**Wojciech Kowalski**

e-mail: 189792@student.ue.wroc.pl

ORCID: 0009-0004-2200-8553

Uniwersytet Ekonomiczny we Wrocławiu

# Sztuczna inteligencja w zarządzaniu bezpieczeństwem masowych imprez. Identyfikacja potencjalnych zagrożeń, takich jak terroryzm i zamieszki

DOI: 10.15611/2024.80.2.06
JEL Classification: C61



**Cytuj jako**: Kowalski, M. (2024). Sztuczna inteligencja w zarządzaniu bezpieczeństwem masowych imprez. Identyfikacja potencjalnych zagrożeń, takich jak terroryzm i zamieszki. W: H. Dudycz (red.), *Informatyka w biznesie* (s. 79-91). Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

**Streszczenie:** W artykule omówiono zastosowanie sztucznej inteligencji (SI) w zarządzaniu bezpieczeństwem imprez masowych. Bezpieczeństwo na wydarzeniach tego typu jest kluczowe ze względu na ryzyko zamieszek lub terroryzmu. SI może wspierać służby porządkowe poprzez analizę danych w czasie rzeczywistym i przewidywanie potencjalnych zagrożeń. W opracowaniu przedstawiono technologie, takie jak rozpoznawanie twarzy, zarządzanie tłumem oraz wykrywanie niebezpiecznych przedmiotów.

**Słowa kluczowe:** sztuczna inteligencja, imprezy masowe, rozpoznawanie twarzy, wykrywanie przedmiotów, zarządzanie tłumem

## 1. Wstęp

Bezpieczeństwo jest kluczowym aspektem podczas organizacji imprez i wydarzeń masowych, takich jak koncerty, festiwale czy zgromadzenia publiczne. Terroryzm i zamieszki podczas takich przedsięwzięć stanowią zagrożenie dla bezpieczeństwa, często prowadząc do utraty zdrowia lub życia ich uczestników. Mogą się także przyczyniać do powszechnego chaosu i utrudnienia działania służb porządkowych.

Zamieszki we Francji w 2005 r. stanowią przykład tego, jak zachowania masowe mogą rozwijać się w sposób nieprzewidywalny i stawać się nie do opanowania przez organy porządkowe lub rząd (Bonnasse-Gahot i in., 2018). Badania podkreślają wieloaspektowy charakter terroryzmu, definiując go jako przemoc lub groźbę mającą na celu wzbudzenie strachu i bodziec do wszczęcia alarmu (Gassebner i Luechinger, 2011). Zrozumienie dynamiki i konsekwencji takich zdarzeń może mieć kluczowe

znaczenie dla skutecznego zarządzania bezpieczeństwem imprez masowych, szczególnie jeśli zostaną wykryte w ich początkowych fazach rozwoju.

Sztuczna inteligencja (SI) odnosi się do zdolności systemów komputerowych do wykonywania zadań, które normalnie wymagają ludzkiej inteligencji, jak rozpoznawanie obrazów, przetwarzanie języka czy podejmowanie decyzji (Chollet, 2019). W kontekście bezpieczeństwa imprez masowych SI może być wykorzystywana do analizy danych z monitoringu w czasie rzeczywistym i przewidywania potencjalnych zagrożeń. Monitoring oparty na SI umożliwia szybszą i bardziej efektywną reakcję na sytuacje kryzysowe.

Celem niniejszego artykułu jest określenie, w jaki sposób sztuczna inteligencja może być wykorzystana do poprawy bezpieczeństwa podczas imprez masowych. Uwaga skupiona będzie na analizie istniejących technologii, ich zastosowaniach w praktyce oraz korzyściach i wyzwaniach związanych z ich implementacją. W artykule postawiono następujące pytania badawcze: Jakie technologie sztucznej inteligencji są najskuteczniejsze w identyfikacji zagrożeń podczas imprez masowych? Jakie są główne wyzwania związane z implementacją sztucznej inteligencji w zarządzaniu bezpieczeństwem? Jakie korzyści mogą przynieść nowoczesne technologie w kontekście zapobiegania terroryzmowi i zamieszkom?

W artykule wykorzystano kombinację metod badawczych, w tym analizę literatury oraz studia przypadków, w celu zidentyfikowania roli sztucznej inteligencji w zarządzaniu bezpieczeństwem. Analiza literatury pozwoliła na syntetyzowanie aktualnych badań nad technologiami SI stosowanymi w kontekście imprez masowych, podczas gdy studia przypadków umożliwiły praktyczne zrozumienie realnych przykładów implementacji tych technologii. Przeprowadzono również analizę danych z różnych źródeł, co pozwoliło na wyciągnięcie wniosków dotyczących skuteczności SI w identyfikacji zagrożeń.

