ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
«31» 08 2024 р.

СИЛАБУС

Навчальна дисципліна: *"Стеганографія і комп'ютерна графіка "*

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: Перший бакалаврський

Загальна інформація

Позиція	Інформація
Викладач(і)	Муляр Ігор Володимирович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/mulyar-igor-volodymyrovych
E-mail викладача(ів)	muliariv@khmnu.edu.ua
Контактний телефон	+3 8 067 938-15-44
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=6189
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/5011940672 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр І (осінньо-зимовий)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
ОД	-	-	8	240	85	34	34	17		155			+	

Анотація дисципліни

Дисципліна «Стеганографія і комп'ютерна графіка» є вибірковою, викладається для студентів очної денної форми навчання, рекомендована для здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» першого (бакалаврського) рівня, охоплює сучасні підходи в галузі обробки зображень двовимірних та тривимірних об'єктів за допомогою комп'ютера, та надає необхідні знання та навики створення та виявлення прихованого каналу передачі інформації в інформаційних та комунікаційних системах при вирішенні задач захисту інформації.

Пререквізити –.

Кореквізити –.

Мета дисципліни. Формування системи знань та розуміння сучасних комп'ютерних графічних технологій, їх можливостей по створенню, обробці і публікації різних видів зображень; отримання студентами необхідних знань та навиків створення та виявлення стеганоканалу передачі інформації в інформаційних та комунікаційних системах при вирішенні задач захисту інформації.

Предмет дисципліни. Сучасні методи обробки зображень, як засобами відповідних графічних редакторів, так і засобами візуальних мов програмування; створення та виявлення стеганоканалів передачі інформації.

Завдання дисципліни. Зформувати знання про принципи, що лежать в основі растрового і векторного способів представлення графічної інформації, математичні та алгоритмічні основи комп'ютерної графіки; формування умінь і навичок створення та виявлення стеганоканалу передачі інформації в інформаційних та комунікаційних системах; практичну основу підготовки бакалавра як проектувальника графічних і стеганографічних систем. Практичні навики роботи з генеративним ШІ. Використання OSINT для дослідження цифрових зображень.

Вивчення дисципліни має забезпечити набуття компетентностей та досягнення результатів навчання:

компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

результати навчання:

ПЗН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПЗН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПЗН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно- телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

ПЗН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПЗН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* знання теорії і прийомів комп'ютерної графіки та стеганографії у практичних ситуаціях професійної діяльності, *вміти* створювати нові зображення і редагувати наявні, перетворювати формати комп'ютерних зображень та їхні колірні моделі, імпортувати належним чином підготовлені графічні зображення в офісні документи, у вебсторінки, у електронні та поліграфічні видання; *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного та стеганографічного захисту інформації; *здійснювати* вибір стеганографічних методів та алгоритмів згідно з вимогами конкретного застосування *застосовувати* відомі програмні засоби приховування даних і вбудовування цифрових водяних знаків у різного виду інформацію; *розробляти* програмні та апаратні засоби, що реалізують стеганографічні методи та алгоритми та *давати* оцінку якості прийнятих в них рішень для застосування в системах захисту; *оцінювати* стійкість стеганографічної системи.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції*	Тема лабораторної роботи та практичних занять**	Самостійна робота студента		
				Зміст	Години	Літера-тура
1	*2*	*3*	*4*	*5*	*6*	*7*
1	1	**Основні поняття комп'ютерної графіки.** Основні поняття комп'ютерної графіки (колір, роздільна здатність,). Області застосування. Растрова графіка (Растрова графіка, загальні відомості. Растрові представлення зображень. Види растрів. Фактори, що впливають на кількість пам'яті, займаної растровим зображенням. Переваги і недоліки растрової графіки. Геометричні характеристики растра (роздільна здатність, розмір растра, форма пікселів). Кількість кольорів растрового зображення.) Векторна графіка (загальні відомості, спосіб збереження зображення, елементи (об'єкти) векторної графіки, об'єкти і їхні атрибути). Фрактальна графіка. Найвідоміші графічні редактори. Мови програмування графіки.	**ЛР1.** Знайомство з інтерфейсом і інструментами Photoshop, створення простих зображень в графічному редакторі Adobe Photoshop	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1	9	Літ.: [7] с.3-17, с.33-39, с.57-61; [22] с.29-70.
2	1	**Колір та моделі кольору. Формати збереження графічних зображень.** Основи теорії кольору. Характеристики	**ПЗ1.** Використання генеративного ШІ для створення растрових зображень	Опрацювання теоретичного матеріалу, виконання ПЗ1, підготовка до захисту ЛР1	9	Літ.: [6] с.26-50; [7] с.17-27.

