Informatyka techniczna i sztuczna inteligencja
Technical informatics and Artificial Intelligence
Engineer of XXI Century'2024

Feature identification system in digital images of biometric traces

Jan Spataro [1], Łukasz Hamera[2], Łukasz Więcław[3,*]

[1] *inż., Department of Computer Science and Automatics, Faculty of Mechanical Engineering and Computer Science, University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biala, Poland, js057210@student.ubb.edu.pl*
[2] *mgr inż., Department of Computer Science and Automatics, Faculty of Mechanical Engineering and Computer Science, University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biala, Poland, lhamera@ath.edu.pl*
[3] *dr, Department of Computer Science and Automatics, Faculty of Mechanical Engineering and Computer Science, University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biala, Poland, lwieclaw@ubb.edu.pl*
* *Corresponding author, lwieclaw@ubb.edu.pl*

Abstract: This work focuses on evaluating and comparing the accuracy of various artificial intelligence (AI) models in identifying features in digital images of biometric traces, with a particular emphasis on fingerprints. The objective is to apply these models in forensic science, particularly in the process of fingerprint features identification. Achieving this goal involves a series of research tasks: data collection and preparation, AI model training, testing and comparing the results.

Keywords: Artificial Intelligence; Biometrics; Digital Forensics; YOLO;

System identyfikacji cech w cyfrowych obrazach śladów biometrycznych

Jan Spataro[1], Łukasz Hamera[2], Łukasz Więcław[3,*]

[1] *inż., Department of Computer Science and Automatics, Faculty of Mechanical Engineering and Computer Science, University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biala, Poland, js057210@student.ubb.edu.pl*
[2] *mgr inż., Department of Computer Science and Automatics, Faculty of Mechanical Engineering and Computer Science, University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biala, Poland, lhamera@ath.edu.pl*
[3] *dr, Department of Computer Science and Automatics, Faculty of Mechanical Engineering and Computer Science, University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biala, Poland, lwieclaw@ubb.edu.pl*
* *Corresponding author, lwieclaw@ubb.edu.pl*

Streszczenie: Niniejsza praca skupia się na ocenie i porównaniu skuteczności różnych modeli sztucznej inteligencji (AI) w kontekście identyfikacji cech na cyfrowych obrazach śladów biometrycznych, ze szczególnym uwzględnieniem odcisków palców. Celem pracy jest wdrożenie tych modeli w kryminalistyce, głównie w procesie identyfikacji cech odcisków palców. Realizacja tego celu obejmuje szereg działań badawczych: zbieranie i przygotowanie danych, trenowanie modeli AI oraz testowanie i porównywanie ich wyników.

Słowa kluczowe: Sztuczna inteligencja; Biometria; Kryminalistyka cyfrowa; YOLO; AI; ML;

1. Wstęp

Odciski palców stanowią niezwykle ważny dowód w wielu dochodzeniach kryminalistycznych. Są one jednym z najbardziej niezawodnych śladów pozostawianych przez przestępców, wielokrotnie przyczyniając się do ich

DOI: https://doi.org/10.53052/9788367652292.10

identyfikacji i zatrzymania [8]. Techniki analizy odcisków palców ewoluowały na przestrzeni lat i nadal podlegają intensywnym ulepszeniom, aby sprostać rosnącym wymaganiom współczesnej kryminalistyki [2].

Współczesne technologie cyfrowe znacznie zrewolucjonizowały sposób, w jaki odciski palców są skanowane i analizowane. Tradycyjne metody, choć skuteczne, były czasochłonne i wymagały dużego nakładu pracy. Obecnie, dzięki algorytmom, proces ten został znacznie uproszczony i przyspieszony. Algorytmy komputerowe są w stanie przetwarzać ogromne ilości danych w krótkim czasie, co znacznie zwiększa efektywność analizy.
Skanowanie odcisków palców i ich cyfrowe przetwarzanie pozwala na uzyskanie niezwykle dokładnych wyników, co jest kluczowe w procesie identyfikacji. Technologia ta nie tylko przyspiesza analizę, ale również poprawia jej precyzję, eliminując wiele błędów, które mogłyby pojawić się przy manualnym przetwarzaniu danych.

Celem niniejszej pracy jest przeprowadzenie analizy porównawczej wybranych modeli sztucznej inteligencji (AI) w kontekście detekcji cech na cyfrowych obrazach śladów biometrycznych, ze szczególnym uwzględnieniem odcisków palców. Szerokie zastosowanie technologii biometrycznej w różnych dziedzinach, sprawia, że temat tej pracy jest szczególnie istotny i aktualny. Niniejsze badania skupiają się jednakże na ich wykorzystaniu w kryminalistyce, gdzie wykorzystanie algorytmów AI jest znikome. Porównanie wydajności różnych modeli AI w kontekście identyfikacji odcisków palców może przyczynić się do dalszego rozwoju tej dziedziny oraz zwiększenia skuteczności identyfikacji w śledztwach kryminalnych.

1.1. Biometria

Biometria jest nauką zajmującą się mierzeniem i statystyczną analizą cech fizycznych i behawioralnych człowieka [1]. To nauka, która ma swoje korzenie w starożytności, gdzie w starożytnym Egipcie pracownicy byli identyfikowani na podstawie cech fizycznych [2]. Babilońscy sprzedawcy protokołowali swoje transakcje za pomocą odcisków palca [3]. W późniejszych latach, wraz z postępem technologicznym, biometria stała się bardziej zaawansowana i precyzyjna.

Najwcześniejsze systemy biometryczne były stosowane już w XIX wieku, a jednym z pierwszych przykładów było wykorzystanie odcisków palców w Indiach do identyfikacji przestępców i podpisywania umów [4]. Z czasem, zastosowanie biometrii rozszerzyło się na różne dziedziny, w tym bezpieczeństwo, bankowość, zdrowie i edukację. Dzięki zaawansowanym technologiom, takim jak skanowanie oka, rozpoznawanie twarzy, rozpoznawanie mowy, rozpoznawanie traktu pisania na klawiaturę, a nawet rozpoznawanie DNA, biometria zrewolucjonizowała sposób, w jaki identyfikujemy osoby [5].

