Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(AIML)

Field	Details
Course Name	Soft Computing
Course Code	AM-701
Semester	7
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Proficiency in Python (or equivalent) programming

• Fundamentals of linear algebra, probability, and statistics

• Basic algorithms and data structures knowledge

2. Course Learning Objectives

• Guide students to develop a comprehensive understanding of both classical AI techniques and soft-computing paradigms, and how they complement each other in solving real-world problems.

• Equip learners with the ability to design, implement, and evaluate hybrid AI systems that integrate expert-system reasoning, fuzzy logic, neural networks, and evolutionary optimization using Python and MATLAB toolkits.

• Foster critical thinking about the ethical, societal, and legal implications of AI technologies, encouraging responsible design and deployment of intelligent systems.

• Cultivate practical software-engineering skills for end-to-end AI project development, including requirement analysis, modular architecture design, testing, documentation, and reproducibility.

• Prepare students to analyze emerging trends in explainable and edge AI, and to articulate future research or industry directions for hybrid intelligent systems.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
			Total	100 marks

5. Course Modules

Module	Topics	Hours
1	**Foundations of AI & Soft Computing-** - Core AI workflow: problem formulation, data acquisition, model building, evaluation, deployment - Introductory machine-learning concepts (supervised vs. unsupervised, basic algorithms) - Soft-computing paradigm: contrast with hard computing, why uncertainty handling matters - Essential prerequisites for AI work: basic probability & statistics, linear algebra basics, algorithmic thinking, programming in Python (or C/Java/MATLAB) and critical thinking - Ethical, societal, and legal considerations in AI development	5

	- Overview of industry tools and platforms (scikit-learn, TensorFlow/Keras, MATLAB AI toolbox)	
2	**Expert Systems and Search Strategies** - Motivation and typical applications of expert systems in industry - Knowledge-base design: facts, rules, ontologies, and knowledge acquisition techniques - Inference engine fundamentals: forward vs. backward chaining, conflict resolution - User-interface considerations and system integration basics - Classical search strategies: depth-first, breadth-first, uniform-cost, heuristic (A*) - Simple constraint-satisfaction and planning examples - Development workflow: from requirement analysis to prototype implementation - Introductory hybridization: combining rule-based reasoning with basic machine-learning components	6
3	**Fuzzy Logic Foundations and Applications** - Fuzzy set theory: membership functions, linguistic variables, basic set operations - Fuzzy relations, propositions, and implication operators - Building fuzzy rule bases and inference mechanisms (Mamdani & Takagi-Sugeno) - Defuzzification methods (centroid, bisector, mean-of-maximum) - Simple fuzzy clustering: C-means and fuzzy C-means - Design of fuzzy-logic controllers (MATLAB/Simulink labs) - Industry case studies: automotive cruise control, consumer-electronics temperature regulation, decision-support systems	7
4	**Artificial Neural Networks** - Biological neuron vs. artificial neuron model - Core network architectures: feed-forward, recurrent, Radial Basis Function, introductory convolutional concepts - Learning paradigms: supervised, unsupervised, reinforcement (high-level view) - Key algorithms: perceptron, back-propagation, Hebbian learning, competitive learning - Training best practices: data preprocessing, regularization, early stopping, performance metrics - Hands-on labs with Python (Keras/TensorFlow) and MATLAB for function approximation,	8

	classification, and simple control tasks - Real-world examples: image recognition, time-series prediction, fault diagnosis	
5	**Evolutionary and Bio-Inspired Optimization** - Fundamentals of evolutionary computation and nature-inspired metaheuristics - Genetic Algorithms: chromosome encoding, selection, crossover, mutation, simple GA variants - Differential Evolution and Particle Swarm Optimization (basic concepts and implementation) - Ant Colony Optimization (path-finding illustration) - Intro to multi-objective optimization: Pareto dominance, simple NSGA-II outline - Practical parameter tuning and convergence monitoring - Industry applications: scheduling, routing, hyper-parameter tuning for ML models, design optimization.	8
6	**Hybrid AI Techniques** - Neuro-fuzzy systems: combining ANN learning with fuzzy inference, design steps - Hybrid expert systems enhanced by evolutionary search for rule optimization - Integrated soft-computing pipelines: fuzzy preprocessing, ANN modelling, evolutionary optimization - Project-based development cycle: requirement capture, design, implementation, testing, documentation - Use of MATLAB and Python (scikit-learn, DEAP, PyFuzzy) for rapid prototyping - Validation & verification methods, reproducibility, and basic deployment considerations - Future trends: explainable hybrid AI, edge-AI implementations, industry case studies	8