		кольору: колірний тон, яскравість, насиченість. Закони змішування кольорів. Колірне охоплення та колірні моделі: RGB,CMY та CMYC, HSB та HLS, Lab. Кодування кольору. Палітра, Типи растрових зображень. Графічні файли. Класифікація форматів. Растрові формати BMP, TIFF, PCX, GIF, JPRG, PNG, JBIG2, JPEG 2000, LWF. Приклади запису растрового зображення в різних форматах. Розвиток растрових форматів. Формати DXF, MIF-MID. Мета файли:CGM, EPS, PICT,WMF/EMF,CD, FH7, FH5, PostScript. Призначення. Переваги та недоліки.				
3	1	**Формат Jpeg.** Структура формат Jpeg. Службові маркери. Просторова область зображення. Стиснення Jpeg. Дискретно-косинусне перетворення. Вейвлети.	**ЛР2.** Складання колажу у програмі Adobe Photoshop.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2	9	Літ.: [6] с.50-56.
4	1	Математичні засоби комп'ютерної графіки. Перетворення на площині. Афінні перетворення на площині. Перехід від однієї координатної системи на площині до іншої. Поворот R (rotation). Розтягування (стискування) D (dilatation). Відображення відносно осі абсцис M (reflection). Перенос T (translation). Причини використання	**ПЗ2**. Використання ШІ для редагування існуючих растрових зображень	Опрацювання теоретичного матеріалу, виконання ПЗ2, підготовка до захисту ЛР2	9	Літ.: [7] с.39-43; [10] с.83-164; [22] с.204-212.

		афінних перетворень. Матричний запис афінних перетворень. Од-норідні координати точки. Матриці перетворень. Технологія застосування мат-риць перетворень для реалізації графічних перетворень на площині.				
5	1	Перетворення в просторі. Проеціювання. Афінні перетворення в просторі. Однорідні координати точки в просторі. Матриці перетворень в просторі. Поворот R (rotation) – навколо осей абсцис, ординат і аплікат. Розтягування (стискування) D (dilatation) – вздовж осей абсцис, ординат і аплікат . Відображення відносно осі абсцис M (reflection) – відносно площин xy, yz, xz. Перенос T (translation) – на вектор (x,y,z). . Технологія застосування матриць перетворень для реалізації графічних перетворень в просторі.	**ЛР3**. Робота з графічним редактором Corel Draw – основні прийоми і правила	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР3	9	Літ.: [7] с.39-43; [10] с.83-124; [22] с.213-257.
6	1	**Тривимірна графіка.** Основні поняття. Моделювання і рендеринг. Моделі опису поверхонь. Шейдери. Рендеринг. Матричні обчислення в тривимірній графіці. Програмне забезпечення. Фізичне представлення трьохвимірних обєктів.	**ПЗ3.** Використання генеративного ШІ для створення векторних зображень	Опрацювання теоретичного матеріалу, виконання ПЗ3, підготовка до захисту ЛР3	9	Літ.: [7] с.61-84; [10] с.164-267; [22] с.259-299.
7	2	**Вступ до стеганографії.** Предмет стеганографії, основні	**ЛР4.** Виконання креслеників в Corel Draw.	Опрацювання теоретичного матеріалу, підготовка до	9	Літ.: [1] с.17-42; Літ.: [4] с.20-55; [6] с.5-22.