Cechy biometryczne są podzielone na dwie główne kategorie: fizyczne i behawioralne. Cechy fizyczne to te, które są nierozłącznie związane z naszą budową biologiczną. Obejmują one odciski palców, skany siatkówki i tęczówki oka, geometrię dłoni, a także cechy twarzy. Cechy behawioralne to te, które są związane z zachowaniem, działaniem jednostki. Przykłady to podpisy, sposób poruszania się (chód), a nawet sposób, w jaki mówimy [6].

Identyfikacja biometryczna w kontekście cech fizycznych człowieka ma wiele zalet [7]. Przede wszystkim jest trudna do sfałszowania, co jest kluczowe dla bezpieczeństwa. Poza tym, jest zazwyczaj wygodna - nie wymaga od użytkownika pamiętania haseł czy kodów. Biometria jest też niezwykle wszechstronna, z potencjalnym zastosowaniem wszędzie, gdzie wymagana jest weryfikacja tożsamości, od telefonów komórkowych po systemy bezpieczeństwa w bankach. Jednak mimo tych zalet, istnieją także pewne wyzwania, takie jak ochrona prywatności i zagrożenia dla bezpieczeństwa danych.

1.2. Daktyloskopia

Daktyloskopia, znana także jako daktylografia, jest dziedziną zajmującą się szczegółowym studiowaniem i analizą odcisków linii papilarnych palca, dłoni, a nawet stopy [1]. Współcześnie ta nauka znajduje szerokie zastosowanie, szczególnie w sferze prawnej, kryminalistyce oraz w identyfikacji personalnej na urządzeniach mobilnych.

Zgodnie z szacunkami Galtona, prawdopodobieństwo powtórzenia się układu wszystkich minucji na dwóch odciskach tego samego palca różnych osób wynosi około 1,45 × 10^-11 [9]. Najnowsze badania D. Stoney'a wskazują, że prawdopodobieństwo uzyskania dwóch identycznych obrazów linii papilarnych, gdzie układ, ukierunkowanie oraz

liczba listewek skórnych będą takie same, wynosi w przybliżeniu 1,2 × 10^-80. Dzięki temu odciski palców są niezwykle wartościowym dowodem w śledztwach, umożliwiającym jednoznaczną identyfikację sprawców przestępstw [6].

W dziedzinie daktyloskopii funkcjonuje fundamentalna Zasada 3N, obejmująca **Niezmienność**, **Niepowtarzalność** i **Nieodwracalność,** opracowana jeszcze przez Francisa Galtona [9]:

- **Niezmienność**: Wzory linii papilarnych, które formują się na dłoniach i palcach w okresie płodowym, pozostają stałe i niezmienne przez całe życie człowieka.
- **Niepowtarzalność**: Ta zasada stwierdza, że każdy człowiek posiada unikalne wzory linii papilarnych, które różnią się od odcisków palców innych osób.
- **Nieodwracalność**: Oznacza, że procesu formowania odcisków palców nie można zatrzeć ani odwrócić, co czyni je niezawodnym środkiem identyfikacji.

W systemie Galtona-Henry'ego, wprowadzono podstawowe pojęcia stosowane do dziś w daktyloskopii. Jednym z tych pojęć, które będą wykorzystywane w niniejszych badaniach są minucje. Są to indywidualne cechy listewek skórnych, obejmujące zazwyczaj początki, zakończenia, rozwidlenia, złączenia, oczka, haczyki, mostki, punkty, odcinki. Współczesne standardy klasyfikacji minucji w Polsce opierają się na systemie opracowanym przez Czesława Grzeszyka [8]. Jego praca nie tylko ujednoliciła klasyfikację tych cech, ale także określiła częstość występowania poszczególnych typów minucji na palcach i dłoniach zarówno prawej, jak i lewej ręki, uwzględniając przy tym zmienne takie jak płeć i typ wzoru linii papilarnych. W zaproponowanej przez niego klasyfikacji wyodrębniono 21 typów minucji, z czego 17 jest unikalnych:

- Początek / Zakończenie
- Rozwidlenie / Złączenie pojedyncze
- Rozwidlenia podwójne / Złączenie podwójne
- Rozwidlenie potrójne/ Złączenie potrójne
- Haczyk
- Oczko pojedyncze
- Oczko podwójne
- Mostek pojedynczy
- Mostek bliźniaczy
- Punkt
- Odcinek
- Styk boczny
- Linia przechodząca
- Skrzyżowanie
- Trójnóg
- Linia szczątkowa
- Minucja typu „M"

1.3. Sieć neuronowa

Sztuczna inteligencja (AI) to gałąź informatyki zajmująca się opracowywaniem i doskonaleniem algorytmów komputerowych, które wykonują trudne zadania, normalnie wymagającej ludzkiej inteligencji, w procesie uczenia się, w celu osiągnięcia sukcesu [10]. Te zadania obejmują m.in. przetwarzanie mowy, rozpoznawanie wzorców i obrazów, uczenie się na podstawie doświadczeń oraz podejmowanie decyzji i rozwiązywanie problemów.

Uczenie maszynowe (ML) jest specjalizacją w ramach sztucznej inteligencji, skupiającą się na tworzeniu modeli komputerowych zdolnych do uczenia się na podstawie doświadczeń. Modele ML są trenowane na dużych zbiorach danych, co pozwala im rozpoznawać wzorce i trendy. Celem uczenia maszynowego jest umożliwienie komputerom samodzielnego doskonalenia swoich algorytmów bez konieczności bezpośredniego programowania przez ludzi.

Uczenie maszynowe obejmuje różnorodne techniki, takie jak nadzorowane, nienadzorowane i wzmacniające [10].
W przypadku uczenia nadzorowanego, model jest szkolony przy użyciu zestawu danych wejściowych oraz odpowiadających im wyników, co pozwala na przewidywanie wyników dla nowych danych. Uczenie nienadzorowane

polega na tym, że model identyfikuje wzorce w danych bez potrzeby posiadania wyników końcowych. W uczeniu ze wzmocnieniem, model zdobywa umiejętności poprzez interakcję ze środowiskiem i otrzymywanie nagród za podejmowanie właściwych decyzji.

