie, „Multi-criteria active deep learning for image classification," *Knowledge-Based Systems 172*, p. s. 86–94, 2019.

[3] [Online]. Available: https://www.projectpro.io/article/pytorch-vs-tensorflow-2021-a-head-to-head-comparison/416. [Data uzyskania dostępu: 16 10 2022].

[4] M. Popov, M. Topolnytskyi i V. Pylypchuk, „A Method for Object Classification in Aerial/Satellite Images with Incorporating Geospatial Information," w *Advances in Military Technology*, 2021.

[5] [Online]. Available: https://www.projectpro.io/article/pytorch-vs-tensorflow-2021-a-head-to-head-comparison/416. [Data uzyskania dostępu: 16 10 2022].

[6] D. Ellsworth i M. Cox, „Application-controlled demand paging for out-of-core visualization,," *Proceedings. Visualization '97 (Cat. No. 97CB36155)*, pp. s. 235-244, 1997. DOI: 10.1109/VISUAL.1997.663888..

[7] D. Ellsworth i M. Cox, Managing big data for scientific visualization, 1997.

[8] V. Mayer-Schonberger i K. Cukier, Big data, efektywna analiza danych, Warszawa, 2017, p. 15.

[9] [Online]. Available: https://bernardmarr.com/what-is-big-data/ . [Data uzyskania dostępu: 11 12 2022].

[10] [Online]. Available: https://www.gartner.com/en . [Data uzyskania dostępu: 21 10 2022].

[11] M. Tabakow, J. Korczak i B. Franczyk, „Big data – definicje, wyzwania i technologie informatyczne," *Informatyka Ekonomiczna Business Informatics*, nr 1(31), 2014. DOI: 10.15611/ie.2014.1.12.

[12] M. Khalid i M. Yousaf, „A Comparative Analysis of Big Data Frameworks: An Adoption Perspective.," *Appl. Sci.*, nr 11033, 11 2021. DOI: https:// doi.org/10.3390/app112211033.

[13] [Online]. Available: https://datareportal.com/global-digital-overview. [Data uzyskania dostępu: 30 11 2021].

[14] [Online]. Available: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world. [Data uzyskania dostępu: 30 11 2021].

[15] S. Kulshrestha, „Data really powers everything that we do," *Big Data in Military Information & Intelligence*, 22 January 2016.

[16] [Online]. Available: https://www.domo.com/data-never-sleeps.

[17] K. Matela, Ewolucja wybranych algorytmów sztucznej inteligencji stosowanych w dziedzinie widzenia komputerowego, w oparciu o przykłady sieci neuronowych, Lublin: Wydawnictwo Naukowe TYGIEL, 2022.

[18] N. White, „Big Data and Business Analytics comes of age, 28th October 2011,," 28 09 2011. [Online]. Available: http://researchcomputing.blogspot.com/2011/10/big-data-and-business-analytics-comes.html?view=magazine .

[19] K. Steen-TveitBjørn i E. E. Munkvold, „From common operational picture to common situational understanding: An analysis based on practitioner perspectives," DOI: https://doi.org/10.1016/j.ssci.2021.105381.

[20] A. Gupta, A. Efros i H. M., „Blocks World Revisited: Image Understanding Using Qualitative Geometry and Mechanics.," w *Lecture Notes in Computer Science, vol 6314.*, DOI: https://doi.org/10.1007/978-3-642-15561-1_35.

[21] „Historia fotografii. Jak zatrzymać czas," [Online]. Available: https://histmag.org/Historia-fotografii-jak-nauczylismy-sie-zatrzymywac-czas-16597 . [Data uzyskania dostępu: 01 12 2021].

[22] C. Cortes i V. Vapnik, „Support-Vector Networks," *Machine Learning 20,* p. 273–297, 1995, DOI: https://doi.org/10.1023/A:1022627411411.

[23] F. Yoav i S. R.E., „Experiments with a New Boosting Algorithm," w *Proceedings of the Thirteenth International Conference*, 1996.

[24] R. Duda, P. Hart i D. Stork, Pattern classification, Second Edition red., Nowy Jork: A Wiley-Interscience Publication, 2001, p. 16.

[25] J. Deng, W. Dong, R. Socher, L. Li, L. Kai i L. Fei-Fei, „ImageNet: A large-scale hierarchical image database," w *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009. DOI: 10.1109/CVPR.2009.5206848.

[26] [Online]. Available: https://image-net.org/about.php. [Data uzyskania dostępu: 30 07 2021].

