BIOSINF

Multimedia Technologies in Biometrics and Information Security Applications

– Syllabus –

Biometric Technologies. Speech and Biological Signals Analysis (1st sem.)

Dragoș Burileanu, Șerban Mihalache, Ana Neacșu

The subject teaches the fundamentals of biometric technologies and the analysis of speech and biological signals.

The first part of the lectures covers biometric technologies, offering an understanding of their role and operation in realistic scenarios, as well as how to apply the gained knowledge in testing and evaluating various parameter-based solutions with specific requirements. Additionally, the main similarities and differences between the fields of biometric technologies and forensic expertise are also studied, with a deeper look into speaker recognition. The second part focuses on the analysis and processing of speech signals (physical modeling, acoustic-level and phonetic-level characterizations, representation in the time and frequency domains) and of electromyography (EMG) and electroencephalography (EEG) signals, being accompanied by a review of the most important features used in automated solutions to classification tasks.

The first half of the lab familiarizes students with software tools employed for extracting speech features, as well as manually implementing speech feature extraction algorithms. In the second half, using specialized hardware equipment for acquisition, specific feature extraction algorithms for EMG signals are studied and implemented. The programming language for the labs is Python.

Artificial Intelligence I: Classical Machine Learning Systems (1st sem.)

Șerban Mihalache

The subject provides a detailed perspective on classical machine learning models: the *K*-means Model (KMM), the *K*-nearest Neighbors algorithm (KNN), Gaussian Mixture Models (GMM), linear and logistic regression, Decision Trees (DT), Random Forests (RF), Support Vector Machines (SVM), Hidden Markov Models (HMM), and fundamental artificial neural networks, specifically Fully-connected Neural Networks (FCNN).

The lectures cover an introduction into the domain's specific concepts and challenges and tackles the 3 fundamental learning paradigms (supervised learning, unsupervised learning, and reinforcement learning), with a comparative analysis between them and of the types of applications native to each. The most important machine learning techniques and methods are presented in detail, with study cases for clustering, classification, and regression tasks (KMM, KNN, GMM, linear and logistic regression, DT, RF, SVM, and FCNN).

The lab covers the practical implementation of the machine learning models studied in the lectures, using the Python programming language and essential packages employed in the machine learning field (*numpy*, *scipy*, *pandas*, *matplotlib*, *scikit-learn*, *Keras*/*TensorFlow* etc.), with study cases for diverse clustering, classification and regression applications.

Digital Video Analysis and Processing (1st sem.)

Radu-Ovidiu Preda, Claudia-Cristina Oprea

The subject familiarizes students with the main approaches, techniques and theories concerning the analysis and digital processing of video signals. The implications of solving practical tasks in fields using image and video data are presented. The main specific basic concepts and principles covered are: multidimensional signal transforms; 3D analog and digital signals, video formats; perceptual quality estimation for images and video signals; spatial segmentation of images and video frames; analysis and estimation of two-dimensional movement; video compression, the H.264 and H.265 video compression standards; object detection and tracking in video sequences; multimedia content distribution; adaptive video streaming; content distribution networks.

Forensic Expertise Methodology (1st sem.)

Constantin Mirea

The lectures present the most often solicited types of forensic expertise. Within this context, the methods for identifying people and objects with an assumed link to unlawful conduct, using cutting-edge technology, are studied. They also cover the roadmap for long-term higher education graduates to specialize in the field of forensics (to become forensic experts), taking into account that, in Romania, so far there is no specific educational form to award the aforementioned title. Additionally, practical activities are included, using dedicated hardware tools, for various types of forensic analyses, taking place both in the classroom as well as within the laboratories of the National Institute for Forensic Expertise, part of the Ministry of Justice.

Research and Documentation Project S1 (1st sem.)