Głębokie uczenie, będące zaawansowaną dziedziną uczenia maszynowego, skupia się na sieciach neuronowych o wielu warstwach, często trzech lub więcej [11]. Te sieci próbują naśladować działanie ludzkiego mózgu, choć są dalekie od jego pełnej emulacji. Ich celem jest nauczenie komputerów samodzielnego rozpoznawania złożonych wzorców w danych. Głębokie uczenie odgrywa kluczową rolę w obszarach takich jak przetwarzanie obrazów, rozpoznawanie mowy oraz analiza szeregów czasowych. Wśród głównych architektur stosowanych w głębokim uczeniu wyróżnia się sieci konwolucyjne (CNN)[12] oraz sieci rekurencyjne (RNN)[13].

2. Założenia

Niniejsza praca obejmuje porównanie różnych architektur sieci, które specjalizują się w procesie wykrywania obiektów na obrazach. W niniejszym problemie wybrany model sieci neuronowej ma za zadanie odszukać minucję na obrazie linii papilarnych. Wykryta cecha oznaczona jest poprzez pozycję, wielkość oraz typ.
Do przeprowadzania badań wybrano następujące modele:

- **YOLOv5** [14], należący do rodziny architektur You Only Look Once (YOLO), jest zaawansowanym modelem wykorzystywanym do detekcji obiektów w czasie rzeczywistym. Opracowany i udostępniony przez firmę Ultralytics, YOLOv5, mimo iż na rynku dostępne są już jego nowsze wersje, wyróżnia się wyjątkowym kompromisem między szybkością a precyzją detekcji.
- **YOLOv8** [15]**,** to najnowsza wersja modelu detekcji obiektów YOLO, opracowana przez firmę Ultralytics. Charakteryzuje się nowoczesnością, wysoką precyzją i efektywnością, umożliwiając klasyfikację, detekcję oraz segmentację obiektów w czasie rzeczywistym. Wprowadza liczne innowacje i ulepszenia, które zwiększają dokładność i wydajność w porównaniu do poprzednich wersji YOLO. YOLOv8 został zaprojektowany jako elastyczny framework, kompatybilny z wszystkimi wcześniejszymi wersjami YOLO, co pozwala na łatwe przełączanie i porównywanie wyników między różnymi wersjami.
- **Roboflow 3.0** [16], najnowsza wersja platformy Roboflow, to zaawansowany system do detekcji obiektów w zakresie wizji komputerowej. Umożliwia efektywną anotację, zarządzanie oraz przetwarzanie zbiorów danych obrazowych. Roboflow 3.0 wprowadza liczne usprawnienia i optymalizacje, w tym bardziej intuicyjny interfejs użytkownika oraz zaawansowane narzędzia analityczne. Te zmiany przyspieszają proces rozwoju projektów związanych z wizją komputerową, jednocześnie zwiększając precyzję i efektywność wdrażanych rozwiązań.
- **Detectron2** [17], to otwartoźródłowa platforma stworzona przez Facebook AI Research (FAIR) do rozpoznawania obiektów i segmentacji. Jest to druga generacja biblioteki Detectron, zbudowana na bazie PyTorch, co zapewnia większą elastyczność i łatwość integracji z funkcjami tej nowoczesnej biblioteki. Detectron2 umożliwia implementację najnowszych modeli i algorytmów do detekcji obiektów, segmentacji instancji i segmentacji semantycznej, a także klasyfikacji. Ponadto, dostarcza narzędzi, które są nieocenione dla naukowców i inżynierów w pracach badawczych oraz wdrażaniu praktycznych rozwiązań.
- **YOLO-NAS** [18], (You Only Look Once - Neural Architecture Search) to model wykrywania obiektów, który integruje strategię YOLO, popularną w czasie rzeczywistym metodę detekcji obiektów, z Neural Architecture Search (NAS). NAS jest techniką automatycznego wyszukiwania optymalnej architektury sieci neuronowej dla specyficznych zadań.

3. Realizacja

Na potrzeby niniejszego badania wykorzystano bazę danych składającą się z 703 obrazy linii papilarnych, pobranych z wykorzystaniem skanera optycznego Cross Match LSCAN 1000T. Obrazy były pobierane w rozdzielczości 1000dpi, co umożliwia rejestrację odcisków palców z dużą liczbą szczegółów. Dane te zostały poddane augumentacji poprzez wykonanie operacji: lustrzanemu odbiciu poziomemu, obrotowi o 90° (zarówno zgodnie z ruchem wskazówek zegara, jak i przeciwnie do niego) oraz obrotowi w zakresie od -15° do +15°. Dodatkowo, została zmieniona ekspozycja w zakresie od -25% do +25%. Łącznie, po przetwarzaniu i augmentacji danych, całkowity zbiór danych liczył 1819 obrazów. Działania te wykonano w pakiecie Roboflow.
Następnie przeprowadzono podział zbioru danych na trzy części:

- **TRAIN SET** (Zestaw treningowy): Składał się z 92% wszystkich obrazów, co stanowiło 1674 obrazy. Jest to główna część zbioru danych, która służy do treningu modeli uczenia maszynowego.
- **VALID SET** (Zestaw walidacyjny): Stanowił 4% zbioru danych, zawierający 76 obrazów. Ten zestaw jest używany do oceny wydajności modelu w trakcie treningu i pomaga w doborze optymalnych hiperparametrów.
- **TEST SET** (Zestaw testowy): Składał się z 4% wszystkich obrazów, co daje 69 obrazów. Jest to niezależna część zbioru danych, która jest wykorzystywana do ostatecznej oceny wydajności modelu po zakończeniu treningu.

Z wykorzystaniem narzędzia Computer Vision Annotation Tool [19] , skrótowo nazywanego CVAT, przygotowano dane treningowe do zadań uczenia maszynowego. Celem było etykietowanie obiektów na obrazach, zgodnie z następującymi kategoriami: tło / linie papilarne, minucje typów: zakończenie, rozwidlenie, odcinek i mostek oraz pory.

Finalnie przeprowadzono proces trenowania modeli w platformie Google Colab, z wykorzystaniem procesora NVIDIA Tesla T4, który jest powszechnie wykorzystywany w uczeniu maszynowym.