[27] [Online]. Available: https://image-net.org/challenges/LSVRC/2012/. [Data uzyskania dostępu: 30 07 2021].

[28] „The data that transformed AI research—and possibly the world, QUARTZ," 30 07 2021. [Online]. Available: https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world/.

[29] K. Simonyan i A. Zisserman, Very Deep Convolutional Networks for Large-Scale Image Recognition, CoRR, abs/1409.1556, 2015.

[30] A. Krizhevsky, I. Sutskever i G. Hinton, „ImageNet Classification with Deep Convolutional Neural Networks," w *Communications of the ACM 60 (6)*, 2017. DOI: 10.1145/3065386.

[31] I. Goodfellow, Y. Bengio i A. Courville, „Deep Learning," *Adaptive computation and machine learning series*, p. 24, 2017.

[32] A. Geron, Hands-On Machine Learning with Scikit-Learn, Keras and Tensorflow: Concepts, Tools and Techniques to Build Intelligent Systems, 2nd Edition red., Helion S.A., 2020.

[33] I. E. Commission, „White Paper, Artificial intelligence across industries," 2018.

[34] L. Meemong, C. Anderson i R. Weidner, State of the Art in Image Processing. Jet Propulsion Laboratory, California Institute of Technology Pasadena Ca. 91109, Berlin Heidelberg: Springer-Verlag, 1993.

[35] A. Sonka, V. Hlavac i R. Boyle, Image processing, Analysis and Machine Vision, Cengage Learning, 2013, p. 6.

[36] S. Vahini Ezhilraman i S. Sujatha, „State of the art in image processing & big data analytics: issues and challenges," *International Journal of Engineering & Technology*, nr 7 (2.33) (2018), pp. 195-199, 2018.

[37] [Online]. Available: https://manisha-sirsat.blogspot.com/2019/04/confusion-matrix.html . [Data uzyskania dostępu: 03 11 2022].

[38] D. W. Aha, A study of instance-based algorithms for supervised learning tasks: mathematical, empirical, and psychological evaluations. PhD thesis, Irvine: University of California, 1990.

[39] T. Orczyk, Klasyfikacja danych niekompletnych w oparciu o komitet klasyfikatorów. Rozprawa doktorska, Sosnowiec, 2018.

[40] „An essay towards solving a problem in the doctrine of chances," *Reson 8,* p. 80–88, 2003. DOI: https://doi.org/10.1007/BF02883540.

[41] B. Ying, X. Bing, Mengjie i Zhang, „Using a small number of training instances in genetic programming for face image classification," *Information Sciences,* nr 593, p. 488–504, 2022.

[42] W. Min, M. Fan, Z. Zhi-Heng i W. Yan-Xue, „Active learning through density clustering".

[43] K. Nigam, A. Mccallum, S. Thrun i T. Mitchell, „Text Classification from Labeled and Unlabeled Documents using EM," *Machine learning,* Tomy %1 z %22000-05, Vol.39 (2), p. 104, 2000.

[44] [Online]. Available: https://www.youtube.com/watch?v=Bi7f1JSSlh8. [Data uzyskania dostępu: 15 07 2021].

[45] B. Settles, Active learning literature survey. Technical report, University of Wisconsin-Madison Department of Computer Sciences, 2009.

[46] Y. Ouali, C. Hudelot i M. Tami, An Overview of Deep Semi-Supervised Learning, Université Paris-Saclay, CentraleSupélec, MICS, 91190, Gif-sur-Yvette, France, 2020. DOI: arXiv:2006.05278v2 [cs.LG].

[47] A. Mottaghi i S. Yeung, Adversarial Representation Active Learning, Stanford University, 2009. DOI: rXiv:1912.09720v1 [cs.CV].

[48] W. Cai, Y. Zhang i J. Zhou, „Maximizing Expected Model Change for Active Learning in Regression," w *2013 IEEE 13th International Conference on Data Mining,* 2013. DOI: 10.1109/ICDM.2013.104.

[49] S. Dasgupta, „Analysis of a greedy active learning strategy," *Advances in neural information processing systems,* p. 337–344, 2005.

[50] M. Minakawa, B. Raytchev, T. Tamaki i K. Kaneda, „Sequence Recognition with Active Learning Using Uncertainty Sampling," w *Proc. IEEE International Joint Conference on Neural Networks (IJCNN2013),* 2013.

