Biometrics and Artificial Intelligence: Security and Modern Challenges

IMPK Program

Faculty of Computer Science, Bialystok University of Technology

1. Introduction

The rapid development of artificial intelligence, machine learning, and modern sensing technologies has transformed the way identity, security, and digital trust are managed across the world. Biometrics has become a core component of authentication systems, border control, financial services, healthcare, and everyday consumer electronics. This program provides an integrated, practice-oriented introduction to both biometric systems and the AI methods that power them.

"Biometrics and Artificial Intelligence: Security and Modern Challenges" is designed for international students seeking a solid understanding of how biometric data is acquired, processed, and analyzed using classical algorithms and modern deep learning approaches. The program combines theoretical lectures with intensive workshops, giving students the opportunity to work with real biometric images, machine-learning models, and practical tools such as Python, NumPy, scikit-learn, OpenCV, TensorFlow/Keras, and PyTorch.

Students completing the program will acquire both the foundational knowledge and hands-on experience required to understand, implement, and critically evaluate biometric recognition systems and AI-based identity technologies.

2. Program Structure

The program consists of 3 complementary subjects, each focusing on a key layer of expertise:

1. Fundamentals of Biometric Systems (PSB)
2. Fundamentals of Artificial Intelligence (PSI)
3. Artificial Intelligence in Biometrics (SIwB)

Together they form a coherent learning path beginning with basic concepts, progressing through core AI techniques, and culminating in the application of classical and deep-learning methods in biometric pipelines.

3. Subject Overviews

3.1 Fundamentals of Biometric Systems (PSB)

This module introduces the essential principles of biometric identification and verification. Students explore the main physiological and behavioral biometric modalities, such as fingerprints, face, iris, voice, and signature, along with system architectures, error types, and security considerations.

Lectures cover the full biometric pipeline: from image acquisition and preprocessing, through feature extraction and template creation, to classification, matching, and evaluation of error metrics such as FAR and FRR. The course also presents real-world applications, ranging from personal authentication to large-scale surveillance systems.

Workshops develop practical skills using Python and OpenCV. Students load and preprocess fingerprint images, perform thinning and skeletonization, extract simple minutiae, and implement a minimal matching algorithm. The hands-on project integrates acquisition, enhancement, minutiae extraction, and matching into a small working biometric pipeline.

3.2 Fundamentals of Artificial Intelligence (PSI)

This course provides the AI foundation necessary for later work with biometric data. Students learn the core concepts of artificial intelligence and machine learning, including supervised and unsupervised learning, regression, classification, neural networks, and evaluation metrics.

Lectures introduce classical AI ideas, expert systems, the evolution of machine learning, and modern approaches to predictive modeling. Students study linear and logistic regression, decision trees, k-NN methods, simple neural network models, and basic deep-learning concepts.

Workshops use Python, NumPy, matplotlib, and scikit-learn. Students practice data preprocessing, visualization, feature scaling, model training, and evaluation. They build regression models, binary classifiers, decision trees, and small ML pipelines, learning how to validate results through accuracy, precision, recall, and confusion matrices.

3.3 Artificial Intelligence in Biometrics (SIwB)

This advanced module integrates biometrics with AI-driven approaches, image processing, feature extraction, classical ML models, and deep-learning methods for biometric recognition.

Lectures begin with the role of AI in biometric systems and proceed through topics such as HOG/LBP descriptors, SVM and Random Forest classifiers, CNN fundamentals, face embeddings, fingerprint recognition approaches, liveness detection, surveillance and person re-identification, dataset challenges, and security/privacy considerations including spoofing and deepfakes.

Workshops cover a broad range of practical skills: preprocessing biometric images, extracting features using HOG/LBP, training SVM and Random Forest models, implementing basic neural networks in TensorFlow/Keras or PyTorch, performing data augmentation, building embeddings using pretrained CNNs, and conducting

similarity-based matching using cosine distance. Students also generate ROC/DET curves and evaluate models using FAR, FRR, and EER.

