KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Cyberkryminalistyka multimedialna [S1Cybez1>CMm]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
16

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

3,00

Koordynatorzy

dr inż. Sławomir Maćkowiak
slawomir.mackowiak@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student powinen posiadać podstawową wiedzę z zakresu technologii multimedialnych, w tym analizy danych audiowizualnych oraz ich przetwarzania. Wymagana jest także znajomość podstawowych pojęć z zakresu informatyki, w tym architektury systemów komputerowych i sieci komputerowych, a także znajomość narzędzi używanych do analizy danych cyfrowych. Dodatkowym atutem będzie umiejętność interpretacji metadanych, identyfikacji manipulacji w materiałach multimedialnych oraz znajomość podstawowych procedur związanych z prowadzeniem badań kryminalistycznych w środowisku cyfrowym.

Cel przedmiotu

Celem przedmiotu Cyberkryminalistyka multimedialna jest zapoznanie studentów z metodami oraz narzędziami stosowanymi w analizie i weryfikacji danych multimedialnych w kontekście kryminalistycznym. Przedmiot ma na celu rozwinięcie umiejętności identyfikacji i analizy materiałów audiowizualnych, w tym wykrywania manipulacji, odzyskiwania ukrytych danych oraz analizy metadanych. Studenci zdobędą wiedzę teoretyczną i praktyczną z zakresu wykorzystywania technologii informatycznych w badaniach dowodów cyfrowych, z naciskiem na ich zastosowanie w procesach prawnych i śledczych.

Przedmiotowe efekty uczenia się

Wiedza:
K1_W05: Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna podstawy teorii, zna zasady administrowania danymi i związanymi z nimi standardami; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych.
K1_W07: Ma pogłębioną wiedzę o cyklu życia, projektowaniu i korzystaniu z odpornych na ataki programowych systemów informatycznych; zna i rozumie zasadę ich działania; zna narzędzia wykorzystywane do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo.
K1_W13: Zna zasady ukrywania danych, tj. kryptografię i steganografię; ma zaawansowaną wiedzę z zakresu kryptografii, algorytmów kryptograficznych, ich ograniczeń i ich udziału w cyberbezpieczeństwie.

Umiejętności:
• K1_U03: Potrafi zaplanować i przeprowadzić testy oprogramowania oraz systemów i sieci komputerowych w celu wykrycia w nich podatności na ataki; potrafi zaproponować rozwiązania poprawiające bezpieczeństwo działania.
• K1_U05: Przy formułowaniu i rozwiązaniu zadań inżynierskich z zakresu cyberbezpieczeństwa potrafi wykorzystać znane modele matematyczne i algorytmy oraz metody symulacyjne, eksperymentalne i analityczne.
• K1_U09: Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych.
• K1_U10: Na podstawie dostępnej dokumentacji i specyfikacji oraz standardów potrafi zaprojektować i zaimplementować w językach wysokiego poziomu bezpieczną aplikację internetową lub mobilną.
• K1_U11: Na podstawie dokumentacji technicznej, obowiązujących standardów, przy użyciu właściwych metod, narzędzi i elementów, potrafi zbudować, skonfigurować i uruchomić typowy system lub sieć komputerową spełniające wymogi cyberbezpieczeństwa.