[51] S. Huang, R. Jin i R. Zhou, „Active Learning by Querying Informative and Representative Examples," w *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2014. DOI: 10.1109/TPAMI.2014.2307881.

[52] D. Lewis i W. Gale:, „A sequential algorithm for training text classifiers," w *SIGIR '94,* 1994.

[53] C. Zhang i T. Chen, „An active learning framework for content-based information retrieval," w *IEEE Transactions on Multimedia,* 2002. DOI: 10.1109/TMM.2002.1017738.

[54] C. Shannon, „A mathematical theory of communication," *The Bell System Technical Journal,* Tomy %1 z %2vol. 27, no. 3, pp. 379-423, 1948. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[55] T. Scheffer, C. Decomain i S. Wrobel, „Active hidden Markov models for information extraction," w *Proceedings of the International Conference on Advances in Intelligent Data Analysis (CAIDA),* 2001.

[56] J. Yuan, X. Hou, Y. Xiao, D. Cao i W. N. L. Guan, „Multi-criteria active deep learning for image classification," *Knowledge-Based Systems,* nr 172, p. 86–94, 2019.

[57] P. Donmez, J. Carbonell i P. Bennett, „Dual Strategy Active Learning," w *Proc. 18th European Conf. Machine Learning,* 2007.

[58] H. Seung i M. S. H. Opper, „Query by committee," w *Proc. 5th Annu. ACM Workshop Computational Learning Theory,* Pittsburgh, PA, 1992.

[59] A. Naok i H. Mamitsuka, Query Learning Strategies Using Boosting and Bagging, 1998.

[60] K. Nigam, A. McCallum, S. Thrun i T. Mitchell, „Text Classification from Labeled and Unlabeled Documents using EM," *Machine Learning,* nr 39, p. 103–134, 2000.

[61] I. M. S. Muslea i C. Knoblock, „Selective sampling with co-testing,” w *CRM Workshop on Combining and Selecting Multiple Models With Machine Learning*, Montreal, 2000.

[62] I. Goodfellow, Y. Bengio i A. Courville, Deep Learning, Cambridge, MA: MIT Press[2017], Series: Adaptive computation and machine learning series, 2017, p. 24.

[63] E. Hüllermeier, S. Destercke i I. Couso, „Learning from Imprecise Data: Adjustments of Optimistic and Pessimistic Variants,” w *13th International Conference on Scalable Uncertainty Management (SUM 2019)*, Compiègne, 2019. DOI: ff10.1007/978-3-030-35514-2_20ff. ffhal-02417287f.

[64] Z. Xu, K. Yu, V. Tresp, X. Xu i J. Wang, Representative sampling for text classification using support vector machines, F. Sebastiani, Red., Heidelberg: Springer, 2003.

[65] A. McCallum i K. Nigam, „Employing EM and pool-based active learning for text classification,” w *ICML ’98*, 1998.

[66] Y. Baram, R. El-Yaniv i K. Luz, „Online choice of active learning algorithms,” w *ICML ’03*, 2003.

[67] A. Stachurski i A. Wierzbicki, Podstawy optymalizacji, Warszawa: Oficyna wydawnicza Politechniki Warszawskiej, 2001, pp. s. 7-21.

[68] S. (. R. A. D. Kulshrestha, „Big Data in Military Information & Intelligence Date,” *Indian Navy "Data really powers everything that we do." - Jeff Weiner, Chief Execut*, January 22 2016.

[69] A. Wierzbicki, Teoria i Praktyka Wspomagania Decyzji, Warszawa: Wydawnictwa Uniwersytetu Warszawskiego, 2018, p. s. 36.

[70] E. Figielska, „Algorytmy ewolucyjne i ich zastosowania,” Zeszyty Naukowe 81-92, Politechnika Warszawska.

[71] M. Komosiński, „Optymalizacja wielokryterialna. Algorytmy metaheurystyczne – podsumowanie,” Instytut Informatyki, Politechnika Poznańska, 2018.

[72] „http://algorytmy.ency.pl/artykul/symulowane_wyzarzanie,” [Online].

[73] W. Ogryczak, Skrypt wykładów, Warszawa: Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych, Instytut Automatyki i Informatyki Stosowanej, 2020, p. s.89.

[74] J. Dubois-Lacoste, M. López-Ibáñez i T. Stützle, „Anytime Pareto local search,” *European Journal of Operational Research*, Tomy %1 z %2Volume 243, Issue 2, pp. p. 369-385, 2015, https://doi.org/10.1016/j.ejor.2014.10.062.