4. Skills and Learning Outcomes

Across all three subjects, students will:

- Understand biometric modalities, acquisition methods, and the identification and verification pipeline
- Learn preprocessing techniques for biometric images (normalization, enhancement, thinning, segmentation)
- Apply feature extraction methods (minutiae, geometric, texture-based descriptors such as HOG/LBP)
- Train classical ML models (logistic regression, k-NN, SVM, Random Forest)
- Implement neural network models, including simple CNNs for biometric data
- Evaluate biometric system performance using metrics such as FAR, FRR, EER, ROC, DET
- Identify threats, risks, and ethical issues related to biometric AI technologies
- Build small end-to-end pipelines combining acquisition, preprocessing, feature extraction, model training, and scoring

Students complete the program with a strong understanding of both the theoretical foundations and practical engineering approaches used in modern biometric systems.

Document produced under the CC BY-NC-ND license.

<table>
<tr><td colspan="9">Bialystok University of Technology</td></tr>
<tr><td>Study programme:</td><td colspan="5">Computer Science</td><td>Degree level</td><td>Engineer's degree</td></tr>
<tr><td rowspan="2">Module name:</td><td colspan="5" rowspan="2">Artificial Intelligence in Biometrics</td><td>Module ID:</td><td>SIwB</td></tr>
<tr><td>Module type</td><td>mandatory</td></tr>
<tr><td rowspan="2">Teaching form and hours</td><td>L</td><td>C</td><td>LC</td><td>P</td><td>SW</td><td>S</td><td>Semestre</td><td>1</td></tr>
<tr><td>20</td><td></td><td></td><td></td><td>20</td><td></td><td>ECTS points</td><td>1</td></tr>
<tr><td>Course objectives</td><td colspan="8">Present AI methods used in biometric systems, teach computer vision and deep learning techniques, and develop practical skills in building biometric recognition pipelines.</td></tr>
<tr><td>Course content</td><td colspan="8">Lecture:
1. Introduction to AI in Biometrics. Role of AI in recognition and verification tasks.
2. Biometric Modalities. Fingerprints, face, iris, voice, key data characteristics.
3. Biometric System Pipeline. Acquisition, preprocessing, features, matching.
4. Image Preprocessing Methods. Enhancement, normalization, segmentation basics.
5. Feature Extraction Techniques. Geometric, statistical, and texture features (HOG/LBP).
6. Classical ML for Biometrics. k-NN, SVM, Random Forest, when and why they work.
7. Matching and Scoring. Distance metrics, similarity scores, thresholding.
8. Error Metrics in Biometrics. FAR, FRR, EER, ROC/DET concepts.
9. Introduction to Deep Learning. Why DL improves biometric performance.
10. CNN Fundamentals. Convolutions, pooling, feature maps, basic concepts.
11. Simple CNN Architectures. LeNet-style models for small biometric images.
12. Training Deep Biometric Models. Data augmentation, overfitting control.</td></tr>
</table>