4. Wyniki

W niniejszym rozdziale przeprowadzono szczegółową analizę wyników eksperymentów dotyczących różnych zaawansowanych modeli detekcji obiektów. Skupiono się na ocenie ich wydajności, precyzji, recallu oraz innych kluczowych wskaźnikach, takich jak średnia dokładność (mAP). Wyniki zilustrowano za pomocą tabel i wykresów, co ułatwia zrozumienie i porównanie skuteczności każdego modelu. Dodatkowo, przeanalizowano macierze pomyłek, aby lepiej zrozumieć specyficzne wyzwania i ograniczenia poszczególnych modeli.

4.1. Ocena jakości modelu

Metryki modeli stanowią fundamentalne narzędzie w budowie i ocenie modeli uczenia maszynowego. Umożliwiają one ilościową ocenę jakości modelu, identyfikując zarówno jego mocne, jak i słabe strony, a także wskazują kierunki dalszej optymalizacji. Poniżej przedstawiono kluczowe metryki wykorzystywane w ocenie modeli uczenia maszynowego, zwłaszcza w kontekście problemów klasyfikacji i detekcji obiektów:

1. **Dokładność (*Accuracy*)**: Proporcja poprawnie sklasyfikowanych przypadków do wszystkich przypadków.
2. **Precyzja (*Precision*)**: Proporcja prawdziwie pozytywnych wyników do wszystkich wyników uznanych za pozytywne.
3. **Czułość (*Recall*)**: Proporcja prawdziwie pozytywnych wyników do wszystkich rzeczywistych pozytywnych przypadków.

Powyższe metryki zostały obliczone na podstawie wartości wyliczonych z tzw. macierzy pomyłek (Tabela 1). Jest to narzędzie stosowane w statystyce i uczeniu maszynowym do oceny wydajności modeli klasyfikacyjnych. Reprezentowana jest przez tabele, która pozwala zrozumieć, jak model radzi sobie z przewidywaniami i w których przypadkach popełnia błędy. Oto kluczowe elementy confusion matrix:

- **True Positive (*TP*)**: Liczba przypadków, które model poprawnie sklasyfikował jako pozytywne.
- **True Negative (*TN*)**: Liczba przypadków, które model poprawnie sklasyfikował jako negatywne
- **False Positive (*FP*)**: Liczba przypadków, które model błędnie sklasyfikował jako pozytywne, mimo że są negatywne.
- **False Negative (*FN*)**: Liczba przypadków, które model błędnie sklasyfikował jako negatywne, mimo że są pozytywne.

Tabela 1. Macierz pomyłek

	Przewidywania pozytywne	**Przewidywania negatywne**
Prawdziwie pozytywne	TP	FN
Prawdziwie negatywne	FP	TN

Poniżej przedstawiono wzory (1, 2, 3, 4) poszczególnych metryk:

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$mAp = \frac{1}{Q}\sum_{q=1}^{Q} AP(q) \tag{3}$$

gdzie:

Q - liczba zapytań $AP(q)$,

$$AP(q) = \frac{1}{Recall(q)}\int_0^1 p(r)dr \tag{4}$$

gdzie:

$p(r)$ - to precyzja przy danym progu recall r ,

$Recall(q)$ - maksymalny recall dla zapytania q .

W praktyce wartość AP obliczana jest zazwyczaj jako sumę powierzchni prostokątów pod krzywą Precision-Recall (P -R):

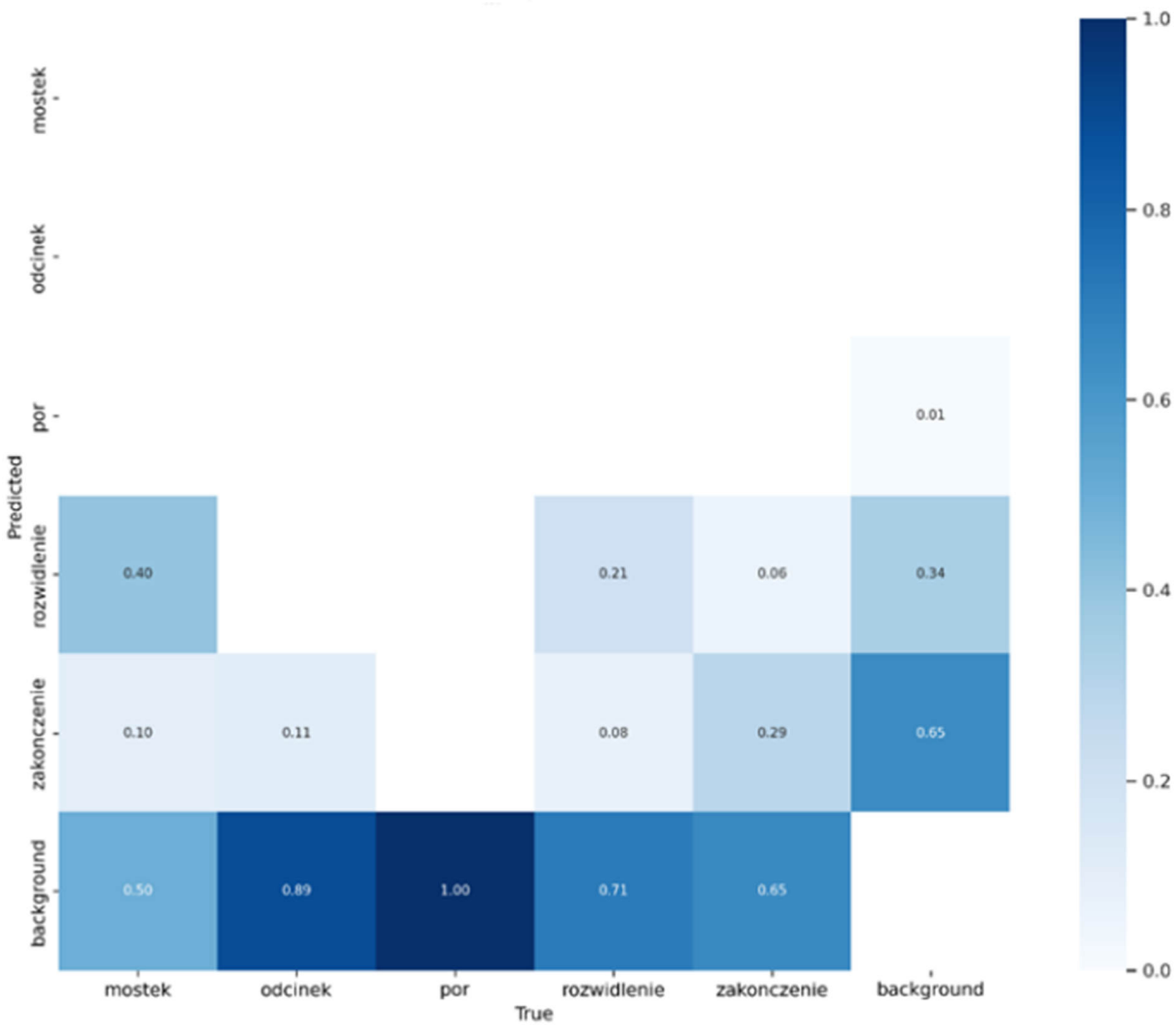
$$AP(q) \cong \sum_n \left(R_n - R_{(n-1)}\right)P_n \tag{5}$$