[75] 15 01 2023. [Online]. Available: https://newsletter.altdeep.ai/p/the-story-of-mnist-and-the-perils .

[76] 15 01 2023. [Online]. Available: https://www.cs.toronto.edu/~kriz/cifar.html.

[77] „https://www.cs.toronto.edu/~kriz/cifar.html Dostęp z 6.07.2020,” [Online].

[78] „http://refhub.elsevier.com/S0950-7051(19)30074-7/sb52,” [Online].

[79] „http://arxiv.org/abs/1412.6980,” [Online].

[80] „http://refhub.elsevier.com/S0950-7051(19)30074-7/sb50,” [Online].

[81] K. Matela, „Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania (ISR),” *Wiedza Obronna*, 2021.

[82] R. Faligot i R. Kauffer, Służby specjalne. Historia wywiadu i kontrwywiadu na świecie, Warszawa : Wyd. ISKRY, 2006, p. s. 8.

[83] A. Glen i W. Marud, Kontrola przestrzeni powietrznej w czasie kryzysu i wojny, Warszawa : Akademia Obrony Narodowej, 2002, pp. s. 11-12.

[84] A. I. Kuk, Kanwa wywiadu agenturalnego. Podstawy wywiadu osobowego, Warszawa: Akademia Sztuki Wojennej, 2020, p. s. 18.

[85] AJP-2.7, „Allied Joint Doctrine for Intelligence, Counterintelligence and Security," Published by NATO, 2916.

[86] K. Danielewicz, „Komórka sztabowa 2X w operacji typu COIN– wybrane zagadnienia," *Przegląd ABW,* pp. s.1-3.

[87] L. Benes, „OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm.," *Journal of Strategic Security 6, no. 3 Suppl. ,* pp. s. 22-37, 2013.

[88] J. P. 2-01, „Joint and National Intelligence Support to Military Operation," pp. s.III-41, 5 July 2017.

[89] M. Kamiński, „Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community," *Security Dimensions, NO. 32,* pp. s. 90-93, 2019 (82–105), DOI:10.5604/01.3001.0014.0988.

[90] „Federation of American Scientists," [Online]. Available: https://fas.org/irp/program/masint.htm.

[91] S. r. n. Markiewicz, „Sposoby zdobywania informacji," w *System rozpoznania Sił Zbrojnych RP. Doświadczenia i wnioski z funkcjonowania ISTAR. Część I. ISTAR jako element systemu walki,,* Warszawa, 2016, pp. s. 246-247.

[92] M. Wrzosek, „Rozpoznanie wojskowe w wojnach przyszłości – prognozowane kierunki rozwoju," *Bellona Quart. 2020(2): 2021,,* pp. s. 105-126, 2021 DOI: 10.5604/01.3001.0014.4756.

[93] G. Rogova i A. Steinberg, „Formalization of "Context" for Information Fusion," w *Context-Enhanced Information Fusion,* Springer, 2016, DOI 10.1007/978-3-319-28971-7_2. [, pp. s. 27-43 .

[94] M. Contat, V. Nimier i R. Reynaud, „Request Management Using Contextual Information for Classification," w *In: Proceedings of the 5th International Conference on Information Fusion. FUSION ,* Annapolis, 2002 DOI 10.1109/ICIF.2002.10.

[95] B. Essendorfer i W. Mueller, Interoperable Sharing of Data with the Coalition Shared Data (CSD), 2018.

[96] Z. Modrzejewski i P. Balon, System rozpoznania w operacjach poza granicami kraju, Warszawa: Akademia Sztuki Wojennej, 2017, pp. s. 124-125.

[97] S. r. n. Markiewicz, „Sposoby zdobywania informacji," w *[w:] System rozpoznania Sił Zbrojnych RP. Doświadczenia i wnioski z funkcjonowania ISTAR. Część I. ISTAR jako element systemu walki*, Warszawa, Wydawnictwo Akademii Sztuki Wojennej, 2016, pp. s.246-247.

[98] „Defense News, Pentagon tech advisers target how the military digests data," [Online]. Available: https://www.defensenews.com/pentagon/2017/04/06/pentagon-tech-advisers-target-how-the-military-digests-data/ [data dostępu: 13.08.2021].

[99] E. Summary:, „DoD Data Strategy. Unleashing Data to Advance the National Defense Strategy," Office of Prepublication and Security Review, 2020 Sep 30, .