Dragoș Burileanu, Șerban Mihalache

The project aims to familiarize students with the documentation and discovery stages involved in research and the writing of a scientific review article. The most important bibliographical resources are presented, as well as rules and suggestions for developing a state-of-the-art for a specific research area and for writing a scientific article giving a detailed and complete overview of the chosen topic. The project milestones include choosing a research topic relevant to the machine learning field, acquiring and studying an appropriate list of references, developing a rigorous and detailed state-of-the-art, writing a short scientific review article, and giving an oral presentation on the topic.

Artificial Intelligence II: Deep Neural Networks (2nd sem.)

Ana Neacșu, Horia Cucu

The subject offers a detailed overview of the deep learning field using advanced neural networks: fully-connected neural networks with multiple hidden layers (Multilayer Perceptrons – MLP), convolutional neural networks (CNN), recurrent neural networks (RNN).
The concepts and ideas covered by the lectures mainly focus on developing an intuition for the underlying training mechanisms and applications of deep neural networks, at the same time following a rigorous mathematical modeling of the training process and of the studied models. The most important types of deep neural networks employed for classification and regression problems (MLP, CNN, RNN) are presented, as well as different learning strategies to improve the performance of these systems.
The lab debuts with a detailed introduction to the Git platform and of computation resource management tools: virtual environments (*venv*), *slurm*. The subsequent lessons cover the

practical implementation of the deep neural network models studied in the lectures, using the TensorFlow and PyTorch libraries, and applying them to specific audio and image classification and regression tasks.
The project consists of developing, training, and validating an artificial intelligence system based on deep neural networks for different multimedia applications.

Personal Computer and Mobile Terminal Security (2nd sem.)

Octavian Fratu, Răzvan Crăciunescu

The subject aims to discuss the basic principles and the main technologies used in securing personal computers and mobile terminals, security management of fixed and/or mobile personal computers running standard operating systems (Windows, Linux, etc.), security services for protecting personal computers and mobile terminals: definitions, techniques and mechanisms, the study of software tools used for recovering data destroyed in information attacks or deleted by users, methods employed in investigations concerning cybercriminality.
The lab covers developing practical abilities to detect and remove malware programs.

Voice Communication Interfaces with Intelligent Systems (2nd sem.)

Dragoș Burileanu, Horia Cucu

The first part of the lectures aims to offer students basic knowledge on the principles and paradigms of human-computer interaction, as well as advanced theoretical and practical knowledge concerning voice communication interfaces with various intelligent systems. Additionally, skills in developing and evaluating advanced dialog systems are introduced, together with the concept of multimodality in developing modern interactive interfaces.
The second part of the lectures aims to familiarize students with automatic speech recognition (the process through which speech is transcribed into text), as a first step required in voice communication with an intelligent system, including deep neural network architectures used successfully to extract characteristics (embeddings) and for transcription. Additionally, the resources required for training and adapting a speech transcription system, as well as post-processing techniques for the resulting text, are presented.
The lab covers the development of a vocal chat-bot system. The implementation is done using the Python programming language and is based on an existing automatic speech transcription and synthesis system.

Artificial Intelligence Applied in Speech Forensics (2nd sem.)

Șerban Mihalache

The subject offers a theoretical and practical perspective on employing artificial intelligence systems for speech forensics applications.
The lectures will first provide an introduction into speech forensics and present the main tasks associated with the field, as well as opportunities and challenges encountered in using artificial intelligence systems for their automatization. In the second part, applications based on the recognition of paralinguistic speech content are studied, including emotion recognition, stress detection and lie detection. Additionally, the lectures discuss the key principles and challenges in developing datasets specific for these tasks.
The project consists of developing, training, and validating an artificial intelligence system based on deep neural networks for automatic lie detection from speech.

Research Project in Speech Technology (2nd sem.)

Horia Cucu

The research project aims to familiarize students with the concept of speaker recognition. Different working scenarios are presented (for example, identification vs. verification, closed sets of speakers vs. open sets) and one of them is chosen for practical study. Students use publicly available Romanian and multilingual datasets, and modern neural network architectures. The project ensures students are well-trained in formulating experimental hypotheses and methodologies, and reporting scientific results.

Artificial Intelligence III: Advanced Techniques for Developing Machine Learning Systems (3rd sem.)