4.2. YOLOv5

Model YOLOv5 uzyskał suboptymalne wyniki z *mAP* na poziomie 5,87% (tabela 2), co jest niewystarczające dla aplikacji wymagających wysokiej dokładności klasyfikacji. Precyzja tego modelu wyniosła 41,44%, co sugeruje, że model jest zdolny do generowania poprawnych detekcji, ale z niewielką częstotliwością. Niska wartość *Recall* na poziomie 7,73% wskazuje na pomijanie dużej liczby istotnych obiektów, co prowadzi do niepełnej detekcji. Macierz pomyłek dla tego modelu widnieje na rysunku Rysunek 1.

Tabela 2. Podstawowe metryki modelu YOLOv5

Model	**mAP**	**Precision**	**Recall**
YOLOv5	5.87%	41.44%	7.73%



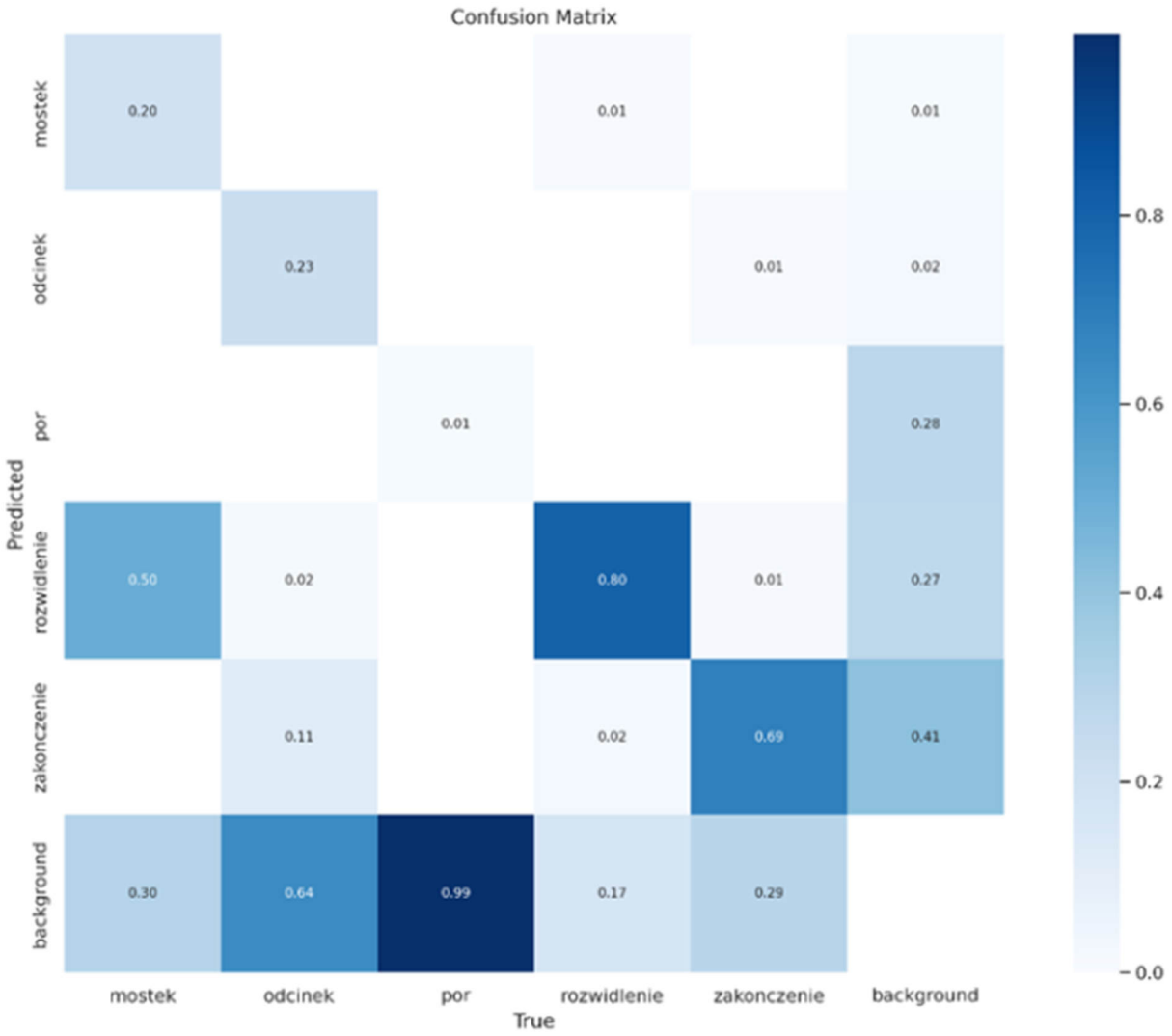
Rysunek 1. Macierz pomyłek dla modelu YOLOv5

4.3. YOLOv8

Modele YOLOv8, w wariantach L i M, wykazały wyższą efektywność, osiągając *mAP* wynoszące odpowiednio 37,09% i 35,85%. Precyzja dla wariantu L wyniosła 65,76%, natomiast dla wariantu M – 61,25%. Oba modele uzyskały zbliżone wartości *Recall*, oscylujące wokół 33%, co sugeruje potrzebę dalszej poprawy zdolności do detekcji obiektów. Macierz pomyłek dla modelu YOLOv8L widnieje na rysunku Rysunek 2.