[100] [Online]. Available: https://www.projectpro.io/article/pytorch-vs-tensorflow-2021-a-head-to-head-comparison/416 . [Data uzyskania dostępu: 4 10 2022].

[101] M. Popov1, M. Topolnytskyi i V. Pylypchuk, „A Method for Object Classification in Aerial/Satellite Images with Incorporating Geospatial Information".

[102] [Online]. Available: https://www.globalmediainsight.com/blog/youtube-users-statistics/. [Data uzyskania dostępu: 30 11 2021].

[103] S. Devitt, T. Pearce, T. Perez i P. Bruza, „Mitigating against Cognitive Bias when Eliciting Expert Intuitions," w *International Conference on Thinking*, Brisbane, 2016.

[104] V. Prava, „Identifying and Correcting Cognitive Biases in Subjective Probability Elicitation Surveys: Model Based Approaches," *Military Technology, 2021, vol. 16, no. 2,,* Tomy %1 z %2vol. 16, no. 2 , pp. 309-331, 2016.

[105] P. Donmez, J. Carbonell i P. Bennett, „Dual Strategy Active Learning," w *Proc. 18th European Conf. Machine Learning*, 2007.

[106] [Online]. Available: ship.library.jhu.edu/bitstream/handle/1774.2/39698/PRAVA-DISSERTATION 2016.pdf.

[107] [Online]. Available: https://bernardmarr.com/what-is-big-data/ . [Data uzyskania dostępu: 11 12 2022].

[108] [Online]. Available: https://www.baeldung.com/cs/lazy-vs-eager-learning . [Data uzyskania dostępu: 2 02 2023].

[109] P. Büchlmann i B. Yu, „Analyzing Bagging. The Annals of Statistics," *The Annals of Statistics*, nr 30(4), 2002.

SPIS TABEL

Tabela 1 Wyniki działania sieci neuronowych [17] 54
Tabela 2 Architektury zaprojektowane dla metody MCADL 55
Tabela 3 Przykładowe zestawienie wielu kryteriów 63
Tabela 4 Architektura CNN dla zbioru danych MNIST 69
Tabela 5 Architektura sieci dla bazy CIFAR - 10 70
Tabela 6 Parametry przekazywane do modelu 71
Tabela 7 Wyniki działania modelu MCADL przed wyodrębnieniem 86
Tabela 8 Wyniki działania modelu MCADL po treningu z 86
Tabela 9 Wyniki działania nowej metody przed 87
Tabela 10 Wyniki działania nowej metody po treningu z 87
Tabela 11 Wyniki metody MCADL 93
Tabela 12 Lista rodzajów wywiadu 99

SPIS RYSUNKÓW

Rysunek 1 Infografika przedstawiająca dynamikę i trend wzrostu liczby danych na świecie na przykładzie terytorium USA. Za: [16] 13
Rysunek 2 Koncepcja komponentów i przepływu danych na rzecz Połączonego Obrazu Sytuacji Operacyjnej. Opracowanie własne 15
Rysunek 3 Poziomy reprezentacji obrazu 18
Rysunek 4 Niezrównoważone zbiory klas. 21
Rysunek 5 Zrównoważone zbiory klas 21
Rysunek 6 Metryki oceny klasyfikacji. Opracowanie własne na podstawie [37] 23
Rysunek 7 Schemat uczenia strumieniowego i opartego na puli 30
Rysunek 8 Wizualizacja entropii 32
Rysunek 9 Wizualizacja metody least confident 34
Rysunek 10 Wizualizacja metody margin sampling 35
Rysunek 11 – Schemat działania metody MCADL., na podstawie [2] 44
Rysunek 12 Interpretacja geometryczna funkcji straty dla każdego z czterech kryteriów 50
Rysunek 13 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz 51
Rysunek 14 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz 51
Rysunek 15 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz 52
Rysunek 16 Zestawienie wyników działania metody MCADL, metody MCADL z poziomem wagi alpha =0, oraz metody losowej (RD) 52
Rysunek 17 Zbiór rozwiązań w oparciu o dane symulowane. Tylko dwa wektory niezdominowane y1 i y2 mogą być wyznaczone za pomocą maksymalizacji ważonej sumy ocen. 64
Rysunek 18 Wektory dominujące 66
Rysunek 19 Wektory zdominowane 66