W części pierwszej artykułu omówione zostały ogólne aspekty zastosowania SI w zarządzaniu bezpieczeństwem imprez masowych, w kolejnych częściach przedstawiono szczegółowe omówienie technologii rozpoznawania twarzy, monitoringu tłumu oraz wykrywania potencjalnych zagrożeń. Artykuł kończy się omówieniem zalet, wyzwań oraz przyszłych kierunków rozwoju technologii SI w kontekście bezpieczeństwa publicznego.

## 2. Rola sztucznej inteligencji w bezpieczeństwie masowych imprez

Zapewnienie bezpieczeństwa podczas imprez masowych, np.: koncertów, festiwali, wydarzeń sportowych czy zgromadzeń publicznych, jest kluczowym aspektem ich organizacji. Wydarzenia te przyciągają tysiące uczestników, co stanowi wyzwanie dla służb porządkowych. Duża liczba ludzi na ograniczonej przestrzeni zwiększa ryzyko terroryzmu i zamieszek. W celu identyfikacji potencjalnego zagrożenia oraz

niezwłocznej na nie reakcji, niezbędne są zaawansowane metody zarządzania bezpieczeństwem.

Zastosowanie Sztucznej inteligencji (SI) w celach zapewnienia lub poprawy bezpieczeństwa na imprezach masowych wzrasta. Dzięki zdolności do analizy danych w czasie rzeczywistym SI może wspierać służby porządkowe w identyfikacji podejrzanych zachowań i przewidywaniu potencjalnych zagrożeń. Przykładem są systemy rozpoznawania twarzy mogące monitorować tłumy, identyfikując osoby z list poszukiwanych lub znane z przestępczej działalności. Dzięki temu możliwe jest wyeliminowanie zagrożeń, zanim zdążą one eskalować (Deng i in., 2021).

SI może analizować wzorce ruchu tłumu, identyfikując miejsca o ryzyku przeludnienia, co pozwala na podejmowanie działań prewencyjnych, jak relokacja uczestników lub zwiększenie liczby służb porządkowych w newralgicznych punktach (Tyagi i in., 2022).

Kolejnym przykładem zastosowania SI w praktyce jest wykorzystanie dronów wyposażonych w kamery, które monitorują teren imprezy z powietrza. Dane zbierane przez drony są analizowane w czasie rzeczywistym przez algorytmy SI, które identyfikują podejrzane zachowania i informują o nich odpowiednie służby. (Husman i in., 2021). Drony te mogą być wyposażone w systemy do wykrywania niebezpiecznych przedmiotów: broni czy materiałów wybuchowych. Wykorzystanie dronów zwiększa zasięg i skuteczność monitoringu, umożliwiając służbom porządkowym szybką i precyzyjną reakcję na potencjalne zagrożenia (Ha i in., 2024).

Sztuczna inteligencja nie tylko zwiększa efektywność monitoringu, ale również wspiera proces decyzyjny służb porządkowych, dostarczając im precyzyjnych i aktualnych informacji. Algorytmy SI potrafią analizować dane z różnych źródeł – kamer monitoringu, mediów społecznościowych i raportów terenowych w celu dostarczenia kompleksowego obrazu sytuacji. Dzięki temu zapewniona jest szybka reakcja na zmieniającą się sytuację i minimalizowanie ryzyka wystąpienia incydentów zagrażających życiu i zdrowiu uczestników. SI może także wspierać działania prewencyjne poprzez prognozowanie potencjalnych zagrożeń na podstawie analizy wcześniejszych zdarzeń i wzorców zachowań. Przykładowo, algorytmy SI mogą przewidzieć, które obszary są potencjalnie niebezpieczne w określonych warunkach, co pozwala na wcześniejsze rozmieszczenie tam dodatkowych służb porządkowych.

Ważnym aspektem zastosowania SI w zabezpieczaniu imprez masowych jest analiza danych w czasie rzeczywistym. SI wykrywają i zgłaszają nieprawidłowości, takie jak nagłe zmiany w ruchu tłumu, niebezpieczne zachowania czy pojawienie się podejrzanych obiektów. Dzięki temu służby porządkowe mogą natychmiast reagować na zagrożenia zamiast polegać na opóźnionych raportach lub obserwacjach (Jadhav i in., 2023).