	13. Face Recognition Basics. Embeddings and similarity-based matching. 14. Fingerprint Recognition Basics. Minutiae and ridge-based DL approaches (overview only). 15. Iris & Voice Biometrics – Intro. Only main ideas, no deep dive. 16. Liveness Detection. Simple anti-spoofing concepts (texture cues, blinking, noise patterns). 17. AI in Surveillance. Person re-ID and basic object tracking (light introduction). 18. Dataset Challenges. Quality, imbalance, noise, real-world variability. 19. Security & Privacy Issues. Spoofing risks, deepfakes, GDPR basics. 20. Trends and Limitations. Multimodal biometrics, constraints of current AI systems. Workshop: 1. NumPy Basics for Biometric Data. Arrays, simple operations on fingerprint/face images. 2. Pandas for Biometric Features. Loading small datasets, summary stats. 3. Visualization. Histograms, distributions, heatmaps (matplotlib/seaborn). 4. Biometric Image Preprocessing. Resize, normalization, thresholding (OpenCV). 5. HOG and LBP Feature Extractions 6. Intro to SVM/Random Forrest classifiers 7. Intro to TensorFlow/Keras/Pytorch. Build a minimal dense network for a simple biometric task. 8. Data augmentation techniques 9. Performance Metrics. FAR/FRR/EER score interpreatation 10. Embeddings with Pretrained Model. Extract simple embeddings (e.g., MobileNet) and compare. 11. Similarity Matching. Cosine distance between embeddings for identity verification. 12. Evaluation Curves. ROC and DET plotting for model comparison. 13. Final Project: mini Biometric Pipeline. Preprocess, extract features, classify, evaluate.
Bibliography	K. Saeed, J. Pejaś, R. Mosdorf (Eds), Biometrics, Computer Security Systems and Artificial Intelligence Applications, Springer Science + Business Media, NY, 2006. Ian Goodfellow, Yoshua Bengio, Aaron Courville: Deep Learning, 2016. Anil K. Jain, Arun Ross, Karthik Nandakumar: Introduction to Biometrics, 2025.

Teaching methods	Lecture, specialization workshop classes	
Form of assesment	Lecture: Written knowledge test. Specialised laboratory: Assessment of the completion of computational and experimental tasks. The assessment includes the correctness of the completed problem-solving projects.	
Symbol	**Learning outcomes**	**Outcome type**
LO #1	Understands image processing techniques	Knowledge
LO #2	Knows feature extraction methods	Knowledge
LO #3	Understands matching and error metrics, including evaluation measures, and their practical interpretation	Knowledge
LO #4	Performs preprocessing and feature extraction for biometric images	Skills
LO #5	Selects and trains classical ML or DL models for biometric classification.	Skills
LO #6	Evaluates biometric system performance using FAR, FRR, EER, ROC/DET.	Skills
LO #7	Recognizes the social and ethical implications of biometric AI systems, including issues of privacy and security.	Social competences
Symbol	**Learning outcome verification method**	**Verifying activity**
LO #1	Written exam	Lecture
LO #2	Written exam	Lecture
LO #3	Project review	Workshop
LO #4	Project review	Workshop
LO #5	Project review	Workshop
LO #6	Project review	Workshop
LO #7	Discussions	Workshop

Student work hours		**Work hours:**	
	Attending lectures	20	
	Attending workshops	20	
	Project implementation	8	
	Self learning	8	
Quantitative indicators		**Hours**	**ECTS**
Student workload associated with classes requiring direct teacher involvement		20	1
Student workload associated with practical classes		20	1
Unit	Faculty of Digital Media and Computer Graphics	**Programme preparation date: 25.11.2025**	

© 2025. This work is licensed via CC BY-NC-ND 4.0.

<table>
<tr><td colspan="9">Bialystok University of Technology</td></tr>
<tr><td>Study programme:</td><td colspan="5">Computer Science</td><td>Degree level</td><td>Engineer's degree</td></tr>
<tr><td rowspan="2">Module name:</td><td colspan="5" rowspan="2">Fundamentals of Artificial Intelligence</td><td>Module ID:</td><td>PSI</td></tr>
<tr><td>Module type</td><td>mandatory</td></tr>
<tr><td rowspan="2">Teaching form and hours</td><td>L</td><td>C</td><td>LC</td><td>P</td><td>SW</td><td>S</td><td>Semestre</td><td>1</td></tr>
<tr><td>10</td><td></td><td></td><td></td><td>10</td><td></td><td>ECTS points</td><td>1</td></tr>
<tr><td>Course objectives</td><td colspan="8">Provide foundational knowledge of AI, introduce core machine learning methods, and develop basic practical skills in data processing and simple predictive models.</td></tr>
</table>

