KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Techniki deepfake [S1Cybez1>TD]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
12

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Tomasz Grajek
tomasz.grajek@put.poznan.pl

mgr inż. Błażej Szydełko
blazej.szydelko@put.poznan.pl

Wykładowcy

Wymagania wstępne

Podstawowa znajomość algorytmów uczenia maszynowego oraz technik głębokiego uczenia. Umiejętność programowania w języku Python. Podstawowa wiedza z zakresu przetwarzania obrazu i dźwięku.

Cel przedmiotu

Celem przedmiotu jest zaznajomienie studentów z technikami tworzenia i detekcji treści multimedialnych generowanych za pomocą sztucznej inteligencji, tzw. deepfake'ów. Studenci poznają algorytmy generowania i analizy deepfake'ów, zdobędą praktyczne umiejętności w zakresie tworzenia oraz detekcji syntetycznych treści, a także zgłębią aspekty prawne i etyczne związane z wykorzystaniem tych technik.

Przedmiotowe efekty uczenia się

Wiedza:
Student posiada zaawansowaną wiedzę na temat zasad tworzenia i wykorzystania algorytmów komputerowych oraz struktur języków programowania w kontekście generowania i detekcji

deepfake'ów. Zna podstawy inżynierii oprogramowania, które pozwalają na implementację narzędzi do przetwarzania multimediów. K1_W06
Student zna podstawowe zasady działania systemów maszynowego uczenia się i sztucznych sieci neuronowych, takich jak autoenkodery, GAN oraz StyleGAN, a także metody optymalizacji i podejmowania decyzji wykorzystywane w algorytmach generatywnych. K1_W16
Rozumie współczesne zagrożenia związane z masowym wykorzystaniem technologii deepfake, w szczególności w kontekście bezpieczeństwa cyfrowego i społeczeństwa informacyjnego, oraz orientuje się w najnowszych trendach związanych z wykorzystaniem sztucznej inteligencji w tej dziedzinie. K1_W20
Posiada podstawową wiedzę w zakresie prawa autorskiego, ochrony danych osobowych oraz własności intelektualnej, w szczególności w kontekście generowania i wykorzystania syntetycznych treści multimedialnych. K1_W21

Umiejętności:
Student potrafi korzystać z literatury naukowej i dokumentacji technicznej dotyczącej technologii deepfake, integrować i oceniać informacje oraz wyciągać wnioski w celu rozwiązywania problemów związanych z tworzeniem i detekcją syntetycznych treści. K1_U01, K1_U02, K1_U11
Dostrzega systemowe i pozatechniczne aspekty deepfake'ów, w tym etyczne, prawne i społeczne, szczególnie w kontekście cyberbezpieczeństwa. K1_U07, K1_U08
Dokonuje krytycznej analizy i oceny narzędzi stosowanych w tworzeniu i wykrywaniu deepfake'ów, wykorzystując odpowiednie metody analityczne. K1_U09

Kompetencje społeczne:
Student rozumie znaczenie wiedzy w rozwiązywaniu problemów związanych z tworzeniem i detekcją deepfake'ów, jest świadomy konieczności korzystania z ekspertyzy specjalistów, gdy zadanie wykracza poza jego kompetencje. K1_K02
Potrafi formułować i przekazywać społeczeństwu informacje na temat pozytywnych i negatywnych aspektów technologii deepfake, uwzględniając interes publiczny. K1_K03
Ma świadomość odpowiedzialności za wykonywaną pracę, przestrzega zasad etyki zawodowej, jest gotowy do pracy w zespole i ponoszenia odpowiedzialności za wspólne zadania. K1_K05

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wykład: egzamin pisemny lub ustny, pytania o charakterze otwartym, z oczekiwaną odpowiedzią opisową.
Laboratorium: ocena samodzielnie wykonywanych zadań w czasie semetru oraz projekt końcowy.
Skala ocen: <50% - 2,0 (ndst); 50% do 59% - 3,0 (dst); 60% do 69% - 3,5 (dst+) ; 70% do 79% - 4,0 (db); 80% do 89% - 4,5 (db+); 90% do 100% - 5,0 (bdb).
Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Treści programowe obejmują wprowadzenie do technologii deepfake, omówienie algorytmów sztucznej inteligencji takich jak autoenkodery, GAN i StyleGAN oraz technik generowania i detekcji treści multimedialnych, w tym analizy niespójności, widmowej, behawioralnej, biometrycznej i czasowej. Przedstawione są również przykłady algorytmów detekcji, takich jak XceptionNet czy MesoNet, oraz praktyczne zastosowania deepfake'ów w różnych obszarach, z uwzględnieniem aspektów prawnych i etycznych.

Tematyka zajęć

1. Wprowadzenie: czym jest deepfake, przykłady zastosowań.
2. Algorytmy głębokiego uczenia w generowaniu deepfake.
3. Przegląd technik technik detekcji deepfake. Wykrywanie ingerencji w treść multimedialną.
4. Analiza przypadków: deepfake w mediach, multimediach, cyberbezpieczeństwie.
5. Dyskusja: prawne i etyczne aspekty technik deepfake.

Metody dydaktyczne

Wykład online wspierany prezentacjami. Aktywna praca w laboratorium, w tym szczególnie przeprowadzanie eksperymentów i pomiarów. Studia literaturowe.

Literatura

Podstawowa:
1. GANs in Action: Deep learning with Generative Adversarial Networks, J. Langr, V. Bok, 2019
2. Deep Learning, I. Goodfellow, 2016
3. Exploring deepfakes, B. Lyon, M. Tora, 2023

Uzupełniająca:
1. Deep learning with Python, F. Chollet, 2017
2. FAIK, P. Carpenter, 2024

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	103	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	58	2,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	45	1,50