Kompetencje społeczne:
K1_K01: Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują.
K1_K02: Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje.
K1_K03: Rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii na temat pozytywnych i negatywnych aspektów cyberbezpieczeństwa, a także jest gotowy do działania na rzecz interesu publicznego.
K1_K05: Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
1. Wykład
Zadanie z rozwiązywania problemów: studium przypadków, które wymagają współpracy w zespołach w celu analizy i rozwiązania problemów. Ocena umiejętności współpracy, ustalania priorytetów i proponowania skutecznych rozwiązań. Ocena krytycznego myślenia, umiejętności rozwiązywania problemów i dynamiki pracy zespołowej.
Próg zaliczeniowy wynosi 50% punktów.
W przypadku zaliczenia pisemnego i ustnego punkty są sumowane.
Skala ocen: <50% - 2,0 (ndst); 50% do 59% - 3,0 (dst); 60% do 69% - 3,5 (dst+) ; 70% do 79% - 4,0 (db); 80% do 89% - 4,5 (db+); 90% do 100% - 5,0 (bdb).
2. Laboratorium
Umiejętności osiągnięte w laboratorium określa się na podstawie raportów (sprawozdań) z przeprowadzonych ćwiczeń laboratoryjnych (OL) oraz zaliczenia końcowego (ZK) w formie samodzielnie realizowanego ćwiczenia lub projektu.
Kompetencje społeczne (KS) ocenia się na podstawie oceny umiejętności aktywnego słuchania, umiejętności współpracy i efektywnego udziału w dyskusjach zespołowych oraz poziomu zaangażowania

w procesy rozwiązywania problemów .
Wyznacza się średnią ważoną: OK = 0,5 x OL + 0,3 x ZK + 0,2 x KS i wystawia oceny:
5,0 dla OK > 4,75;
4,5 dla 4,75 > OK > 4,25;
4,0 dla 4,25 > OK > 3,75;
3,5 dla 3,75 > OK > 3,25;
3,0 dla 3,25 > OK > 2,75;
2,0 dla OK < 2,75.
Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Przedmiot wprowadza studentów do technik analizy cyfrowych multimediów, w kontekście wykrywania manipulacji i fałszerstw, odzyskiwania ukrytych danych oraz badania autentyczności i integralności plików multimedialnych. Kurs oferuje dogłębną eksplorację metod i narzędzi stosowanych w cyfrowej analizie śladów, szczególnie w zakresie obrazów, sekwencji wizyjnych i dźwięku.

Tematyka zajęć

Studenci poznają, jak z metadanych odczytywać informacje, które mogą być kluczowe w dochodzeniach kryminalistycznych, takie jak geolokalizacja, czas wykonania, atrybuty techniczne i inne, które mogą wskazywać na potencjalne manipulacje lub nietypowe zmiany.
Ważną częścią kursu jest wykrywanie manipulacji i fałszerstw, z naciskiem na cyfrowe obrazy i sekwencje wizyjne. Omówione zostaną techniki pozwalające na identyfikację zmian wynikających z edycji, takich jak splicing, modyfikacje cieni i poziomów kompresji, oraz wielokrotna kompresja JPEG. Studenci dowiedzą się, jak różne manipulacje wpływają na strukturę plików i jak można je wykryć za pomocą specjalistycznych narzędzi i technik. Kurs obejmuje także zastosowanie analizy histogramów, gradientów i tekstur w celu zidentyfikowania zmian i niespójności wizualnych.
Integralną częścią przedmiotu jest również temat odzyskiwania i analizy ukrytych danych w multimediach, gdzie studenci zapoznają się z technikami steganograficznymi oraz metodami odzyskiwania informacji zaszytych w plikach multimedialnych. Omówione zostaną sposoby ukrywania danych w obrazach, audio i wideo, a także różne metody wykrywania i odszyfrowywania tych informacji. Uczestnicy kursu poznają techniki pozwalające na identyfikację nietypowych struktur i niezgodności w formatach multimedialnych, które mogą wskazywać na obecność ukrytych danych lub złożonych archiwów zagnieżdżonych.
Ostatni blok kursu dotyczy narzędzi do analizy kryminalnej audio i wideo. Studenci będą badać, jak formaty audio i wideo mogą być analizowane pod kątem manipulacji, rozpoznawania ukrytych sygnałów oraz badania integralności nagrań. Kurs wprowadza techniki analizy widmowej oraz metody wykrywania zmian wynikających z edycji i kompresji, jak również podstawowe narzędzia stosowane w analizie kryminalistycznej dźwięku i obrazu ruchomego. Dodatkowo, omówione zostaną aspekty techniczne związane z formatami plików, kodekami oraz narzędziami wspierającymi proces analizy i przetwarzania multimediów.
Przedmiot łączy teorię z praktyką, aby dać uczestnikom umiejętności niezbędne do samodzielnej analizy multimediów w kontekście kryminalistycznym. Po ukończeniu kursu studenci będą zdolni do identyfikowania i analizowania różnorodnych manipulacji oraz uzyskiwania kluczowych informacji, które mogą wspierać dochodzenia w sprawach cyfrowych.
Zajęcia praktyczne w laboratorium:
- Analiza metadanych i ich rola w kryminalistyce
- Wykrywanie manipulacji i fałszerstw w multimediach
- Odzyskiwanie i analiza ukrytych danych w multimediach
- Narzędzia do analizy kryminalnej audio i wideo

