DO NOT TYPE IN THIS BOX

Bulletin # : 5

Academic Year : 2020-2021

FLORIDA INTERNATIONAL UNIVERSITY
UNIVERSITY CURRICULUM COMMITTEE
Proposal for a New Course

1. **School/College** Engineering and Computing

   Div./Dept. in Which Taught School of Computing and Information Sciences

2. | CIS | 5 | XXX | | 3 |
   |---|---|---|---|---|
   | Alpha Prefix | 1st Digit | Last 3 Digits | "C"-lec-lab "L"-Lab | Cr. Hrs. |

   CIP Code *(Leave this blank):*

CIS 5207

3. **Grading Method (select one):** ☒ Graded ☐ Pass/Fail

4a. **Course Title** Advanced AI/ML Techniques for Digital Forensic Applications

b. **Abbreviated course Title** *(for computer class schedules, transcripts)* Advanced Digital Forensic

LIMITED TO 25 Characters *(including spaces)*

5. **Statewide Course Numbering Subject Matter Area** CIS (Computer Science and Information Systems)

6. **Catalog Description/Major Topics** *(not to exceed 200 characters including spaces)*

College of Medicine and College of Law: Attach description not exceeding 1,000 characters including spaces.

Presents advanced AI/ML-based concepts in forensic software, tools, technology. Provides experience in selection and use of different tools for analyzing evidence and aiding investigations.

7. **Attach detailed syllabus course outline and course justification on separate page(s).**
8. **Prerequisite(s):** Graduate standing
9. **Corequisite(s):** None
10. **Objective(s) of Course:**

Understand the concepts of Forensic Software, hardware, tools, technology and practices along with experience of using different forensic tools for analyzing evidence and aid in investigation.

11. **Does this course duplicate/overlap other courses at FIU?** ☒ No ☐ Yes
    If yes, please explain:
12. **What other closely related department(s) have been consulted about this course?**

Reviewed courses offered at ECE. Ours is focused on AI/ML techniques

13. **Is this course used for the assessment of a program or a certificate (if yes, then send a notification to assessment@fiu.edu)?** **No** **Yes**

PROPOSAL REQUESTED BY:

Faculty Contact S. S. Iyengar — 02 / 02 / 2021
(Type name) (Signature)
iyengar@cis.fiu.edu — 305-348-3947
(Email address) (Phone number)

Chairperson (Dept./Div.) Jason Liu — 02 / 02 / 2021
(Type name) (Signature)

Chairperson (Curr. Comm.) Wei-Chiang Lin — 02 / 07 / 2021
(Type name) (Signature)

College/School Dean John Volakis — Anthony McGoron Digitally signed by Anthony McGoron Date: 2021.02.16 08:35:43 -05'00' — / / 2021
(Type name) (Signature)

Submit one original form. Attach one copy of the course justification and course syllabus, course description, objectives, major topics and textbooks.

Course Justification

Course: CIS-5XXX - Advanced AI/ML Techniques for Digital Forensic Applications

Rapid growth, proliferation and reliance on digital devices permeates our society, government and federal agencies exposing a potential vulnerability that attackers can use for cybercrimes. More importantly, there is ongoing concern of malfeasance, cyberattacks and illegal penetration of devices exposing valuable information to our nation's enemies. Once an incident occurs, the forensics process begins. But the need for digital forensics expertise, tools and techniques is now critical and will continue to increase exponentially with the advent of autonomous vehicles, more mobile devices, drones and connections to the Internet of Things, coupled with the rapid growth of computer espionage and cybercrime. In addition to a wide range of civilian applications, the problems under consideration also have significant applications in military decision-making and cyber security systems. AI applied to perception tasks such as imagery analysis can extract useful information from raw data and equip leaders with increased situational awareness. This course will provide near-real time use of analyzed data for decision making in Digital Forensic scenarios. This new course presents advanced AI/ML-based concepts in forensic software, tools, and technology, providing student experience in selection and use of different tools for analyzing evidence and aiding investigations. Furthermore, the course will also provide students with the knowledge to develop models and tools to understand and extract high-value, actionable information from digital data/devices for cybercrime analysis. The course will also include digital forensic experts from government, industry, and academia participating in providing hands-on approaches to solve real-time Digital Forensic applications.

With the knowledge gained from the course, students will be ready for multiple career paths including technical software and tool development and non-technical digital forensic investigations, criminal investigations and court cases.

School of Computing and Information Sciences

Course Title: Advanced AI/ML Techniques for Digital Forensic Applications
Date: 1/26/2021

Course Number: CIS-5XXX

Number of Credits: 3

Catalog Description: Presents advanced AI/ML-based concepts in forensic software, tools, technology. Provides experience in selection and use of different tools for analyzing evidence and aiding investigations.
Textbook: • **Handbook of Digital Forensics and Investigations**, by Eoghan Casey ed., 2009, Elsevier, Academic Press, ISBN 13: 978-0-12-374267 • **Cybercrime, Digital Forensics and Jurisdiction** by Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, 2015, Springer, ISBN ISBN-13: 978-3319151496
References: • **Big Data Forensics – Learning Hadoop Investigations** by Joe Sremack • **Hands-on Incident Response and Digital Forensics** by Mike Sheward
Prerequisites Courses: Graduate standing
Corequisite Courses: None

Type: Elective

Prerequisites Topics:

1. Solve algebraic equations
2. Selection statements
3. Data collection and Analysis
4. Understanding of Windows, Linux and other OS

Course Outcomes:

This course is designed to present the students with advanced Digital Forensics techniques involving the use of AI/ML based approaches. Furthermore, the course will provide the methodologies and procedures associated with digital forensic analysis using machine learning techniques. Students will learn advanced methods association with protocols needed to conduct forensic analysis. The course will highlight the current tools and the best practices in this field and showcase its importance in analyzing and solving crime scenes. Students will learn the various stages involved in the digital forensic investigation and the different tools that are used in each of the stages for data collection, preservation, orchestration of a crime scene using log data, storage requirements for the collected data, evidence maintenance and archiving etc. Students will also get to understand various case-studies

providing them with the various directions to perform analysis and learn different techniques and procedures that enable them to perform digital investigations.