		терміни та визначення. Історичні приклади стеганосистем. Цифрова стеганографія. Предмет, термінологія, галузь використання. Математична модель стеганосистем. Стеганографічні протоколи. Практичні аспекти вбудування даних.		виконання ЛР4		
8	2	**Методи стеганографії. Приховування даних у текстових файлах.** Напрямки стеганографії. Класифікація стегосистем. Класифікація методів приховання інформації. Класифікація методів стеганографічного захисту. Приховування даних у текстових файлах. Методи текстової стеганографії.	**ПЗ4.** Використання генеративного ШІ для створення аудіо та відео контенту	Опрацювання теоретичного матеріалу, виконання ПЗ4, підготовка до захисту ЛР4 Підготовка до тестування	10	Літ.: [1] с.89-92, с.353-372; [2] с.9-43; [6] с.130-134.
9	2	**Приховування даних у нерухомих зображеннях.** Основні властивості ЗСЛ, що використовуються при приховуванні даних в зображеннях. Стійкість стеганосистеми до активних атак. Приховування даних у просторовій області зображень. Методи приховування в найменш значущому біті даних.	**ЛР5.** Побудова двомірних зображень з допомогою графічних примітивів мов програмування Тестування.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5	9	Літ.: [1] с.89-92; [6] с.23-26, 58-76.
10	2	**Приховування даних просторовій області зображення.** Блокове приховування. Метод квантування, метод «хреста».	**ПЗ5.** Застосування технології OSINT для пошуку за зображенням	Опрацювання теоретичного матеріалу, виконання ПЗ5, підготовка до захисту ЛР5	9	Літ.: [1] с.93-162; [6] с.23-26; с.76-77.

11	2	**Приховування даних у частотній множині зображень.** Метод Коха-Жао та його модифікації.	**ЛР6.** Приховування інформації у текстові та графічні файли за допомогою стеганографічних програм.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6	9	Літ.: [1] с.163-184; [6] с.78-79.
12	2	**Приховування даних у частотній множині зображень (2 частина).** Метод Хсу – Ву. Метод Фрідріха. Приховування даних у нерухомих зображеннях за допомогою методів розширення спектра.	**ПЗ6.** Використання ШІ длі програмування двох і трьохвимірної графіки	Опрацювання теоретичного матеріалу, виконання ПЗ6, підготовка до захисту ЛР6	9	Літ.: [1] с.185-256; [6] с.79-111.
13	2	**Цифрові формати аудіосигналів.** Особливості слухової системи людини (ССЛ). Основні властивості ССЛ, що використовуються при приховуванні даних в аудіосигналах. Цифрові формати аудіосигналів (формати WAV, WMA,MP3, AAC, OGG Vorbis). Особливості комп'ютерної обробки аудіосигналів. Приховування даних у просторій множині аудіосигналу (приховування в найменш значущому біті даних та за допомогою ехосигналів).	**ЛР7** Приховування інформації у аудіоафайли за допомогою стеганографічних програм.	Опрацювання теоретичного матеріалу, підготовка до до виконання ЛР7	9	Літ.: [1] с.257-267; [6] с.112-121**.**
14	2	Приховування в звукових та відео файлах. Приховування даних у частотній множині аудіосигналу (фазове кодування). Приховування даних в аудіосигналах за допомогою методів розширення спектра.	**ПЗ7.** Дослідження існуючих стеганографічних програм, та використання в якості контейнеру згенерованого ШІ контенту	Опрацювання теоретичного матеріалу, виконання ПЗ7, підготовка до захисту ЛР7	9	Літ.: [1] с.268-352; [4] с.59-104**;** [6] с.122-129**;** [23].
15	2	**Цифрові водяні знаки (ЦВЗ).** Математична модель та структурна схема	**ЛР8.** Метод стеганографії LSB для зображень формату .bmp. Приховування	Опрацювання теоретичного матеріалу, підготовка до до	9	Літ.: [1] с.9-55; [5] с.143-177.

