COURSE TITLE	**BIOMETRICS**
COURSE CODE	**01CC0509**
COURSE CREDITS	**3**

Objective:

1 This course provides a focused examination of the security and privacy aspects of biometric systems used for authentication and identification. Students will learn about various biometric modalities, the architecture of biometric systems, and the unique security threats and vulnerabilities they face, including presentation attacks (spoofing) and template database compromises. The course will cover techniques for evaluating system performance and security, countermeasures such as liveness detection and template protection, and the critical ethical, privacy, and legal considerations surrounding the use of biometrics.

Course Outcomes: After completion of this course, student will be able to:

1 Apply knowledge of biometric system concepts, components, and modalities to design or configure a basic biometric system for a given application.

2 Develop a secure biometric authentication framework that addresses identified security and privacy challenges.

3 Apply knowledge of biometric system architecture to identify potential attack vectors and vulnerabilities within different system components.

4 Analyze biometric system performance data and security evaluation metrics (e.g., FAR, FRR, EER) to assess system effectiveness and weaknesses.

5 Evaluate different security measures, including liveness detection and template protection techniques, for their effectiveness in mitigating specific biometric threats.

Pre-requisite of course: Basic understanding of probability and statistics. Familiarity with digital image processing or signal processing fundamentals. Basic understanding of pattern recognition or machine learning concepts. Basic knowledge of cybersecurity and privacy principles.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to Biometrics and System Architecture** What are Biometrics? Definition, history, and purpose., Physiological vs. Behavioral Biometrics (Examples of each)., Applications of Biometrics: Authentication, Identification, Verification., Generic Biometric System Architecture: Sensor, Feature Extractor, Template Database, Matcher, Decision Module., Key Performance Metrics: False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), Receiver Operating Characteristic (ROC) curves.	6
2	**Major Biometric Modalities and their Vulnerabilities** Fingerprint Recognition: Principles, feature extraction, common vulnerabilities (e.g., fake fingers)., Face Recognition: Principles, 2D vs. 3D face recognition, vulnerabilities (e.g., photos, masks, deepfakes)., Iris Recognition: Principles, advantages, vulnerabilities (e.g., printed iris images, contact lenses)., Voice Recognition: Principles, text-dependent vs. text-independent, vulnerabilities (e.g., recorded voice, synthetic speech)., Other Modalities: Signature verification, Gait analysis, Keystroke dynamics (brief overview and vulnerabilities).	7
3	**Biometric System Security Threats and Attacks** The "Attack Zoo": Categorization of attacks on biometric systems (according to Jain et al.)., Attacks at the Sensor: Tampering, bypassing., Presentation Attacks (Spoofing): Creating and presenting fake biometric samples., Attacks on the Channel: Intercepting or modifying data between modules., Attacks on the Template Database: Compromising stored templates., Attacks on the Matcher: Modifying match scores, bypassing the matcher., Attacks on the Decision Module: Overriding the final decision., Insider Threats in Biometric Systems.	7
4	**Biometric System Security Mechanisms and Evaluation** Liveness Detection / Presentation Attack Detection (PAD): Techniques for fingerprint, face, and iris. Active vs. Passive PAD., Biometric Template Protection: Why template protection is needed., Techniques for Template Protection:, Feature Transformation: Applying non-invertible transforms. • Biometric Cryptosystems: Fuzzy Commitment, Fuzzy Vault (concepts and limitations)., Evaluating Biometric System Security: Vulnerability analysis, penetration testing methodologies for biometrics., Benchmarking and Certification Standards (Overview).	7