Tabela 3. Podstawowe metryki modeli z rodziny YOLOv8

Model	***mAP***	***Precision***	***Recall***
YOLOv8L	37.09%	65.76%	33.42%
YOLOv8M	35,85%	61,25%	33,05%



Rysunek 2. Macierz pomyłek dla modelu YOLOv8L

4.4. Roboflow 3.0

Ze względu na fakt, że proces uczenia tego modelu odbywał się na platformie internetowej Roboflow, nie było możliwe wygenerowanie macierzy pomyłek.

Tabela 4. Podstawowe metryki modelu Roboflow 3.0

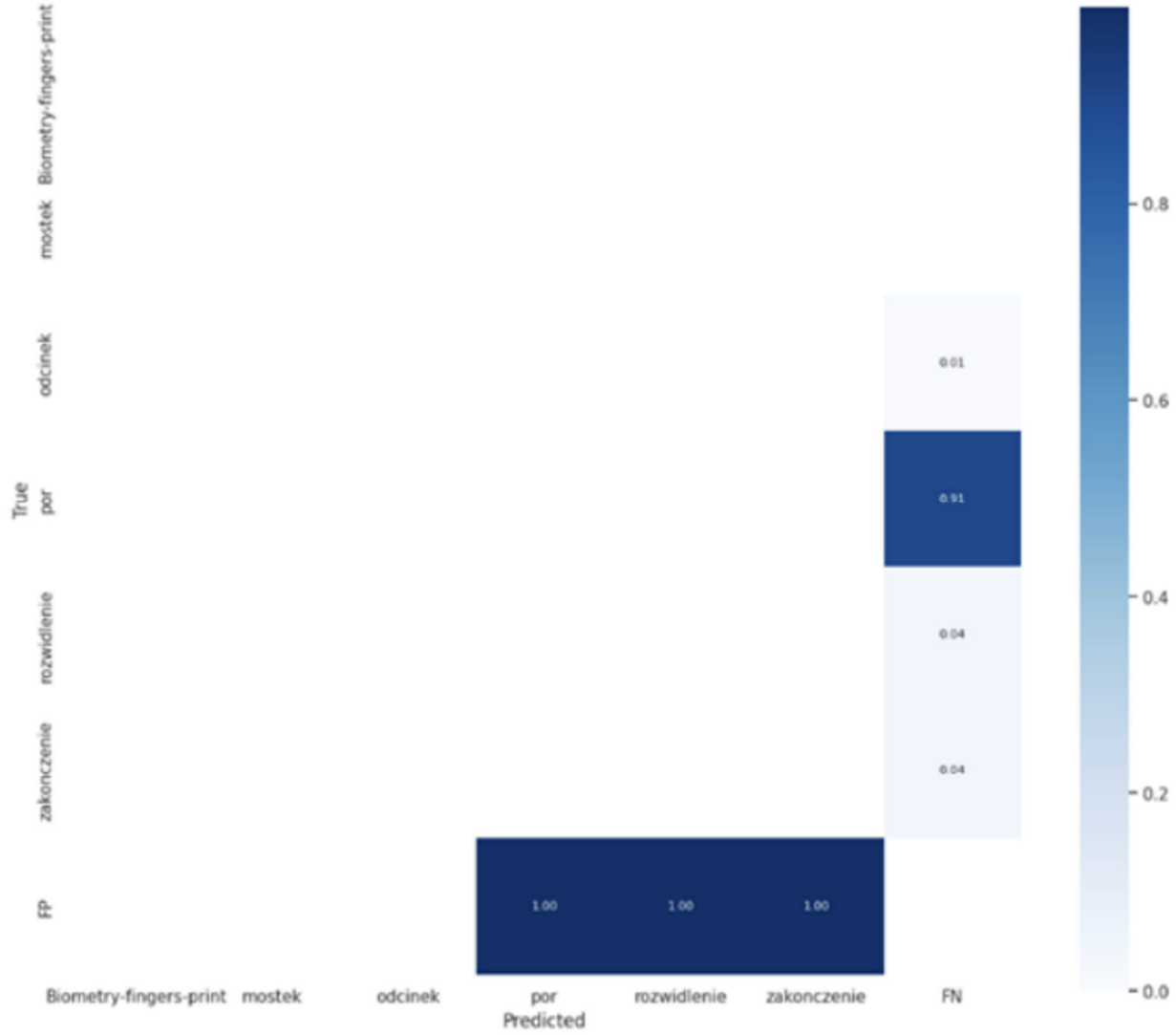
Model	***mAP***	***Precision***	***Recall***
Roboflow 3.0	49.4%	83.0%	42.2%

4.5. Detectron 2

Detectron2 osiągnął najniższą skuteczność spośród wszystkich przetestowanych modeli, z *mAP* na poziomie 7,18%. Sugeruje to istotne ograniczenia modelu w praktycznych zastosowaniach. Duża różnica między wartościami *Precision* i *Recall* wskazuje na konieczność dokładnej analizy błędów klasyfikacji oraz wdrożenia technik zwiększających zdolność modelu do generalizacji.