Course content	Lecture: 1. History of AI. From symbolic AI to modern ML; key milestones. 2. AI Technologies. Rules, expert systems (only basics) 3. Machine Learning Overview. Supervised vs. unsupervised, datasets, labels 4. Regression Models. Linear regression, cost function, overfitting 5. Classification Models. Logistic regression, decision boundaries 6. Neural Networks Basics. Perceptron, activation functions, simple MLP 7. Deep Learning Concepts. Hidden layers, optimization, training loop 8. Evaluation Metrics. Accuracy, precision, recall, confusion matrix 9. Applications of AI. Industry, medicine, robotics, finance 10. Benefits & Risks. Ethical issues, bias, transparency, limitations Workshop: 1. NumPy Basics. Arrays, vectorized operations, broadcasting exercises. 2. Data Visualization. Line charts, histograms, scatter plots (matplotlib). 3. scikit-learn Introduction. Dataset loading, train/test split, basic workflow. 4. Linear Regression. Training a regression model and plotting predictions. 5. Binary Classification. Logistic regression, metrics, confusion matrix. 6. k-NN Classifier. Distance-based classification with different k values. 7. Decision Trees. Non-linear modeling, depth analysis, accuracy check. 8. Model Evaluation. Accuracy, precision, recall, F1-score interpretation. 9. Feature Scaling. Normalization with StandardScaler and model training. 10. Mini ML Pipeline. Preprocessing, model training and evaluation (small dataset).
Bibliography	Stuart Russell, Peter Norvig: Artificial Intelligence: A Modern Approach, 2022. Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirani: An Introduction to Statistical Learning, 2023. Aurélien Géron: Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow, 2022.
Teaching methods	Lecture, specialization workshop classes

Form of assesment	Lecture: Written knowledge test. Specialised laboratory: Assessment of the completion of computational and experimental tasks. The assessment includes the correctness of the completed problem-solving projects.	
Symbol	**Learning outcomes**	**Outcome type**
LO #1	Understands basic concepts, history, and main areas of AI.	Knowledge
LO #2	Understands and can explain core ML methods (regression, classification, simple neural networks).	Knowledge
LO #3	Knows how to use ML tools (scikit-learn)	Skills
LO #4	Knows risks involved in AI, Ethical issues, bias, transparency, limitations	Social competences
Symbol	**Learning outcome verification method**	**Verifying activity**
LO #1	Written exam	Lecture
LO #2	Written exam	Lecture
LO #3	Project review	Workshop
LO #4	Discussions	Workshop
Student work hours		**Work hours:**
	Attending lectures	10
	Attending workshops	10
	Project implementation	4
	Self learning	4
Quantitative indicators		**Hours** / **ECTS**
Student workload associated with classes requiring direct teacher involvement		10 / 1

Student workload associated with practical classes		10	1
Unit	Faculty of Digital Media and Computer Graphics	**Programme preparation date: 25.11.2025**	

© 2025. This work is licensed via CC BY-NC-ND 4.0..

<table>
<tr><td colspan="9">Bialystok University of Technology</td></tr>
<tr><td>Study programme:</td><td colspan="5">Computer Science</td><td>Degree level</td><td>Engineer's degree</td></tr>
<tr><td rowspan="2">Module name:</td><td colspan="5" rowspan="2">Fundamentals of Biometric Systems (PSB)</td><td>Module ID:</td><td>PSB</td></tr>
<tr><td>Module type</td><td>mandatory</td></tr>
<tr><td rowspan="2">Teaching form and hours</td><td>L</td><td>C</td><td>LC</td><td>P</td><td>SW</td><td>S</td><td>Semestre</td><td>1</td></tr>
<tr><td>10</td><td></td><td></td><td></td><td>10</td><td></td><td>ECTS points</td><td>1</td></tr>
<tr><td>Introductory subjects:</td><td colspan="8"></td></tr>
<tr><td>Course objectives</td><td colspan="8">The course introduces the fundamental concepts, methods, and practical applications of biometric systems used for human identification and verification. Students gain theoretical knowledge of biometric modalities, error metrics, system architectures, and security aspects, along with hands-on experience working with biometric images, preprocessing, feature extraction, and fingerprint recognition using real devices.</td></tr>
<tr><td>Course content</td><td colspan="8">Lecture:
1. Introduction to biometrics – history and definitions. Examples of Biometric Systems and their applications from preprocessing to classification.
2. Human identification and verification.
3. Methods and algorithms of data acquisition from input images.
4. Preprocessing – biometric image scanning, thinning, segmentation.
5. Categories of biometrics – physiological and behavioral biometrics and their techniques.
5. Image analysis methods and algorithms in automatic object recognition.</td></tr>
</table>