		стеганографічної системи ЦВЗ. Застосування ЦВЗ.	інформації в форматі Jpeg	виконання ЛР8		
16	2	**Атаки на стеганосистеми.** Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків (ЦВЗ). Класифікація атак на стеганосистеми цифрових відеознаків (ЦВДЗ). Атаки, спрямовані на видалення ЦВДЗ. Геометричні атаки. Атаки проти протоколу, що використовується**.**	**ПЗ8.** Розробка стеганографічної програми з використанням ШІ	Опрацювання теоретичного матеріалу, виконання ПЗ8, підготовка до захисту ЛР8. Підготовка до тестування.	11	Літ.: [1] с.43-65; [3] с.137-199; [5] с.143-177; [5] с.269-320; [6] с.134-183; [8] с.253-256;
17	2	**Методи протидії атакам на стеганосистеми.** Статистичний стегааноаналіз та протидії. Практична оцінка стійкості стеганосистем. Теоретико-складнісний підхід до оцінки стійкості стеганосистем. Напрями підвищення захищеності стеганосистем від статистичних атак. Імітостійкість системи передачі приховуваних повідомлень.	Тестування. Підсумкове заняття	Опрацювання теоретичного матеріалу	8	Літ.: [1] с.66-88, с.373-421; [2] с.85-113; [3] с.221-243; [5] с.339-361; [6] с.183-199; [8] с.253-259.

* лекції проводяться по 2 години., практичні заняття проводяться раз в два тижні по 2 години
** лабораторні роботи проводяться раз у два тижні по 4 годин.

Політика дисципліни.

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні роботи згідно з розкладом, не запізнюватися на заняття, самостійну роботу та інші домашні завдання виконувати відповідно до графіка. Пропущену лабораторну роботу студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ (http://khnu.km.ua/root/files/01/06/03/006.pdf).

Оцінювання результатів навчання студентів

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестування	
Тема	1-4	1-4	
Ваговий коефіцієнт	0,8	0,2	

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд

студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в он-лайн режимі в модульному середовищі для навчання.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
1	***2***
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно".

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи

з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання		
A	4,75–5,00	5		*Відмінно* – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		*Добре* – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		*Добре* – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		*Задовільно* – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		*Задовільно* – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2		*Незадовільно* – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		*Незадовільно* – необхідна серйозна подальша робота і повторне вивчення дисципліни

Питання для самоконтролю студентів

1. Напрямки криптографії та стеганографії.
2. Структурна схему типової стегосистеми цифрових водяних знаків.
3. Класи систем вбудовування цифрових водяних знаків
4. Поняття і типи контейнера стегосистеми.
5. Типи цифрових водяних знаків.
6. Класифікація систем цифрової стеганографії.
7. Потенційні сфери застосування стеганографії.
8. Принцип вбудовування повідомлень в незначущі елементи контейнера-зображення.
9. Протоколи стеганографії з відкритим ключем.
10. Протоколи стеганографії виявлення цифрових водяних знаків з нульовим знанням.
11. Способи впровадження в контейнер бітів цифрових водяних знаків.
12. Переваги та недоліки мають стегоконтейнери зображень.
13. Класифікація методів стеганографічного захисту.
14. Методи текстової стеганографії.
15. Приховування даних у частотній області зображень.
16. Блокове приховування.
17. Метод Коха-Жао та його модифікації.
18. Метод Хсу – Ву. Метод Фрідріха.
19. Приховування даних у нерухомих зображеннях за допомогою методів розширення спектра.
20. Властивості людського зору потрібно враховувати при побудові стегоалгоритмів.
21. Узагальнена схему впровадження даних в зображення..
22. Високорівневі властивості людського зору.
23. Принципи стиснення і відновлення зображень.
24. Принципи приховування даних в просторовій області зображень.