6. References

Textbooks:

1. Fuzzy Logic with Engineering Applications (3rd Edn.), Timothy J. Ross, Willey, 2010.

2. Foundations of Neural Networks, Fuzzy Systems, and Knowldge Engineering, Nikola K. Kasabov, MIT Press, 1998.

3. Fuzzy Logic: A Pratical approach, F. Martin, , Mc neill, and Ellen Thro, AP Professional, 2000.

Reference Books:

1. Neural Networks, Fuzzy Logis and Genetic Algorithms : Synthesis, and Applications, S. Rajasekaran, and G. A. Vijayalakshmi Pai, Prentice Hall of India, 2007.

2. Neural Networks and Learning Machines, (3rd Edn.), Simon Haykin, PHI Learning, 2011.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
AM-701.1	Recall and explain the fundamental concepts of artificial intelligence, soft-computing paradigms, and the essential probability, linear-algebra, and programming prerequisites needed for AI development.	Explain	Understand
AM-701.2	Implement a rule-based expert system and apply classical search strategies (e.g., depth-first, breadth-first, A*) to solve defined problem instances.	Implement	Apply
AM-701.3	Construct and analyze fuzzy-logic controllers by selecting appropriate membership functions, inference mechanisms (Mamdani or Takagi-Sugeno), and defuzzification methods for given control scenarios.	Construct	Analyze
AM-701.4	Design, train, and evaluate artificial neural network models using Python (Keras/TensorFlow) or MATLAB for tasks such as classification, regression, and time-series prediction.	Design	Apply
AM-701.5	Compare and assess the performance of evolutionary and bio-inspired optimization algorithms (Genetic Algorithms, Differential Evolution, Particle Swarm Optimization, Ant Colony Optimization) on benchmark problems, and tune their parameters to achieve convergence criteria.	Evaluate	Evaluate

AM-701.6	Synthesize a hybrid AI solution that integrates fuzzy preprocessing, neural-network modeling, and evolutionary optimization to address a real-world case study, delivering a documented, reproducible implementation.	Synthesize	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	1	1	-	2	-	2
CO2	3	2	3	2	3	1	1	1	2	2	2	2
CO3	3	2	3	2	3	1	1	1	2	2	2	2
CO4	3	2	3	2	3	1	1	1	2	2	2	2
CO5	3	2	3	3	3	1	1	1	2	2	2	2
CO6	3	3	3	3	3	2	2	2	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	3	2	1
CO4	3	3	1
CO5	3	2	1
CO6	3	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(AIML)

Field	Details
Course Name	AI and Cyber Security
Course Code	AM-703
Semester	7
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Proficiency in Python programming (including libraries such as pandas, NumPy, and scikit-learn)

• Fundamental understanding of computer networking and basic cybersecurity concepts (e.g., OSI model, common attack vectors, security controls)

• Introductory knowledge of linear algebra, probability, and statistics for machine learning

2. Course Learning Objectives

• Equip students with a comprehensive understanding of how AI and machine-learning techniques intersect with modern cyber-security challenges, frameworks, and best practices.

• Develop the ability to design, implement, and evaluate AI-driven detection and response solutions--including ML classifiers, deep-learning models, and UEBA systems--using Python and open-source toolchains.

• Cultivate critical skills for integrating AI models into real-world security operations, covering data pipelines, model lifecycle management, automation, and governance considerations such as explainability and bias.

• Foster an awareness of the ethical, legal, and regulatory implications of deploying AI in security contexts, enabling students to make responsible decisions and adhere to compliance standards.

