COURSE DESCRIPTION CARD - SYLLABUS

Course name
Deepfake techniques [S1Cybez1>TD]

Course

Field of study Cybersecurity	Year/Semester 3/6
Area of study (specialization) –	Profile of study general academic
Level of study first-cycle	Course offered in Polish
Form of study full-time	Requirements elective

Number of hours

Lecture 16	Laboratory classes 30	Other 0
Tutorials 0	Projects/seminars 12	

Number of credit points

4,00

Coordinators

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

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

Lecturers

Prerequisites

Basic knowledge of machine learning algorithms and deep learning techniques. Ability to program in Python. Basic knowledge of image and sound processing.

Course objective

The aim of the course is to familiarize students with techniques for creating and detecting multimedia content generated using artificial intelligence, known as deepfakes. Students will learn algorithms for generating and analyzing deepfakes, acquire practical skills in creating and detecting synthetic content, and explore the legal and ethical aspects related to the use of these techniques.

Course-related learning outcomes

Knowledge:
The student has advanced knowledge of the principles of creating and using computer algorithms and programming language structures in the context of generating and detecting deepfakes. They are

familiar with the basics of software engineering, which enables the implementation of multimedia processing tools (K1_W004).
The student knows the fundamental principles of machine learning systems and artificial neural networks, such as autoencoders, GANs, and StyleGAN, as well as optimization methods and decision-making techniques used in generative algorithms (K1_W014).
The student understands the modern threats associated with the mass use of deepfake technology, particularly in the context of digital security and the information society, and is aware of the latest trends related to the use of artificial intelligence in this field (K1_W019).
The student has basic knowledge of copyright law, data protection, and intellectual property, particularly in the context of generating and using synthetic multimedia content (K1_W021).

Skills:
The student is able to apply knowledge and skills related to the creation and detection of synthetic content, using appropriate methods and tools for deepfake generation and detection (K1_U01, K1_U02, K1_U11).
They recognize the system-related and non-technical aspects of deepfakes, including ethical, legal, and social issues, particularly in the context of cybersecurity (K1_U07, K1_U08).
The student is capable of conducting a critical analysis and evaluation of tools used in the creation and detection of deepfakes, utilizing appropriate analytical methods (K1_U09).

Social competences:
The student understands the importance of knowledge in solving problems related to the creation and detection of deepfakes and is aware of the need to consult experts when the task exceeds their own competencies (K1_K02).
They are able to formulate and communicate to the public the positive and negative aspects of deepfake technology, considering the public interest (K1_K03).
The student is aware of the responsibility for their work, adheres to professional ethics, and is ready to work in a team and take responsibility for joint tasks, ensuring the quality of their work. (K1_K05).

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: written or oral examination, open questions with an expected descriptive answer.
Laboratory: assessment of self-performed tasks during the semester and final project.
Grading scale: <50% - 2.0 (ndst); 50% to 59% - 3.0 (dst); 60% to 69% - 3.5 (dst+) ; 70% to 79% - 4.0 (db); 80% to 89% - 4.5 (db+); 90% to 100% - 5.0 (bdb).
The course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university’s electronic systems and during the first class meeting (in each form of classes).

Programme content

The course content includes an introduction to deepfake technology, discussion of artificial intelligence algorithms such as autoencoders, GANs, and StyleGAN, as well as techniques for generating and detecting multimedia content, including inconsistency analysis, spectral, behavioral, biometric, and temporal analysis. It also covers examples of detection algorithms like XceptionNet and MesoNet, as well as practical applications of deepfakes in various fields, taking into account legal and ethical aspects.

Course topics

1. Introduction: What is deepfake, examples of applications.
2. Deep learning algorithms in generating deepfakes.
3. Overview of deepfake detection techniques. Detecting content manipulation in multimedia.
4. Case studies: Deepfakes in media, multimedia, and cybersecurity.
5. Discussion: Legal and ethical aspects of deepfake techniques.

Teaching methods

Lecture online supported by presentations. Active work in the laboratory including, in particular, performing experiments and measurements. Literature review.

Bibliography

Basic:
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

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

Breakdown of average student's workload

	Hours	ECTS
Total workload	103	4,00
Classes requiring direct contact with the teacher	58	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	45	1,50