Rysunek 20 Wektory niezdominowane 66
Rysunek 21 Wektory niezdominowane 66
Rysunek 22 Przykładowy zestaw danych MNIST. Na podstawie: [75] 68
Rysunek 23 Przykładowy zestaw danych CIFAR-10. Na podstawie [76] 69
Rysunek 24 Punkty o maksymalnych wartościach dla kryterium A i kryterium B. 74
Rysunek 25 Punkt o minimalnych wartościach kryterium A i kryterium B. 74
Rysunek 26 Sekwencja działań algorytmu analizy wielokryterialnej 75
Rysunek 27 Przebieg procesu działania nowej metody uwzględniającej punkty odniesienia. Opracowanie własne. 76
Rysunek 28 Schemat iteracyjnego doboru punktów odniesienia w powiązaniu z poziomem dokładności. Opracowanie własne 77
Rysunek 29 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej 78
Rysunek 30 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means 79
Rysunek 31 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej 79
Rysunek 32 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means 80
Rysunek 33 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8). 81
Rysunek 34 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8). 82
Rysunek 35 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji losowej na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8). 82
Rysunek 36 Wykres treningowy przedstawiający zachowanie się iteracyjnego dostosowywania poziomów referencji w zależności od poziomu dokładności algorytmu, przy inicjalizacji PCA-k-means na sieci Cifar-10, gdzie punkty odniesienia zostały ustawione na poziomie: gęstość (0,1), podobieństwo (0,15), niepewność (0,9), oparte na etykietach (0,8). 83
Rysunek 37 Diagram działania nowej metody z zaimplementowaną margin sampling, stanowiącą ostatni etap klasyfikacji. 85
Rysunek 38 Wykres działania modelu przed wyodrębnieniem puli próbek z marginesem kierującym do ponownego treningu 86

Rysunek 39 Wyniki działania modelu po treningu z wykorzystaniem próbek z puli marginesu 86
Rysunek 40 Wykres działania modelu przed wyodrębnieniem puli próbek z marginesem kierującym do ponownego treningu 87
Rysunek 41 Wyniki działania modelu po treningu z wykorzystaniem próbek z puli marginesu 87
Rysunek 42 Wyniki działania metody MCADL, w porównaniu z metodą losową (RL) oraz metodą z założeniem wagi α na poziomie „0”. 89
Rysunek 43 Wyniki działania metody MCADL, w kontekście metody losowej (RL) oraz metody z założeniem wagi α na poziomie „0”. 89
Rysunek 44 Wybór próbek według kryterium podobieństwa (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu. 90
Rysunek 45 Wybór próbek według kryterium gęstości (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu. 91
Rysunek 46 Wybór próbek wg kryterium niepewności (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu. 91
Rysunek 47 Wybór próbek wg kryterium opartego na etykietach (plik gif) oraz wykres dokładności tego kryterium w ramach działania całego algorytmu. 92
Rysunek 48 Wykres przedstawiający wyniki działania oryginalnej metody (MCADL)..... 93
Rysunek 49 Wykres wyników nowej metody z punktami odniesienia (inicjalizacja losowa) 94
Rysunek 50 Wykres wyników nowej metody z punktami odniesienia (inicjalizacja PCA – k-means) 94
Rysunek 51 Wyniki działania metody MCADL, nowej metody (ang. new method) z inicjalizacją losową oraz inicjalizacją PCA – k-means, oraz z uwzględnieniem metody margin sampling. 95
Rysunek 52 Wyniki działania nowej metody (ang. new method) w kontekście metody MCADL, oraz dodanej metody margin sampling zastosowanej z uwzględnieniem wag oraz metody margin sampling z zastosowaniem punktów odniesienia, gdzie oś pionowa wskazuje na poziom dokładności, a oś pozioma na liczbę rund, na bazie MNIST 95
Rysunek 53 Wyniki działania nowej metody (ang. new method) w kontekście metody MCADL, oraz dodanej metody margin sampling zastosowanej z uwzględnieniem wag oraz metody margin sampling z zastosowaniem punktów odniesienia, gdzie oś pionowa wskazuje na poziom dokładności, a oś pozioma na liczbę rund, na bazie MNIST 96
Rysunek 54 Wyniki działania nowej metody (ang. new method) w kontekście metody MCADL, oraz dodanej metody margin sampling zastosowanej z uwzględnieniem wag oraz metody margin sampling z zastosowaniem punktów odniesienia, gdzie oś pionowa wskazuje na poziom dokładności, a oś pozioma na liczbę rund, na bazie MNIST 96
Rysunek 55 Jednostki rozpoznawcze – stan na początek 2023 roku. Opracowanie własne..... 104