Metody dydaktyczne

1. Techniki aktywnego uczenia się: Strategie aktywnego uczenia się, takie jak dyskusje w grupach, rozwiązywanie problemów i studia przypadków, aby aktywnie zaangażować studentów w proces uczenia się. Zachęcanie do wspólnego uczenia się i interakcji, aby wspierać krytyczne myślenie i stosowanie wiedzy.
2. Integracja technologii: Wykorzystanie narzędzi i platformy technologicznej, aby poprawić jakość

nauki. Korzystanie z narzędzi do współpracy online podczas sesji burzy mózgów, wirtualnych symulacji do rozwiązywania problemów oraz prezentacji multimedialnych, aby dostarczać wciągające treści. Ponadto wykorzystanie internetowych forów dyskusyjnych lub systemów zarządzania nauczaniem do asynchronicznego uczenia się i udostępniania zasobów.
3. Uczenie się oparte na przypadkach: włączenie rzeczywistych studiów przypadków do wykładów i laboratoriów, aby zademonstrować praktyczne zastosowanie kreatywnego myślenia w rozwiązywaniu problemów technicznych. Zachęci to do analizowania i omawiania przypadków, identyfikowania kreatywnych rozwiązań i refleksji nad procesem podejmowania decyzji.
4. Informacja zwrotna i nauczanie od studentów: Wprowadzenie mechanizmów informacji zwrotnej od studentów, w ramach których uczniowie przekazują konstruktywne informacje zwrotne na temat podejść do rozwiązywania problemów lub rozwiązań projektowych swoich rówieśników. Zachęcanie do sesji nauczania studenckiego, podczas których studenci mogą dzielić się swoją wiedzą i kreatywnymi technikami z kolegami.
5. Nauka oparta na projektach: Włączenie nauki opartej na projektach do programu nauczania, w której studenci pracują nad rzeczywistymi problemami lub projektują wyzwania wymagające kreatywnego myślenia. Takie podejście pozwala zastosować swoje umiejętności, przeprowadzić dogłębne badania i opracować innowacyjne rozwiązania poprzez praktyczne, empiryczne uczenie się.
6. Wykłady online

Literatura

Podstawowa:
• A. E. Hassanien, M. M. Fouad, A. A. Manaf, M. Zamani, R. Ahmad, and J. Kacprzyk, Multimedia Forensics, Singapore: Springer, 2021. DOI: 10.1007/978-981-16-7621-5.
• A. T. S. Ho and S. Li (Eds.), Handbook of Digital Forensics of Multimedia Data and Devices, Hoboken, NJ, USA: Wiley, 2015. DOI: 10.1002/9781118757079.

IGI Global, 2020. DOI: 10.4018/978-1-7998-4311-1.

Uzupełniająca:
Uzupełniająca
• A. E. Hassanien, M. M. Fouad, A. A. Manaf, M. Zamani, R. Ahmad, and J. Kacprzyk (Eds.), Multimedia Forensics and Security: Foundations, Innovations, and Applications, Cham, Switzerland: Springer, 2016. DOI: 10.1007/978-3-319-44270-9.
• S. Li and K. A. Renaud (Eds.), Handbook of Research on Multimedia Cyber Security, Hershey, PA, USA:

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	88	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	48	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	40	1,50