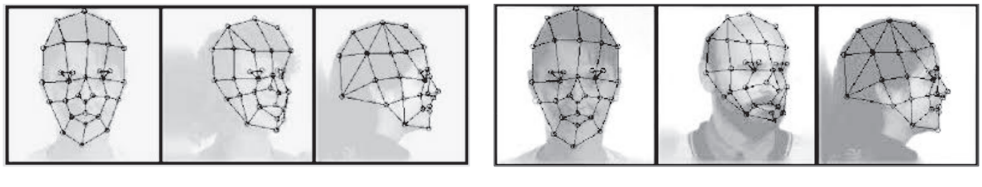
# 3. Technologie SI w praktyce podczas masowych imprez

## 3.1. Rozpoznawanie twarzy

Rozpoznawanie twarzy jest jedną z najbardziej rozwiniętych i szeroko stosowanych technologii sztucznej inteligencji w kontekście bezpieczeństwa publicznego, zwłaszcza podczas masowych imprez. Technologia ta polega na automatycznym identyfikowaniu osób na podstawie ich cech biometrycznych – kształtu twarzy, rozmieszczenia oczu, nosa i ust. W dalszej części artykułu przedstawiono kluczowe technologie i metody stosowane w rozpoznawaniu twarzy.

## 3.2. Rozpoznawanie twarzy w 2D

System rozpoznawania twarzy w przestrzeni dwuwymiarowej (2D) działa na obrazach lub nagraniach wideo z systemów monitoringu, kamer komercyjnych/ prywatnych, CCTV i innych urządzeń codziennego użytku. W celu dokonania kompletnej, automatycznej konfiguracji system musi najpierw wykryć twarz na obrazie/ wideo wejściowym i wyodrębnić ją z wykrytego obszaru. Następnie twarz jest wyrównywana do ustalonej struktury kanonicznej i poddawana obróbce w celu korekty potencjalnych zmian oświetlenia. Z przetworzonego obrazu ekstrahowane są cechy danej jednostki, a następnie przeprowadzane jest rozpoznawanie tożsamości za pomocą odpowiednich metod klasyfikacji. W zależności od użytych metod ekstrakcji i klasyfikacji metody te dzielimy na cztery podklasy: holistyczne, lokalne (geometryczne), oparte na opisach lokalnych tekstur oraz oparte na głębokim uczeniu się (Adjabi i in., 2020). Systemy 2D są stosunkowo proste i tanie, ale ich skuteczność może być ograniczona przez zmiany oświetlenia, kąt widzenia, proces starzenia się i wyrazy twarzy. Mimo tych ograniczeń systemy 2D są powszechnie stosowane ze względu na ich niskie koszty i łatwość implementacji. Jedną z popularnych metod rozpoznawania twarzy opartych na cechach geometrycznych jest metoda dopasowywania grafów elastycznych (*Elastic Bunch Graph Matching* – EBGM), która polega na generowaniu grafu referencyjnego przez nałożenie rzadkiego, elastycznego grafu prostokątnego na obraz obiektu i analizie odpowiedzi banku falek Gabor na każdym węźle grafu (rys. 1). Metoda ta jest rozwinięciem techniki dopasowywania grafów elastycznych (EGM) i pozwala na obsługę różnych zmian w wyglądzie twarzy, takich jak otwarte lub zamknięte usta i oczy.



**Rys. 1.** Przykład wyodrębnienia punktów orientacyjnych przy użyciu EBGM

Źródło: (Adjabi i in., 2020).

### 3.2.1. Rozpoznawanie twarzy w 3D

Chcąc poprawić problemy związane z rozpoznawaniem twarzy w 2D, opracowano systemy rozpoznawania twarzy w trzech wymiarach (3D), mające na celu zapewnienie wysokiego poziomu precyzji oraz większej odporności na zmiany na twarzy spowodowane różnymi czynnikami. Zdolność ta wynika z bardziej zaawansowanych systemów i modeli 3D uwzględniających informacje geometryczne. W przypadku obrazów 2D charakterystyczne punkty na twarzy, takie jak oczy, brwi, usta, mogą być wykrywane bez trudu i stanowią kluczowe elementy służące do identyfikacji. Jednakże w przypadku rozpoznawania twarzy w formacie 3D najważniejszym punktem odniesienia jest nos (Adjabi i in., 2020). Technologie 3D są bardziej odporne na zmiany oświetlenia i kąta widzenia, co zwiększa ich dokładność i niezawodność, są natomiast droższe i trudniejsze do implementacji niż systemy 2D.

### 3.2.2. Algorytmy głębokiego uczenia (*deep learning*) w rozpoznawaniu twarzy

Algorytmy głębokiego uczenia, takie jak sieci neuronowe, znacznie poprawiły dokładność rozpoznawania twarzy. Metody głębokiego uczenia dla modeli 3D stanowią mniej niż 10% ich całości. W teorii są one wydajne, jednakże liczba dostępnych skanów twarzy 3D jest bardzo ograniczona. Przez to modele 3D mogą nie być dokładne, co sprawia, iż większą część rynku stanowią modele 2D. Modele, takie jak FaceNet, VGGFace i DeepID są obecnie standardem w branży rozpoznawania twarzy (Adjabi i in., 2020).