Tabela 5. Podstawowe metryki modelu Detectron 2

Model	***mAP***	***Precision***	***Recall***
Detectron 2	7.18%	15.5%	12.4%



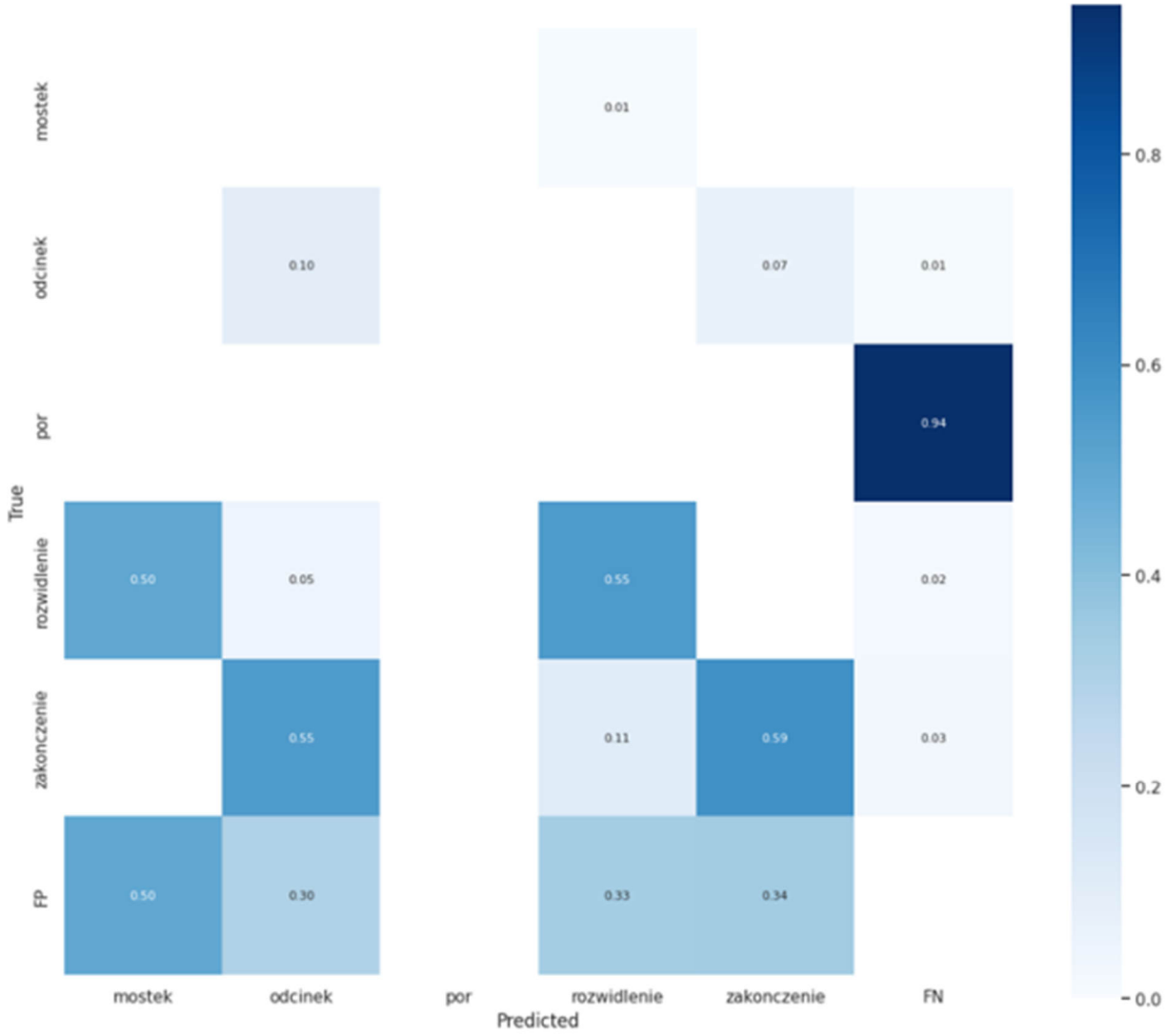
Rysunek 3. Macierz pomyłek dla modelu Detectron 2

4.6. YOLO-NAS

Model YOLO-NAS uzyskał *mAP* na poziomie 18,07%, przy niskiej precyzji (3,125%) i umiarkowanej czułości (35,43%). Wskazuje to na niezbalansowaną strategię detekcji, w której model generuje wiele fałszywie pozytywnych wyników, pomijając jednocześnie prawdziwe obiekty.

Tabela 6. Podstawowe metryki modelu YOLO-NAS

Model	***mAP***	***Precision***	***Recall***
YOLO-NAS	18.07%	3.125%	35.43%



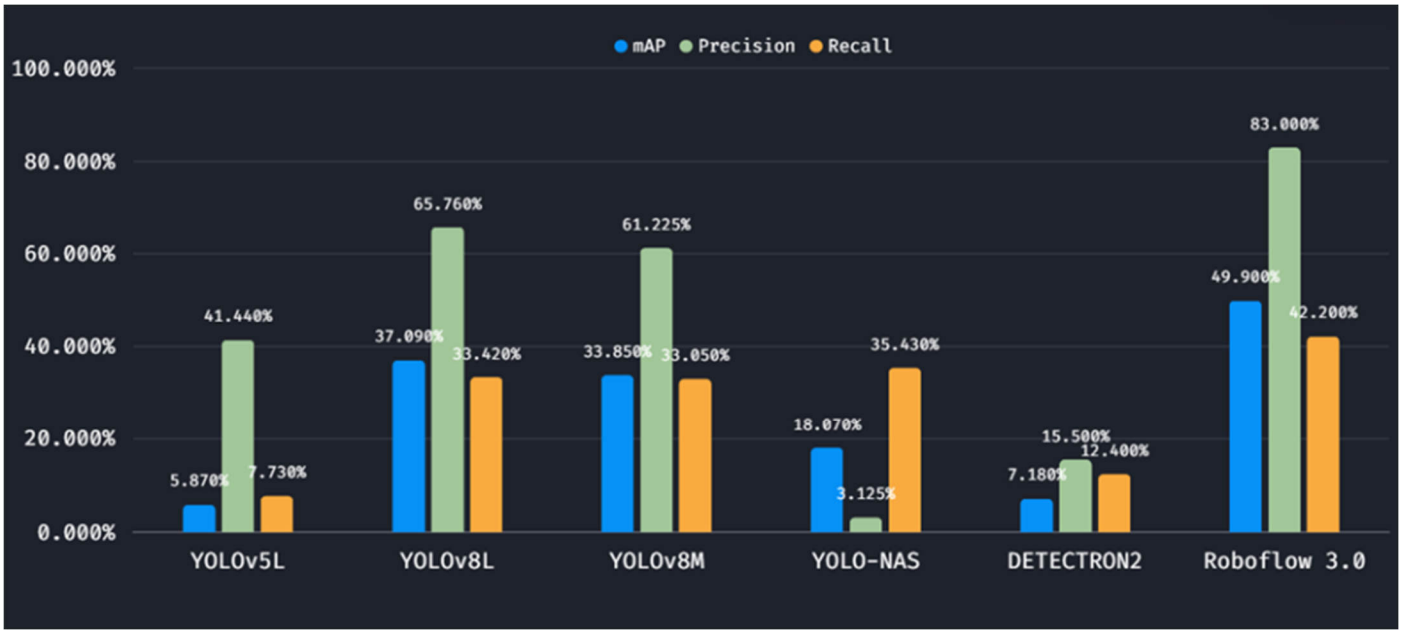
Rysunek 4. Macierz pomyłek dla modelu YOLO-NAS