• Prepare learners for professional advancement by guiding them through a capstone project that synthesizes end-to-end AI-security architecture, and by mapping career pathways, certifications, and emerging trends in the field.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full Marks	Assignment Full Marks	Attendance Full Marks	Total Marks
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	Topics	Hours
1	**Foundations of AI and Cyber Security** - Role of AI in Cyber Security - Overview of Threat Landscape and Common Attack Vectors - Security Frameworks and Standards (NIST, ISO 27001, etc.) - AI-enhanced vs. Traditional Security Controls - Fundamentals of Python for Security Analytics - Data preprocessing and manipulation with pandas & NumPy - Introductory use of AI/ML libraries (scikit-learn,	6

	TensorFlow Keras) - Evolution from Expert Systems to Modern AI in Security	
2	**Machine-Learning Techniques for Threat Detection** - Core concepts of Machine Learning for security analysts - Supervised vs. Unsupervised learning in a security context - Feature engineering for network traffic and log data - Common classification algorithms (Decision Trees, Random Forest, Logistic Regression, SVM) - practical focus - Clustering methods for anomaly detection (K-Means, DBSCAN) - hands-on - Building a simple ML-based Intrusion Detection System - Evaluation metrics for security-oriented ML models (precision, recall, ROC-AUC) - Toolchain overview: scikit-learn, TensorFlow Lite, Jupyter notebooks	8
3	**Deep Learning Essentials for Security** - Introduction to Neural Networks and why they matter for security - Convolutional Neural Networks (CNNs) for malware binary/image analysis - conceptual overview - Recurrent Neural Networks / LSTM basics for log-sequence modeling - Autoencoders for unsupervised anomaly detection - Practical considerations: model training, overfitting, and deployment - High-level view of adversarial threats to deep-learning models - Best practices for using pre-trained models and transfer learning - Hands-on lab with Keras/TensorFlow for a simple detection task	7
4	**AI-Driven Security Operations** - AI for SIEM data correlation and alert prioritization - Machine-learning based phishing detection (email & URL analysis) - Automated malware analysis using sandbox telemetry and AI - Fundamentals of User and Entity Behavior Analytics (UEBA)	7

	- Network traffic classification with machine learning - Integrating AI models into SOC playbooks and incident response workflows - Continuous learning, model retraining, and drift monitoring in operations - Governance, explainability, and trust in AI-enabled SOC environments	
5	**Threat Intelligence, Incident Response & Ethics** - Automating threat-intelligence collection with AI - Natural Language Processing (NLP) for extracting Indicators of Compromise (IOCs) - AI-assisted incident response workflow and threat hunting - Ethical considerations: bias, privacy, and responsible AI use - Legal and regulatory landscape (GDPR, CCPA, cyber-law, compliance frameworks) - Introductory view of adversarial machine learning for defenders - Real-world case studies of AI in cyber-security incidents - Emerging standards and certifications for AI-enabled security practice	8
6	**Integration, Emerging Domains & Professional Pathways** - End-to-end AI-cybersecurity integration architecture - Automated learning pipelines and model lifecycle management - AI applications in e-commerce, digital payments, and fraud detection - Building a lightweight AI-powered security toolkit with open-source components - Career pathways: roles, certifications, and continuing education options - Future trends: Zero-Trust, AI-generated attacks, quantum-resistant security - Capstone project framework, evaluation criteria, and deliverables - Resources, communities, and lifelong-learning strategies for AI security professionals	6

6. References

Textbooks:

1. Leslie F. Sikos (ed.) - "AI in Cybersecurity" (Springer, Intelligent Systems Reference Library, Vol. 151)

2. Clarence Chio, David Freeman - "Machine Learning and Security" (O'Reilly)

Reference Books:

1. Leslie F. Sikos - "Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection" (Wiley)

2. Packt - "Hands-On Artificial Intelligence for Cybersecurity"

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
AM-703.1	Recall the key concepts of AI in cyber security, major threat vectors, core security frameworks (NIST, ISO 27001), and basic Python syntax and primary data-science libraries (pandas, NumPy, scikit-learn).	Recall	Remember
AM-703.2	Explain the differences between traditional security controls and AI-enhanced controls, and describe how supervised, unsupervised, and deep-learning techniques are applied to threat detection, phishing mitigation, and anomaly detection.	Explain	Understand
AM-703.3	Implement data-preprocessing and feature-engineering pipelines with pandas/NumPy, and develop functional machine-learning models (e.g., Random Forest, K-Means) and a simple neural network in TensorFlow/Keras to detect intrusions or malware, achieving at least 85 % recall on the provided test set.	Implement	Apply
AM-703.4	Analyze the performance of multiple ML/DL models using precision, recall, ROC-AUC and conduct a comparative assessment of model robustness against adversarial perturbations and	Analyze	Analyze

	concept drift within a SOC workflow.		
AM-703.5	Evaluate the ethical, legal, and governance implications of deploying AI-driven security solutions--including bias mitigation, privacy compliance (GDPR, CCPA), and explainability--and formulate actionable recommendations for responsible AI use in incident response.	Evaluate	Evaluate
AM-703.6	Design and deliver a complete AI-enabled security solution--covering data ingestion, model-lifecycle management, integration into a SIEM/UEBA workflow, and a capstone presentation--that synthesizes concepts from all modules and includes a professional development pathway plan.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	-	-	-	1	-	2
CO2	3	2	2	2	2	2	-	2	1	2	1	2
CO3	3	2	3	2	3	1	-	1	1	1	2	2
CO4	3	3	2	3	3	2	-	2	1	2	2	2
CO5	2	2	1	2	1	3	2	3	1	2	1	2
CO6	2	2	3	2	3	2	1	2	3	3	3	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	3	3	1
CO4	3	2	1
CO5	2	1	3
CO6	3	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(AIML)

Field	Details
Course Name	Network Security & Cryptography
Course Code	AM-704
Semester	7
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Introductory Computer Science (programming fundamentals and data structures)

• Discrete Mathematics (including modular arithmetic, number theory, and basic combinatorics)

• Fundamentals of Computer Systems and Networking (operating system basics, OSI model, and TCP/IP concepts)

2. Course Learning Objectives

• Guide students to develop a comprehensive understanding of information-security fundamentals and how they intersect with emerging AI technologies, enabling them to assess and articulate security requirements for modern computing environments.

• Equip learners with the mathematical and algorithmic foundations of both classical and modern cryptography, so they can critically evaluate cryptographic schemes, perform basic security analyses, and apply appropriate techniques to protect data and AI models.

• Enable students to design, implement, and evaluate symmetric-key, asymmetric-key, and hash-based security mechanisms--including key management, digital signatures, and authenticated encryption--within real-world software and AI-centric applications.

• Foster the ability to integrate network, application, and cloud security controls (e.g., TLS, IPSec, container hardening, SSO) with legal, policy, and ethical considerations, preparing students to devise holistic security solutions for complex, AI-driven systems.

• Cultivate analytical and problem-solving skills through case-study driven exploration of contemporary threats such as adversarial machine-learning attacks, data-poisoning, and privacy breaches, empowering students to propose and justify robust mitigation strategies.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	**Topics**	**Hours**
1	**Fundamentals of Information Security** - Security concepts: need for security, security approaches, core principles (confidentiality, integrity, availability, authentication)	6