## 3.3. Zarządzanie tłumem

Współczesne wyzwania związane z zapewnieniem bezpieczeństwa podczas masowych imprez i zgromadzeń publicznych wymagają zaawansowanych technologii monitorowania tłumu. Tradycyjne metody (kamery CCTV), choć powszechnie stosowane, okazują się niewystarczające z powodu ograniczeń związanych z pokrywaniem dużych obszarów oraz brakiem elastyczności w perspektywach. Z tego powodu coraz większe zainteresowanie budzą technologie sztucznej inteligencji (AI) oraz bezzałogowe pojazdy latające (UAV), które oferują zaawansowane możliwości monitorowania i analizy tłumu.

### 3.3.1. Monitorowanie tłumu przy użyciu głębokiego uczenia

Jednym z kluczowych osiągnięć w dziedzinie monitorowania tłumu jest wykorzystanie głębokiego uczenia się do wykrywania podejrzanych zachowań. Systemy te mogą poprawić dokładność monitorowania dzięki zastosowaniu sieci w pełni konwolucyjnych (FCN) oraz długoterminowej pamięci krótkotrwałej (LSTM). Główne zalety tych technologii to redukcja fałszywych alarmów, co jest kluczowe w kontekście efektywnego reagowania na zagrożenia. Model FCN + LSTM osiągnął dokładność na poziomie 97,84%, co stanowi poprawę w stosunku do wcześniejszych metod. Wprowadzenie automatycznych systemów monitorowania pozwala na obserwację dużych obszarów bez potrzeby angażowania służb, co jest ważne podczas

masowych imprez. Głębokie uczenie się pozwala na przetwarzanie i analizę obrazów z kamer CCTV, identyfikując zachowania tłumu w czasie rzeczywistym. Takie podejście pozwala na identyfikację potencjalnych zagrożeń, takich jak terroryzm czy zamieszki, co jest kluczowe dla bezpieczeństwa uczestników masowych wydarzeń (Jadhav i in., 2023).

### 3.3.2. Wykorzystanie UAV do monitorowania tłumu

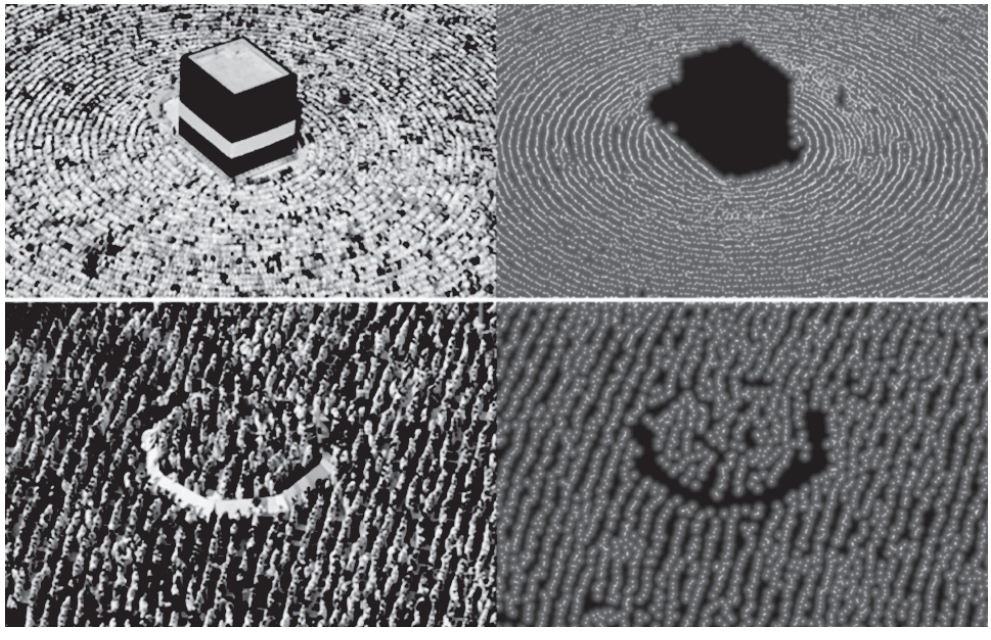
Istotnym elementem nowoczesnych systemów monitorowania tłumu jest zastosowanie bezzałogowych pojazdów latających (UAV). Dzięki mobilności i operowania na wysokościach oferują szereg korzyści. UAV mogą szybko zmieniać pozycję i kąt obserwacji, co pozwala na znacznie lepsze pokrycie dużych obszarów w porównaniu z kamerami CCTV. Dzięki temu możliwe jest monitorowanie dużych przestrzeni, gdzie tradycyjne kamery mogą mieć ograniczone możliwości. Drony mogą być wyposażone w sensory, np. kamery termowizyjne. Są one przydatne w warunkach słabego oświetlenia lub do wykrywania zagrożeń. Umożliwia to monitorowanie tłumów w nocy lub w trudnych warunkach atmosferycznych. Drony mogą być sterowane zdalnie, co pozwala na monitorowanie obszarów trudno dostępnych lub niebezpiecznych. Przykładowo, UAV mogą być używane do patrolowania terenów, np. stadionów, czy zgromadzeń, np. koncertów, gdzie zbierają się grupy ludzi. Zastosowanie Deep CNNs (*Convolutional Neural Networks*) w przetwarzaniu obrazów umożliwia wykrywanie i śledzenie osób oraz analizę wzorców zachowań w tłumie, co zwiększa skuteczność monitorowania. Zarządzanie energią dronów jest ważne dla operacji monitorowania. Proponowane strategie obejmują stacje ładowania, wymianę baterii oraz wykorzystanie technologii hybrydowych. Pozwala to na wydłużenie czasu lotu dronów. Przykładem jest zastosowanie stacji ładowania na mobilnych platformach, które mogą podążać za dronami, zapewniając im źródło energii i długotrwałe operacje monitorowania (Husman i in., 2021).