	6. Examples of biometric tools and methods of classification for human identification and recognition. 7. Error types in human identification and verification methods and their significance in biometric security systems. The error measuring methods (FAR-False Acceptance Rate and FFR-False Rejection Rate). 8. Visual monitoring systems and their module from detection to cracking, classification and decision taking in human recognition approaches. 9. Examples of biometric applications – physiological (fingerprints, hand geometry, face, iris and retina, taste and odor) and behavioral (signature, voice, keystroke and mouse dynamics, gait and many others). Workshop: 1. Image loading & preprocessing. Basic operations using Python + OpenCV. Load fingerprint image, grayscale, histogram, threshold 2. Data acquisition. Introduction to biometric capture workflow. Capture several samples, save images, record metadata 3. Fingerprint enhancement. Simple filters. Apply Gaussian blur, CLAHE, binary threshold 4. Thinning. Skeletonization. Use cv2.ximgproc.thinning, visualize result 5. Simplified minutiae detection. Local neighborhood analysis. Detect ridge endings/bifurcations via pixel-neighbor counting 6. Template representation. Storing features. Build list of minutiae (x, y, type), save to JSON 7. Basic matching. Simple similarity metric. Compare minutiae sets using distance/count metrics 8. Mini-project: full pipeline. Integration. Enhancement, thinning, minutiae, matching, result display
Bibliography	A. K. Jain, R. Bok, S. Pankanti, Biometrics: Personal Identification in Networked Security, Kluwer Academic Publishers, 1999. L. Wayman, Fundamentals of Biometric Authentication Technologies, International Journal of Image and Graphics I (1), 2001, 93-1, 13.

	K. Saeed, J. Pejaś, R. Mosdorf (Eds), Biometrics, Computer Security Systems and Artificial Intelligence Applications, Springer Science + Business Media, NY, 2006. N. K. Ratha, V. Govindaraju (Eds), Advances in Biometrics Sensors, Algorithms and Systems, Springer, 2008.	
Teaching methods	Lecture, specialization workshop classes	
Form of assesment	Lecture: Written knowledge test. Specialised workhop: Assessment of the completion of experimental tasks. The assessment includes the correctness of the completed problem-solving projects.	
Symbol	**Learning outcomes**	**Outcome type**
LO #1	Understands key biometric modalities and principles of identification/verification.	Knowledge
LO #2	Describes the biometric pipeline: acquisition, preprocessing, features, matching.	Skills
LO #3	Applies basic preprocessing (normalization, thresholding, thinning).	Skills
LO #4	Recognizes the social and ethical implications of biometric AI systems, including issues of privacy, security, and potential misuse.	Social competences
Symbol	**Learning outcome verification method**	**Verifying activity**
LO #1	Written exam	Lecture
LO #2	Project review	Workshop

LO #3	Project review	Workshop	
LO #4	Discussions	Workshop	
Student work hours		**Work hours:**	
	Attending lectures	10	
	Attending workshops	10	
	Project implementation	4	
	Self learning	4	
Quantitative indicators		**Hours**	**ECTS**
Student workload associated with classes requiring direct teacher involvement		10	1
Student workload associated with practical classes		10	1
Unit	Faculty of Digital Media and Computer Graphics	**Programme preparation date: 25.11.2025**	

© 2025. This work is licensed via CC BY-NC-ND 4.0.