5. Podsumowanie i wnioski

W ramach niniejszych badań przeprowadzono szczegółową ocenę wydajności modeli detekcji obiektów z rodziny YOLO oraz Detectron2, stosując znormalizowane wskaźniki takie jak średnia precyzja (mean Average Precision, *mAP*), precyzja (*Precision*) oraz czułość (*Recall*). Eksperymenty miały na celu zarówno ocenę skuteczności algorytmów w detekcji obiektów, jak i identyfikację obszarów, które wymagają dalszej optymalizacji i rozwoju. Porównanie wyników wszystkich przebadanych modeli widnieje na rysunku Rysunek 5.

Analiza wyników przeprowadzonych eksperymentów wskazuje, że w kontekście zastosowań kryminalistycznych, takich jak detekcja minucji, modele YOLOv8, w szczególności wariant L, oraz Roboflow 3.0 Object Detection, wykazują najwięcej obiecujących właściwości. Wysoka precyzja modelu YOLOv8 L, w połączeniu z umiarkowaną skutecznością detekcji (*mAP*) oraz zdolnością do identyfikacji większej liczby istotnych obiektów (*Recall*), czyni go potencjalnie wartościowym kandydatem do dalszej optymalizacji pod kątem specyficznych zastosowań kryminalistycznych.

Model Roboflow 3.0 Object Detection uzyskał najwyższą średnią precyzję spośród testowanych algorytmów. Wskazuje to, że model ten jest bardziej skuteczny w ograniczaniu liczby fałszywych alarmów, co jest kluczową cechą w aplikacjach wymagających wysokiej precyzji i niezawodności wyników.



Rysunek 5. Wykres metryk dla zbadanych modeli

Dalsza poprawa skuteczności sieci neuronowych może być przeprowadzana w obszarach:

- **Rozszerzenie zbioru danych**: Wykorzystanie bardziej zróżnicowanego zbioru danych minucji, obejmującego przypadki graniczne i subtelne różnice w cechach charakterystycznych.
- **Optymalizacja hiperparametrów**: Precyzyjne dostrojenie hiperparametrów modeli, takich jak wskaźniki uczenia, rozmiar partii (batch size) oraz parametry regularyzacji, w celu maksymalizacji wydajności modeli w analizie złożonych wzorców minucji.
- **Augmentacja danych**: Wykorzystanie zaawansowanych technik augmentacji danych, takich jak transformacje geometryczne i fotometryczne, aby lepiej symulować rzeczywiste warunki analizy minucji.
- **Analiza błędów**: Dogłębna analiza błędnych klasyfikacji modelu, zwłaszcza tych związanych z fałszywie negatywnymi wynikami, co jest kluczowe dla zastosowań kryminalistycznych.
- **Eksperymenty z architekturą sieci**: Testowanie różnorodnych architektur sieci neuronowych, w tym wersji YOLO oraz Detectron, aby sprawdzić, które najlepiej radzą sobie z detekcją minucji na obrazach o różnej jakości i w różnych warunkach oświetleniowych.

Reference

1. J. Starobinski. Biometric Authentication Systems. Technological Innovations, 2018.
2. T. Nakashima, et al. Applications of Biometric Technology in Forensic Science. Forensic Review Journal, 2019.
3. H. Kim. Biometrics in the 21st Century: Technologies and Applications. Academic Press, 2020.
4. S. Gallagher. Ancient Egyptian Identification Methods. History of Science, 2017.
5. L. Chen. Biometric Identification in Ancient Civilizations. Journal of Historical Studies, 2016.
6. R. Srivastava. Evolution of Fingerprint Identification in India. Indian Journal of Criminology, 2020.
7. A. Johnson, R. Miller. Behavioral Biometrics: Current Trends and Future Directions. Information Security Journal, 2021.
8. Cz. Grzeszyk. Badania nad minucjami linii papilarnych. Problemy Kryminalistyki, (96), 1972,
9. F. Galton. Fingerprints. Galton Laboratory for National Eugenics. London : Macmillan and Co., 1892
10. S.J. Russell; P. Norvig. Artificial Intelligence: A Modern Approach (4th ed.). Hoboken: Pearson. ISBN 978-0-1346-1099-3, 2021.
11. Y. LeCun, Y. Bengio, G. Hinton. Deep Learning. Nature. 521 (7553): 436–444. doi:10.1038/nature14539, 2015.
12. K. Fukushima. Neural network model for a mechanism of pattern recognition unaffected by shift in position—Neocognitron. Trans. IECE (In Japanese). J62-A (10): 658–665. doi:10.1007/bf00344251, 1979.

13. A. Zhang, Z. Lipton, M. Li, A. Smola. 10. Modern Recurrent Neural Networks. Dive into deep learning. Cambridge New York Port Melbourne New Delhi Singapore: Cambridge University Press. ISBN 978-1-009-38943-3, 2024.
14. YOLOv5. Available online: https://github.com/ultralytics/yolov5 (accessed on 20.10.2024).
15. YOLOv8. Available online: https://yolov8.com/ (accessed on 20.10.2024).
16. Roboflow 3.0. Available online: https://blog.roboflow.com/roboflow-train-3-0/ (accessed on 20.10.2024).
17. Detectron2. Available online: https://github.com/facebookresearch/detectron2 (accessed on 20.10.2024).
18. YOLO-NAS. Available online: https://github.com/Deci-AI/super-gradients/blob/master/YOLONAS.md (accessed on 20.10.2024).
19. Dokumentacja oprogramowania CVAT [Online]. Available online: https://github.com/opencv/cvat (accessed on 20.10.2024).