### 3.3.3. Szacowanie liczebności tłumu

Szacowanie liczebności tłumu jest kluczowym elementem zarządzania tłumem, ponieważ liczebność tłumu może wskazywać na ryzyko wynikające z zachowań uczestników. Jedną z metod jest liczenie osób. Wyzwanie stanowi zróżnicowanie skali obrazów tłumu. Wykorzystanie algorytmów Deep CNNs pozwala na liczenie osób w tłumie, co jest znaczące dla oceny zagrożeń i podejmowania działań prewencyjnych (Husman i in., 2021). Przykład przedstawiony został na rys. 2.

### 3.3.4. Śledzenie tłumu

Śledzenie tłumu jest niezbędne do zrozumienia dynamiki tłumu i identyfikacji zagrożeń. UAV mogą być wykorzystane do ciągłego monitorowania ruchu tłumu, co pozwala na wykrywanie nietypowych aktywności. Algorytmy Deep CNNs odgrywają kluczową rolę w jego śledzeniu, umożliwiając podglądanie ruchu jednostek oraz grup. Takie podejście pozwala na reagowanie na zmiany w dynamice tłumu, co jest kluczowe dla bezpieczeństwa imprez masowych (rys. 3) (Husman i in., 2021).



**Rys. 2.** Przykład szacowania wielkości tłumu przy użyciu Deep CNNs

Źródło: (Husman i in., 2021).

**Rys. 3.** Śledzenie tłumu w przypadku osób naruszających SOP w związku z COVID-19

Źródło: (Husman i in., 2021).

### 3.3.5. Zastosowanie algorytmów AI w monitorowaniu tłumu

W pracach dotyczących głębokiego uczenia się i UAV podkreśla się znaczenie algorytmów AI w analizie zachowań tłumu. Kluczowe technologie i algorytmy obejmują algorytmy detekcji tłumu, które umożliwiają wykrywanie jego obecności oraz śledzenie ruchów w czasie rzeczywistym. Dzięki zastosowaniu technik, takich jak *Region of Interest* (ROI) *Extraction* i *Supervised Machine Learning* (SML), możliwe jest precyzyjne identyfikowanie osób w tłumie. Przykładem może być użycie algorytmów CNNs do analizy obrazów i wykrywania osób na podstawie cech wizualnych. Algorytmy analizy zachowań pozwalają na badanie wzorców zachowań tłumu i identyfikację nietypowych zachowań, które mogą wskazywać na potencjalne zagrożenia, np. obserwacja zmiany prędkości poruszania się ludzi w tłumie może być wskaźnikiem paniki lub zamieszek. Takie algorytmy mogą korzystać z technik LSTM do analizy sekwencji danych i przewidywania przyszłych zachowań na podstawie historii ruchów tłumu. Techniki te są niezwykle praktyczne w zarządzaniu bezpieczeństwem podczas masowych imprez, umożliwiając szybkie i skuteczne reagowanie na wszelkie nieprawidłowości i zagrożenia, a tym samym zapewniając bezpieczeństwo uczestników (Jadhav i in., 2023; Husman i in., 2021).

## 3.4. Wykrywanie przedmiotów przy użyciu sztucznej inteligencji

Wykrywanie przedmiotów jest kluczowym aspektem monitorowania bezpieczeństwa zarówno w przestrzeniach publicznych, jak i na platformach internetowych. Prace Ha i in. (2024) oraz Liu i in. (2021) przedstawiają podejście do wykrywania szkodliwych obiektów z wykorzystaniem osiągnięć w dziedzinie uczenia głębokiego. Stosowane w tym celu technologie mają poprawić precyzję i efektywność wykrywania oraz zapewnić lepszą ochronę prywatności danych.