	- Security policies, risk management, and threat modeling - Security lifecycle & secure software development (SDLC, DevSecOps basics) - Overview of OSI security architecture and common security services/mechanisms - Basic categories of threats to computers and networks (malware, insider threats, social engineering) - Introduction to AI-related security concerns (adversarial ML, data privacy, model integrity)	
2	**Mathematical Foundations & Classical Cryptography** - Number-theory basics: primes, modular arithmetic, Euclid's algorithm, congruences - Intractable problems that underpin cryptography: integer factorisation, discrete logarithm, RSA & Diffie-Hellman problems - Classical encryption techniques: substitution, transposition, simple steganography - Foundations of modern cryptography: perfect secrecy, one-way functions, trapdoor functions - Basic cryptanalysis concepts and attack models (ciphertext-only, known-plaintext, chosen-plaintext) - Relevance to AI data protection (key management for model encryption, secure data sharing)	7
3	**Symmetric-Key Cryptography** - Symmetric-key principles and key-management basics - Block-cipher fundamentals and modes of operation (ECB, CBC, CTR, GCM/CCM - authenticated encryption) - Major block ciphers: DES/3DES (historical), AES (current standard) - Stream ciphers: RC4 (historical), modern LFSR-based designs, overview of ChaCha20 - Pseudorandom number generators and key-size considerations - Security analysis basics (differential & linear attacks - conceptual overview) - Application to AI workloads: encrypting model parameters, secure inference pipelines	8
4	**Asymmetric Cryptography, Digital Signatures & PKI** - Public-key mathematics essentials: modular exponentiation, Chinese Remainder Theorem (conceptual) - Core public-key algorithms: RSA, Diffie-Hellman, ElGamal, DSA - Key-exchange basics and protocol flow (DH & variants) - Digital signature schemes: RSA, DSA, ElGamal signatures, basics of blind signatures - Public-Key Infrastructure: X.509 certificates, certificate lifecycle, revocation, trust models - Single Sign-On (SSO) and federated identity basics (SAML, OAuth2/OpenID Connect) - Secure distribution of AI models and data using asymmetric techniques	7
5	**Hash Functions, MACs & Authentication Protocols**	6

	- Cryptographic hash functions: SHA-1 (historical), SHA-2 family, SHA-3, security properties and known attacks - Password-hashing algorithms for storage: bcrypt, scrypt, Argon2 - Message Authentication Codes: MAC concepts, HMAC, CMAC - Authentication mechanisms: passwords, challenge-response, multi-factor authentication - Zero-knowledge proof basics and biometric considerations (high-level overview) - Standards & best practices (ISO/IEC 10118, NIST SP 800-107) - Integrity verification for AI datasets and model artifacts	
6	**Network & Application Security, Legal & Case Studies** - Transport-level security: SSL/TLS architecture, HTTPS, Secure Shell (SSH) - IP security (IPSec): AH, ESP, IKE basics - Wireless security: WPA2/WPA3, mobile device considerations - Email security: PGP, S/MIME - Web security fundamentals: firewalls, secure coding, XSS, SQL injection, CSRF, intrusion-detection systems - Cloud & container security basics (IAM, secrets management, runtime protection) - Legal, policy & cyber-crime overview (privacy regulations, compliance frameworks) - Case studies with AI focus: adversarial attacks on ML models, data-poisoning incidents, secure multi-party computation for federated learning, SSO deployment in AI platforms	8

6. References

Textbooks:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.

2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition.

Reference Books:

1. Behrouz A. Ferouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 3rd Edition, Tata Mc Graw Hill, 2015.

2. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing", Fifth Edition, Prentice Hall, New Delhi, 2015.

3. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber crimes, Computer Forensics and Legal Perspectives", First Edition, Wiley India, 2011.

4. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
AM-704.1	Recall and list the core security principles (confidentiality, integrity, availability, authentication) and identify at least three AI-related security concerns such as adversarial machine learning, data privacy, and model integrity.	Recall	Remember
AM-704.2	Explain the role of number-theory concepts (primes, modular arithmetic, Euclidean algorithm) in cryptographic algorithms and perform modular exponentiation calculations used in RSA and Diffie-Hellman.	Explain	Understand
AM-704.3	Apply symmetric-key encryption (AES in CBC/GCM mode) and stream-cipher techniques to encrypt and securely transmit a sample AI model-parameter file, demonstrating correct key-management and mode selection.	Apply	Apply
AM-704.4	Analyze the operation of public-key algorithms (RSA, Diffie-Hellman, ElGamal) and PKI components (X.509 certificates, trust chains) to assess their suitability for secure distribution of AI models and federated-learning keys.	Analyze	Analyze
AM-704.5	Evaluate different cryptographic hash functions and MAC schemes (SHA-256, SHA-3, HMAC, Argon2) for integrity protection of AI datasets, and recommend the most appropriate construction based on security properties and performance constraints.	Evaluate	Evaluate
AM-704.6	Design an end-to-end security solution for a cloud-based AI/ML platform that integrates transport-level security (TLS), container secrets management, multi-factor authentication, compliance with GDPR/NIST, and mitigations against adversarial attacks and data-poisoning, and justify the design choices.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	2	-	2	1	1	1	2
CO2	3	2	1	2	2	1	-	1	1	1	1	2
CO3	3	2	3	2	3	2	1	2	2	2	2	2
CO4	3	3	2	3	2	2	-	2	2	2	2	2
CO5	3	2	2	2	3	2	-	2	2	2	2	2
CO6	3	3	3	3	3	3	2	3	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	3	2	1
CO4	3	2	1
CO5	3	2	1
CO6	3	3	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(AIML)