1. Identify use of AI/ML in forensic studies and for real-time digital forensics applications
2. Understand DeepFakes techniques and the need for authenticating image and video data in cybercrime analysis
3. Collect software evidence and classify the crime data based on network science techniques
4. Analyze, preserve and store the digital bigdata evidence and use GPU based techniques for real-time processing involving Map-reduce algorithm.
5. Integration of image and video monitoring, classification and storage in distributed blockchains for trusted extraction
6. Compare and analyze existing tools for digital forensics and propose novel AI-based algorithmic tools
7. Hands-on experience on identifying and solving cybercrime and digital forensic problems

School of Computing and Information Sciences
CIS 5XXX
Advanced AI/ML Techniques for Digital Forensic Applications

Outline

Topic	Number of Lecture	Outcome
1. Introduction to digital forensics: introduction to digital principles etc (Inman-Rudin Paradigm, Locard's exchange principle), classification, association, reconstruction, quality assurance in digital forensics (scientific methods in digital forensics, validation processes) etc	3	1
2. Robust Deep Learning based Digital Forensics 2.1. Introduction to Deepfakes 2.2. ML/DL used for Deepfake generation 2.3. Stochastic Neural Network (SNN) for Deepfakes 2.4. Confidence distribution of SNN and the sensitivity of training data to determine authenticity of images 2.5. Multichannel ensemble model to detect video anomalies.	8	1, 2
2. Extract Forensic Event Signatures Using Network Science Techniques 2.1. Similarity with respect to "Offenders" or "Victims" 2.2. Spatial Cascadability of the Crime Events 2.3. Spectral Analysis of the Crime Events 2.4. Clusterability with respect to "Time" 2.5. Spatio-Temporal Assortative Matching of the Crime Events 2.6. Homophily among Crime Events of more than one Law Code 2.7. Network Forensic including modeling, duplication, analysis, file carving, network surveillance, network attack traceback and attribution, multimedia forensics etc.	9	2, 3, 4
3. Big Data Digital Forensics 3.1. Retrieving forensic evidence from Log Files 3.2. Forensic model using Hadoop Distributed File System (HDFS) 3.3. Design Forensics-as-a-Service (FaaS) for Digital Forensic investigators 3.4. GPU-based Architecture for Latent Fingerprints	10	2, 4, 6

4. Drone Forensics with Machine Learning based Fingerprinting and Blockchain 4.1. Video Source Proofing 4.2. Noise pattern extraction and comparison 4.3. DL and Neural Network based identification of image/video authenticity 4.4. Interoperability across image sources	10	4, 5, 7

Learning Outcomes:

Robust Deep Learning based Digital Forensics

1. Explore how ML is being utilized for Deepfakes, including simulation of audio and face swap
2. Develop a novel stochastic PDE-based framework to detect compromised audio and video
3. Investigate fundamental capabilities, challenges, and limitations of ML in detecting deepfakes.
4. Structure and formulate new algorithms that can be used in better forensic detection of fake information
5. Stacked and weighted average to select the best feature set for fusion

Extract Forensic Event Signatures Using Network Science Techniques

1. Understand forensic event networks and how to use it to visualize crime scenes.
2. Explain the development of algorithms and the corresponding software applications.
3. Develop multi-attribute based weighted temporal locality (WTL) graph model, a unique graph theoretic model for complex network analysis
4. Develop a binary search algorithm to determine “Offenders” and “Victims”.
5. Develop an algorithm for spatial crime cascade based on the assumption that crime events have the potential to spread to locations that are within a threshold distance
6. Apply the theory of homophily from social network analysis to explore whether different crimes can exist together in one community

Big Data Digital Forensics

1. Understand the key aspects of digital forensics are use of scientific methods, collection, preservation, validation, identification, analysis, interpretation, and documentation.
2. Develop algorithms to identify the closest match of fingerprint data or image data for a given partial image
3. Use GPU-based programming for real-time matching and ML techniques to automate and expedite the process

4. Preserve evidence in its most original form while performing a structured investigation by collecting, identifying, and validating digital information to reconstruct past events to minimize threats.

Drone Forensics with Machine Learning based Fingerprinting and Blockchain

1. Resolve any dispute about a crime-event using spatio-temporal context that reveals detailed information
2. Determining authenticity of video information for critical decision making
3. Digital watermarking and steganography
4. Maintaining the integrity of video data by getting the hash and storing it in a permissioned blockchain
5. Social media crime, Online defacement crime, Email investigation

School of Computing and Information Sciences
CIS 5XXX
Advanced AI/ML Techniques for Digital Forensic Applications

Oral and Written Communication

No significant coverage

Written Reports		Oral Presentations	
Number Required	Approx. Number of pages	Number Required	Approx. Time for each
1	10	1	30 minutes

Social and Ethical Implications of Computing Topics

No significant coverage

Topic	Class time	student performance measures

Assessments *

Final Examination – 50%

Projects/Class Seminar – 50%

* The University Grading Policy will be used