### 3.4.1. Nowe standardy benchmarkowe

Praca Ha i in. (2024) wprowadza obszerny zbiór danych zawierający ponad 10 000 obrazów podzielonych na sześć kategorii: alkohol, gest obraźliwy, krew, papieros, broń i nóż. Zbiór danych obejmuje zarówno łatwe do wykrycia przypadki, jak i trudniejsze. To czyni go unikalnym w porównaniu do wcześniejszych badań. Uwzględnienie trudnych przypadków jest kluczowe dla rozwijania bardziej odpornych modeli, które mogą działać w różnorodnych warunkach (rys. 4). Dzięki temu nowe standardy benchmarkowe mogą lepiej ocenić zdolności modeli do wykrywania obiektów w realnych scenariuszach. Jest to znaczące dla aplikacji w monitoringu bezpieczeństwa. Wprowadzenie tak różnorodnego zbioru danych pozwala na dokładniejsze testowanie i rozwijanie algorytmów, które mogą radzić sobie z wyzwaniami, jakie napotykają systemy bezpieczeństwa w rzeczywistych warunkach.


**Rys. 4.** Przykładowe obrazy są losowo wybrane z proponowanych zbiorów danych. Pierwszy poziomy rząd przedstawia obrazy z normalnymi przypadkami, a drugi z trudnymi. Kategorie oznaczają odpowiednio: alkohol, obraźliwy gest, krew, papieros, broń i nóż w każdej kolumnie.

Źródło: (Husman i in., 2021).

### 3.4.2. *Federated model training* w detekcji obiektów

*Federated model training* to paradygmat w dziedzinie uczenia maszynowego, który umożliwia trenowanie modeli z rozproszonych zbiorów danych bez konieczności ich centralnego przechowywania. Praca Liu i in. (2021) opisuje platformę FedVision, która wspiera rozwój aplikacji wizyjnych opartych na federacyjnym uczeniu. Umożliwia tworzenie modeli wykrywania obiektów przy jednoczesnym zachowaniu prywatności danych. Platforma FedVision została zaprojektowana, aby umożliwić etykietowanie danych obrazowych. *Federated model training* pozwala na trenowanie modeli bez konieczności przesyłania danych do centralnej jednostki. Znacząco redukuje ryzyko naruszenia prywatności. W ramach FedVision modele są trenowane lokalnie na danych użytkowników, a jedynie parametry modelu są przesyłane do centralnego serwera w celu ich agregacji. Takie podejście umożliwia skuteczne trenowanie modeli. Minimalizuje przy tym ryzyko wycieku danych i zapewnia zgodność z regulacjami dotyczącymi ochrony prywatności (GDPR).

### 3.4.3. Architektura wykrywania przedmiotów i techniki wykrywania

W badaniach Ha i in. (2024) oraz Liu i in. (2021) zastosowano architektury wykrywania obiektów, takie jak Faster R-CNN oraz YOLOv5, wybrane ze względu na ich skuteczność w różnych scenariuszach wykrywania. Faster R-CNN jest znane z precyzji i dokładności w wykrywaniu. YOLOv5 z kolei jest cenione za szybkość i wydajność w czasie rzeczywistym. W platformie FedVision zastosowano federacyjny wariant YOLOv3, który umożliwia kolaboracyjne trenowanie modeli z danych lokalnie przechowywanych u wielu użytkowników. Wykorzystanie głębokich konwolucyjnych sieci neuronowych (*Deep* CNNs) do ekstrakcji cech semantycznych na wysokim poziomie pozwala na precyzyjne wykrywanie obiektów w różnych warunkach. *Deep* CNNs są w stanie rozpoznawać i klasyfikować szkodliwe obiekty nawet w trudnych

przypadkach, np. gdy cechy obiektów są częściowo zasłonięte lub niewyraźne. Techniki te, zintegrowane z systemami federacyjnymi, pozwalają na dynamiczne uczenie się modeli. Adaptują się do nowych danych bez potrzeby centralizowania informacji, co jest kluczowe dla zachowania prywatności i efektywności operacyjnej.

Oba rozwiązania zostały zaprojektowane z myślą o zastosowaniach w czasie rzeczywistym, co jest szczególnie istotne w kontekście monitoringu. Modele YOLOv5 i Faster R-CNN, dzięki swojej architekturze, mogą przetwarzać obrazy w czasie rzeczywistym. Pozwala to na natychmiastową reakcję na zagrożenia. Platforma FedVision, wykorzystując *federated model training,* umożliwia ciągłe aktualizowanie modeli na podstawie nowych danych, co zapewnia ich wysoką skuteczność i adaptacyjność w dynamicznie zmieniających się warunkach. Dzięki temu możliwe jest monitorowanie w czasie rzeczywistym. W praktyce oznacza to, że systemy te mogą natychmiast wykrywać i klasyfikować potencjalnie zagrożenia, np. broń czy materiały wybuchowe. Mogą również reagować na zmiany w otoczeniu, co zwiększa ich użyteczność i skuteczność w operacyjnych zastosowaniach monitoringu.