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
5	**Multimodal Biometrics, Privacy, Ethics, and Standards** Multimodal Biometrics: Combining multiple traits or sensors for improved accuracy and security., Fusion Techniques: Sensor-level, Feature-level, Score-level, Decision-level fusion., Security and Privacy Implications of Multimodal Systems., Privacy Concerns in Biometrics: Data collection, storage, consent, function creep, linking across databases., Ethical Considerations: Bias in biometric systems, surveillance, autonomy, social exclusion., Biometric Standards and Regulations: Overview of relevant ISO standards and data protection regulations (e.g., GDPR) as they apply to biometrics., Case Studies of Biometric System Deployments and their Security/Privacy Issues.	5
Total Hours		**32**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Exploring a Biometric System Simulator: Using a provided software simulator to understand the basic flow of enrollment and verification in a biometric system.	2
2	**Practical 2** Capturing and Preprocessing Biometric Data: Capturing sample images of fingerprints or faces (of consenting participants in a controlled lab) and performing basic preprocessing steps (e.g., resizing, grayscale conversion, simple enhancement).	2
3	**Practical 3** Feature Extraction Demonstration: Using a publicly available library or tool to demonstrate the process of extracting features from a biometric sample (e.g., fingerprint minutiae, facial landmarks).	2
4	**Practical 4** Feature Extraction Demonstration: Using a publicly available library or tool to demonstrate the process of extracting features from a biometric sample (e.g., fingerprint minutiae, facial landmarks).	2
5	**Practical 5** Calculating Performance Metrics: Using a small dataset of genuine and impostor scores (provided), calculate FAR, FRR, and plot an ROC curve.	2
6	**Practical 6** Researching a Presentation Attack: Students research a specific presentation attack technique for a biometric modality (e.g., creating a gummy finger, using a photo to spoof face recognition) and present their findings.	2
7	**Practical 7** Analyzing a Hypothetical System Vulnerability: Given a diagram of a simple biometric system architecture, identify potential points of attack and explain how they could be exploited.	2

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
8	**Practical 8** Exploring Liveness Detection Concepts: Using a demo or description of a liveness detection technique (e.g., blink detection, texture analysis), discuss how it counters spoofing.	2
9	**Practical 9** Investigating Biometric Privacy Concerns: Research a real-world news article or report related to a biometric privacy issue and analyze the concerns raised.	2
10	**Practical 10** Mini-Project: Evaluating a Security Measure: Choose a specific biometric vulnerability and a proposed countermeasure (e.g., a template protection technique described conceptually) and analyze its potential effectiveness and limitations.	2
Total Hours		**20**

Textbook :

1 “Handbook of Biometrics”,, Jain, A.K., Flynn, P., Ross, A.A, Springer, 2007

References:

1 Handbook of Fingerprint Recognition, Handbook of Fingerprint Recognition, Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S, Springer, 2003

2 Advances in Biometrics: Sensors, Algorithms and Systems”, Advances in Biometrics: Sensors, Algorithms and Systems”, Ratha, N., Govindaraju, V., -, 2008

3 Biometrics for Network Security, Biometrics for Network Security, Paul Reid, Pearson, 2003

4 ISO/IEC Standards: a. ISO/IEC 19794 (Biometric data interchange formats) b. ISO/IEC 30107 (Presentation Attack Detection), ISO/IEC Standards: a. ISO/IEC 19794 (Biometric data interchange formats) b. ISO/IEC 30107 (Presentation Attack Detection), -, -, -

Suggested Theory Distribution:

The suggested theory distribution as per Bloom’s taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery

Remember / Knowledge	Understand	Apply	Analyze	Evaluate	Higher order Thinking / Creative
10.00	25.00	20.00	20.00	15.00	10.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

Instructional Method:

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 Biometric Security, edited by David Chek Ling Ngo, Andrew Beng Jin Teoh, and Jiankun Hu, published by Cambridge Scholars Publishing in 2015, ISBN: 978-1-4438-7183-9.

2 Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era, authored by Richard Jiang, Danny Crookes, and Weizhi Meng, published by Springer in 2017, ISBN: 978-3319837031.

3 Biometric-Based Physical and Cybersecurity Systems, authored by Mohammad S. Obaidat, Isaac Woungang, and Petros Nicopolitidis, published by Springer in 2019, ISBN: 978-3-319-98734-7