Field	Details
Course Name	Computer Vision
Course Code	AM-705
Semester	7
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Proficiency in Python programming (including NumPy, OpenCV, and basic data-structure/algorithm concepts)

• Solid foundation in linear algebra, calculus, and probability/statistics (e.g., vectors/matrices, derivatives/integrals, distributions)

• Introductory knowledge of digital signal/image processing fundamentals (sampling, filtering, Fourier basics)

2. Course Learning Objectives

• Provide students with a comprehensive understanding of the theoretical foundations and practical techniques of classical and modern computer vision, spanning image formation, feature extraction, segmentation, 3-D reconstruction, and deep-learning based methods.

• Develop the ability to design, implement, and evaluate end-to-end vision pipelines--ranging from low-level image processing to high-level tasks such as object detection, semantic segmentation, and visual reasoning--using both handcrafted algorithms and state-of-the-art deep learning frameworks.

• Cultivate critical thinking skills for selecting appropriate algorithms, models, and trade-offs (e.g., accuracy vs. efficiency, global vs. local descriptors, classical vs. deep approaches) based on problem requirements and computational constraints.

• Equip students with hands-on experience in modern vision toolchains (OpenCV, PyTorch/TensorFlow, pre-trained models) and best practices for data preparation, model fine-tuning, performance evaluation, reproducibility, and ethical deployment of vision systems.

• Foster interdisciplinary communication by enabling students to articulate vision concepts, algorithmic choices, and experimental results clearly to both technical and non-technical audiences.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full Marks**	**Assignment Full Marks**	**Attendance Full Marks**	**Total Marks**
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	**Topics**	**Hours**
1	**Foundations of Vision and Image Formation** - Human visual system and basic perception concepts - Geometric optics and image formation principles	5

	- Digital image representation, sampling, and quantization - Pinhole camera model - intrinsic & extrinsic parameters - Color fundamentals: RGB, HSV, gamma correction, white-balancing - Basic image enhancement: contrast stretching, histogram equalization & specification - Simple spatial-domain smoothing filters: mean (box) and median - Introductory edge detection: gradient operators (Sobel/Prewitt) and overview of Canny	
2	**Classical Image Processing & Feature Extraction** - Linear filtering: Gaussian smoothing and simple bilateral filter - Image pyramids and scale-space basics - Gradient-based corner detection (Harris) and simple affine-invariant corner ideas - Local descriptors: SIFT, SURF, HOG, LBP - Texture descriptors (e.g., GLCM) and shape descriptors (Hu moments) - Feature aggregation techniques - Bag-of-Words / Fisher Vector - Design trade-offs: global vs. local image descriptors - Practical lab: building a descriptor pipeline with OpenCV	6
3	**Segmentation and Motion Analysis** - Pixel-based thresholding and region-growing segmentation - Super-pixel generation (SLIC) and basic graph-cut segmentation - Mean-Shift clustering for mode-seeking segmentation - Edge linking and Hough Transform for line/ellipse detection - Background subtraction techniques for foreground detection - Optical flow fundamentals - Lucas-Kanade method - Spatio-temporal filtering and introductory video segmentation - Overview of deep-learning segmentation (U-Net) and a hands-on lab	7
4	**Multi-View Geometry, Depth & 3-D Reconstruction** - Epipolar geometry basics and stereo vision concepts - Camera calibration (intrinsic/extrinsic) and	8