## 4. Zalety sztucznej inteligencji w monitoringu i możliwe wyzwania

Sztuczna inteligencja przynosi liczne korzyści w zarządzaniu bezpieczeństwem podczas masowych imprez, a jedną z najważniejszych jej zalet jest możliwość reakcji na zagrożenia dzięki analizie danych w czasie rzeczywistym. Zaawansowane algorytmy SI, takie jak głębokie uczenie (*deep learning*), pozwalają systemom na wykrywanie i klasyfikowanie niebezpiecznych sytuacji i umożliwiają błyskawiczne podjęcie działań. Algorytmy *deep learning* mogą przetwarzać obrazy z kamer CCTV, identyfikując zagrożenia i informując służby. Ponadto systemy SI cechują się dokładnością w identyfikacji zagrożeń. Jest to możliwe dzięki zdolności do analizy ogromnej liczby danych i wykrywania wzorców niewidocznych dla ludzkiego oka. Technologia rozpoznawania twarzy może skutecznie identyfikować osoby z list poszukiwanych, a analiza wzorców ruchu tłumu pozwala na przewidywanie obszarów o ryzyku przeludnienia.

SI wspiera również służby porządkowe poprzez automatyzację monitoringu i dostarczanie im precyzyjnych, aktualnych informacji o sytuacji na terenie imprezy. Dzięki SI możliwe jest nie tylko monitorowanie zachowań tłumu, ale także prognozowanie potencjalnych zagrożeń na podstawie analizy wcześniejszych zdarzeń. Przykładem może być wykorzystanie dronów wyposażonych w kamery do monitorowania terenu z powietrza, co zwiększa skuteczność nadzoru.

Jednak implementacja technologii SI wiąże się również z pewnymi wyzwaniami. Jednym z głównych problemów jest ochrona prywatności uczestników. Technologia zwiazana z rozpoznawaniem twarzy budzi obawy związane z inwazyjnością i nadużyciem danych osobowych. Wymaga to wprowadzenia odpowiednich regulacji prawnych i procedur zabezpieczających prywatność, np. ograniczenia dostępu

do informacji osobowych. Mimo wysokiej dokładności systemy SI nie są wolne od błędów. Zdarzają się przypadki błędnej identyfikacji, które mogą prowadzić do fałszywych alarmów lub niesłusznego oskarżenia niewinnych osób. Takie błędy mogą wynikać z niedoskonałości algorytmów, złej jakości danych wejściowych lub niewłaściwej konfiguracji systemów. Dlatego kluczowe jest ciągłe doskonalenie technologii oraz regularne szkolenie personelu w celu minimalizacji błędów. Dodatkowo, implementacja zaawansowanych technologii SI wiąże się z wysokimi kosztami zarówno związanymi z zakupem sprzętu i oprogramowania, jak i z ich utrzymaniem oraz aktualizacją. Koszty te mogą być barierą dla wielu organizatorów imprez masowych. Konieczność zatrudnienia wykwalifikowanego personelu do obsługi systemów SI również zwiększa koszty.

## 5. Podsumowanie

Sztuczna inteligencja (SI) stanowi przełomowe narzędzie w zarządzaniu bezpieczeństwem podczas imprez masowych. Dzięki algorytmom *deep learning* SI umożliwia wykrywanie i reagowanie na niebezpieczne sytuacje, co pozwala na natychmiastowe podjęcie działań zapobiegawczych. Rozpoznawanie twarzy oraz analiza ruchu tłumu wyróżniają się jako najskuteczniejsze technologie SI, służące do przewidywania zagrożeń. Rozpoznawanie twarzy, oparte na algorytmach głębokiego uczenia, nie tylko umożliwia identyfikowanie osób poszukiwanych, ale także pozwala dostrzec potencjalne niebezpieczeństwo na podstawie analizy wzorców tłumu. Oznacza to, że służby mogą reagować z większą precyzją i efektywnością, co przekłada się na ograniczenie ryzyka wystąpienia zagrożeń w trakcie organizacji imprez masowych.

Z SI wiążą się również z wyzwania. Ochrona prywatności uczestników jest kluczowa. Technologie związane z rozpoznawaniem twarzy budzą obawy dotyczące potencjalnego nadużycia danych osobowych. Ponadto systemy SI nie są wolne od błędów identyfikacyjnych, a co za tym idzie, mogą prowadzić do fałszywych alarmów. Istotne jest również wykrywanie niebezpiecznych przedmiotów, jak broń palna czy nóż, dlatego stale doskonali się technologię oraz regularnie szkoli personel. Oprócz tego koszty związane z zakupem, utrzymaniem i aktualizacją technologii SI mogą być barierą dla wielu organizatorów imprez.

