



No:-

Date:

CSXX2823: *Biometric Security*

L-T-P-Cr: 3-0-0-3

Pre-requisites: Prior knowledge of fundamentals of system security and machine learning.

Objectives/Overview:

- To understand the general principles of design of biometric systems and the underlying trade-offs.
- To impart knowledge of various biometric techniques used and its functioning.
- To analyze the authentication process through biometric systems for high security measurement.
- To discuss the privacy and legal aspects of biometric data in identification systems.
- To decide with evaluation procedures of a given biometric system.

Course Outcomes:

At the end of the course, a student should:

S.No	Course Outcome (CO)	Mapping to POs
1.	Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.	PO1, PO2, PO6, PO8
2.	Review technical challenges of biometric systems to build biometric identification systems.	PO1, PO2, PO4
3.	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems.	PO2, PO3
4.	Apply knowledge to design security systems using biometrics.	PO3

5.	Develop applications with intelligent biometric security systems with machine learning.	PO5
----	---	-----

UNIT I:

Lectures: 6

Overview of Biometrics: Biometric modalities, basic applications, benefits of biometrics over traditional authentication systems, Key biometric terms and processes, biometric characteristic, biometric systems: Identification, Verification. Biometric System Modules, Biometric system Errors: FAR/FRR. Threshold, Score distribution, Applications of biometrics.

UNIT II:

Lectures: 6

Performance Measure of a biometric system, Accuracy, Confusion Matrix, Precision and Recall, null and alternative hypothesis h_0 , h_1 , Error type I/II, Matching score distribution, FM/FNM, ROC curve, DET curve, FAR/FRR curve.

UNIT III:

Lectures: 8

Physiological Biometrics, Fingerprint: Fingerprint Sensing, Feature extraction (Local ridge orientation and frequency, Segmentation, Singularity detection, Enhancement and binarization, Minutiae extraction), Matching (Correlation-based techniques, Minutiae-based methods, Ridge Feature-based techniques), Performance evaluation.

UNIT IV:

Lectures: 8

Introduction to Multibiometrics, Limitations of unimodal systems, levels of fusion, Feature level fusion techniques: concatenation, PCA, LDA, Score fusion techniques: sum rule, product rule, min rule, max rule, hamature t-norm, Normalization techniques, Multibiometrics Using Face and Ear.- Incorporating Ancillary Information in Multibiometric Systems.

UNIT V:

Lectures: 8

Biometric Template Security, Biometric system vulnerability, template protection schemes: Feature Transformation, Biometric Cryptosystem, Salting (e.g., Biohashing), Non-invertible Transform, Key Binding, Key Generation.

UNIT VI:

Lectures: 6

Biometric System Security: Biometric attacks/tampering, solutions, biometric encryption. The Law and the Use of Biometrics. Biometric System Security.- Spoof Detection Schemes. Linkages between Biometrics and Forensic Science. Biometrics in Government Sector. Biometrics in the Commercial Sector. Biometric Standards, Biometrics in Banking Industry, Biometrics in Computerized, Patient Records, Biometrics in Credit Cards, Biometrics in Mass Disaster Victim.

Text/Reference Books:

1. John Chirillo and Scott Blaul : "Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.
2. Anil K jain, Patrick Flynn, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.
3. Julian D. M. Ashbourn, Biometrics: Advanced Identify Verification: The Complete Guide, a. Springer-verlag, 2000.
4. Davide Maltoni, Handbook of Fingerprint Recognition.

5. Biometric Systems: Technology, Design and Performance Evaluation, Editors: J. Wayman,
6. Jain, D. Maltoni and D. Maio, Springer, 2005