	rectification - Fundamental matrix, essential matrix and point correspondence - Depth from disparity and basic 3-D reconstruction pipeline - Point-cloud generation and simple surface reconstruction - Introduction to Structure-from-Motion (SfM) workflow - Overview of deep-learning based monocular depth estimation - Lab: stereo pair processing -> disparity map -> point cloud	
5	**Classical Machine-Learning for Vision & Object Detection** - Feature-based image classification (Bag-of-Words with SIFT) - Supervised classifiers: linear SVM, k-NN, decision trees, ensemble basics - Performance evaluation: accuracy, ROC/PR curves, mAP - Sliding-window detection and the Viola-Jones face detector - Deformable Part Models - concept and simple implementation - Multi-class and fine-grained classification strategies - Transfer learning with handcrafted features (e.g., using pretrained CNN activations) - Lab: building a classic object detector and measuring its performance	8
6	**Deep Learning for Vision and End-to-End Applications** - Deep learning fundamentals: MLP, CNN, back-propagation, gradient descent - Modern CNN architectures (ResNet, EfficientNet) and transfer learning - Object detection frameworks: YOLO family, Faster R-CNN, Mask R-CNN - Semantic segmentation models: FCN, U-Net, transformer-based seg-former overview - Deep-learning depth estimation (monocular & video-based networks) - Image enhancement with CNNs: super-resolution, low-light, dehazing - Generative models overview (GANs) and style transfer basics - Visual captioning & Visual Question Answering (high-level pipeline)	8

	- Practical labs: end-to-end pipeline - data prep -> model fine-tuning -> inference & evaluation - Brief discussion on model deployment, reproducibility and ethical considerations	

6. References

Textbooks:

1. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer-Verlag London Limited, 2011

2. Fundamental of Digital Image Processing by Anil K. jain

Reference Books:

1. Milan Sonka, Vaclav Hlavac and Roger Boyle, "Image Processing, Analysis and Machine Vision", Third Edition, CL Engineering, 2013.

2. Research Papers @ IEEE TIP, IEEE TPAMI, CVPR, etc

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
AM-705.1	Describe the principles of geometric optics, digital image representation, and the pinhole-camera model (including intrinsic and extrinsic parameters), and perform basic image-enhancement operations such as contrast stretching and histogram equalization on sample images.	Describe	Understand
AM-705.2	Implement linear and non-linear filtering, construct image pyramids, and extract local descriptors (SIFT, HOG, LBP) to build a Bag-of-Words representation for a given image dataset using OpenCV.	Implement	Apply
AM-705.3	Analyze and compare pixel-based, super-pixel (SLIC), and graph-cut segmentation methods, and evaluate optical-flow results obtained with the Lucas-Kanade	Analyze	Analyze

	algorithm on video sequences.		
AM-705.4	Evaluate stereo calibration procedures, compute fundamental and essential matrices, generate disparity maps, and reconstruct point clouds, then assess reconstruction accuracy against provided ground-truth data.	Evaluate	Evaluate
AM-705.5	Design and train a classical object-detection pipeline that uses handcrafted features (Bag-of-Words with SIFT) and supervised classifiers (e.g., linear SVM, decision trees), and report performance metrics such as mAP, ROC, and PR curves.	Design	Create
AM-705.6	Synthesize an end-to-end deep-learning solution for a selected vision task (e.g., semantic segmentation or object detection) by fine-tuning a pre-trained CNN (e.g., ResNet, YOLO), evaluating its quantitative performance, and discussing deployment, reproducibility, and ethical considerations.	Synthesize	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	1	1	1	2	1	2
CO2	3	2	3	2	3	1	1	1	2	2	2	2
CO3	2	3	2	3	2	1	1	1	1	2	1	2
CO4	3	3	3	3	3	2	1	1	2	2	2	2
CO5	3	2	3	2	3	2	1	2	2	3	2	2
CO6	3	2	3	3	3	3	2	3	2	3	2	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	3	1
CO3	3	2	1
CO4	3	2	1
CO5	3	3	1
CO6	3	3	3