Największą zaletą wykorzystania wymienionych technologii jest zdolność do prognozowania zagrożeń, jak zamieszki czy terroryzm. Dzięki analizie wzorców ruchu tłumu oraz identyfikacji osób potencjalnie niebezpiecznych możliwe jest podjęcie działań prewencyjnych, zanim zagrożenie eskaluje. Algorytmy analizy zachowań i drony monitorujące przestrzeń z powietrza zwiększają efektywność działania służb porządkowych, pozwalając im na bardziej precyzyjne działania prewencyjne.

W przyszłości rozwój i doskonalenie technologii SI będą miały duży wpływ na lepsze zarządzanie bezpieczeństwem podczas masowych wydarzeń. Badania nad algorytmami, poprawa istniejących systemów oraz opracowanie bardziej efektyw-

nych metod ochrony prywatności uczestników będą miały istotne znaczenie. Integracja SI z innymi technologiami, takimi jak Internet Rzeczy (IoT) czy *blockchain*, może dodatkowo poprawić skuteczność systemów monitoringu. Rozważne podejście do implementacji tych technologii, obejmujące odpowiednie regulacje prawne i procedury, jest kluczowe dla maksymalizacji korzyści i minimalizacji ryzyka zwłaszcza w kontekście zapobiegania zamieszkom, terroryzmowi i wykrywaniu niebezpiecznych przedmiotów.

## Literatura


Adjabi, I., Ouahabi, A., Benzaoui, A., i Taleb-Ahmed, A. (2020). Past, Present, and Future of Face Recognition: A Review. *Electronics*, *9*(8), 1188. https://doi.org/10.3390/electronics9081188

Bonnasse-Gahot, L., i in. (2018). Epidemiological Modelling of the 2005 French Riots: A Spreading Wave and the Role of Contagion. *Scientific Reports*, *8*(1). https://doi.org/10.1038/s41598-017-18093-4

Choi, W. (2020). A Study on the Intelligent Disaster Management System Based on Artificial Intelligence. *Journal of the Korean Society of Hazard Mitigation*, *20*(1), 127-140. https://doi.org/10.9798/kosham.2020.20.1.127

Chollet, F. (2019). *On the Measure of Intelligence*. https://doi.org/10.48550/arxiv.1911.01547

Deng, H., Feng, Z., Qian, G., Lv, X., Li, H., i Li, G. (2021). Mfcosface: A Masked-Face Recognition Algorithm Based on Large Margin Cosine Loss. *Applied Sciences*, *11*(16), 7310. https://doi.org/10.3390/app11167310

Gassebner, M., i Luechinger, S. (2011). Lock, Stock, and Barrel: A Comprehensive Assessment of the Determinants of Terror. *Public Choice*, *149*(3-4), 235-261. https://doi.org/10.1007/s11127-011-9873-0

Gupta, C., Johri, I., Srinivasan, K., Hu, Y., Qaisar, S., i Huang, K. (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks. *Sensors*, *22*(5), 2017. https://doi.org/10.3390/s22052017

Ha, E., Kim, H., i Na, D. (2024). HOD: New Harmful Object Detection Benchmarks for Robust Surveillance. In: *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 183-192. https://doi.org/10.48550/arXiv.2310.05192

Husman, M. A., i in. (2021). Unmanned Aerial Vehicles for Crowd Monitoring and Analysis. *Electronics*, *10*(23), 2974. https://doi.org/10.3390/electronics10232974

Jadhav, C., Ramteke, R., i Somkunwar, R. K. (2023). Smart Crowd Monitoring and Suspicious Behavior Detection Using Deep Learning. *Revue d'Intelligence Artificielle*, *37*(4), 955-962. https://doi.org/10.18280/ria.370416

Liu, Y., i in. (2021). Federated Learning-Powered Visual Object Detection for Safety Monitoring. *AI Magazine*, *42*(2), 19-27. https://doi.org/10.1609/aimag.v42i2.15095

Tyagi, B., Nigam, S., i Singh, R. (2022). A Review of Deep Learning Techniques for Crowd Behavior Analysis. *Arch Computat Methods Eng*, (29), 5427–5455. https://doi.org/10.1007/s11831-022-09772-1

## Artificial Intelligence in Managing Security of Mass Events: Identification of Potential Threats Such as Terrorism and Riots

**Abstract:** The article discusses the application of artificial intelligence (AI) in managing the safety of mass events. Security at such events is crucial due to the risks of riots or terrorism. AI can support law enforcement by analysing real-time data and predicting potential threats. Technologies such as facial recognition, crowd management, and the detection of dangerous objects are presented.

**Keywords:** artificial intelligence, mass events, facial recognition, object detection, crowd management