Ana Neacșu, Horia Cucu, Jean-Christophe Pesquet

The subject extends the knowledge gained in the "Artificial Intelligence I: Classical Machine Learning Systems" and "Artificial Intelligence II: Deep Neural Networks" courses, presenting the most recent and high performing artificial intelligence systems and techniques.
The first part of the lectures details advanced optimization algorithms, regularization and dynamic normalization techniques for data during the training process, as well as advanced learning strategies (transfer learning, joint learning, attention mechanisms). In the second part, the lectures cover complex neural network architectures including generative-adversarial networks (GAN), auto-encoders and variational auto-encoders, and transformers. The final part comprises concepts and techniques for evaluating and improving the robustness of neural network-based systems against adversarial attacks.
The project consists of implementing and training a deep neural network-based system, testing different simple and advanced architectures.

Security in Computer Networks (3rd sem.)

Dragoș Drăghicescu, Alexandru Caranica

The subject's main goal is to provide theoretical and practical knowledge in cybersecurity, one of the fields in the information technology and computing industry with the highest growth.
In the lectures, students will gain essential knowledge required in the secure design and employment of information systems, as well as to protect digital information within institutions and companies from a procedural standpoint. Additionally, the lectures allow students to gain expertise in investigating incidents concerning the cybersecurity of computer networks and IoT devices, and applying standards, models, and best practices to solve and preempt security issues in computer networks. The lectures also provide basic concepts regarding the development of security policies, necessary for preventing risks and threats on digital infrastructures.
The lab covers the following subjects: Linux administration and operating system security; working with networking software and automating their usage by means of Bash scripting; exercising general networking knowledge (general security principles, the study and usage of IPsec protocols, etc.); secure coding standards and principles (applied to the Python and C languages); exploiting application vulnerabilities; principles of data integrity, confidentiality, and authentication.

Audio-Video Forensics (3rd sem.)

Gheorghe Pop

The lectures' main objective is to provide deep theoretical and practical knowledge in the following areas: methods and techniques for falsifying / manipulating audio-video signals, preprocessing and advanced analysis techniques of these signals for forensic investigation, advanced techniques for detecting traces of digital editing in audio-video recordings (compressed and uncompressed), detection and identification of speakers or people shown in images, and authenticating recordings.
The lab applications' goal is the experimental validation of the theoretical concepts presented in the lectures, developing skills in configuring editing tools for multimedia recordings, as well as experimentally detecting traces of recording manipulation.

Artificial Intelligence for Embedded Systems (3rd sem.)

Georgian Nicolae

The subject offers a theoretical and practical perspective on developing and implementing artificial intelligence models for embedded systems (reduced computational power, reduced data resolution) and their real-time operation.
The first part of the lectures presents the main challenges and limitations encountered in the context of resource-constrained systems, alongside techniques for adapting and optimizing neural networks (weight quantization, model complexity reduction, computational optimization) for real-time operation in embedded systems. The second part presents principles and development methodologies for artificial intelligence models for specific multimedia applications, in the context of resource-constrained systems: multimodal data usage, robotic systems, functional safety aspects.
The lab debuts with an introduction of the development environment and the NVIDIA Jetson Nano development kit, as well as how to configure them. The subsequent lessons cover neural network adaptation and optimization techniques to ensure real-time operation in embedded systems.
The project consists of developing, training, and validating an artificial intelligence model based on neural networks for a multimedia application, followed by adapting and implementing the model on a resource-constrained system (NVIDIA Jetson Nano).

Integrated Research Project in Computer Security (3rd sem.)

Dragoș Drăghicescu

The research project's main goal is to integrate the knowledge gained in the computer security courses, emphasizing the practical side of the field. The project involves students in choosing from a list of proposed assignments, each requiring them to solve a complex security task using the Linux operating system, Bash scripting, as well as originally developed code (for example, implementing a vulnerable software and testing it in a secure environment). The project allows students to gain a deeper understanding of the learned security principles in a highly applied manner.