25. Алгоритм стегокодера із застосуванням широкосмугових сигналів.
26. Стегоалгоритми на основі лінійного вбудовування даних в зображення.
27. Модель «сліпої» стегосистеми.
28. Принцип вбудовування інформації із застосуванням модуляції індексу квантування.
29. Принцип застосування в схемі модуляції індексу квантування дізерізованого квантувателя.
30. Алгоритми вбудовування ЦВЗ з використанням скалярного квантування.
31. Алгоритми вбудовування ЦВЗ з використанням векторного квантування.
32. Вимоги до стегосистем вбудовування інформації в аудіосигнали.
33. Блок-схема стегокодера і стегодекодера вбудовування інформації в аудіосигнал методом кодування з розширенням спектру.
34. Принцип вбудовування інформації модифікацією фази аудіосигналу.
35. Приховування даних у просторій множині аудіосигналу
36. Приховування даних у частотній множині аудіосигналу (фазове кодування).
37. Приховування даних в аудіосигналах за допомогою методів розширення спектра.
38. Класифікація атак на стеганосистеми.
39. Практична оцінка стійкості стеганосистем.
40. Принцип вбудовування інформації за рахунок зміни часу затримки луна-сигналу.
41. Методи маскування ЦВЗ.
42. Малювання геометричних об’єктів.
43. Модельно-видові перетворення.
44. Матеріали і висвітлення.
45. Текстурування та робота з пікселями.
46. Шейдери та робота з ними.

Методичне забезпечення

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі на сторінці дисципліни https://msn.khnu.km.ua/course/view.php?id=6189

Рекомендована література

Основна

№	Назва	Режим доступу
1.	Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. – 558 с.	https://drive.google.com/file/d/1LrFZzBnglycIvmfWOcxe58WgikyXcont/view?usp=sharing
2.	Steganography Techniques for Digital Images / Edited by Abid Yahya. – Springer International Publishing AG, 2019. – 131 p	https://www.pdfdrive.com/steganography-techniques-for-digital-images-d176365799.html
3.	Digital Watermarking and Steganography: Fundamentals and Techniques / Edited by Frank Y. Shih. – Taylor & Francis Group, 2017. – 293 p	https://www.pdfdrive.com/digital-watermarking-and-steganography-fundamentals-and-techniques-d185303952.html
4.	Баранник В. В. Основы теории структурно-комбинаторного стеганографического кодирования: монография / В. В. Баранник, А. Э. Бекиров, Д. В. Баранник. – Х. : ХНУРЕ, 2017. - 256 с	https://openarchive.nure.ua/handle/document/5921
5.	Handbook of Image-Based Security Techniques / Editors: Shivendra Shivani, Suneeta Agarwal, Jasjit S. Suri. – Taylor & Francis Group, 2022. – 443 p	https://www.pdfdrive.com/handbook-of-image-based-security-techniques-d187816749.html
6.	Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.	http://repository.hneu.edu.ua/handle/123456789/2289
7.	Комп'ютерна графіка : конспект лекцій з курсу «Комп'ютерна графіка» / Укладач: Скиба О.П. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2019. – 88 с.	http://elartu.tntu.edu.ua/bitstream/lib/27541/1/КОНСПЕКТ%20ЛЕКЦІЙ%20комп%20графіка.pdf
8.	Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.	https://drive.google.com/file/d/1jACvCh2O4duJOYA3uLUID8cdVf2EFSWU/view?usp=sharing
9.	Introduction to Visual Computing. Core Concepts in Computer Vision, Graphics, and Image Processing / Editors: Aditi Majumder, M. Gopi. – Taylor & Francis Group, 2018. – 393 p	https://www.pdfdrive.com/introduction-to-visual-computing-core-concepts-in-computer-vision-graphics-and-image-processing-d158449761.html
10.	Mathematical Structures For Computer Graphics / Edited by Steven J. Janke. – John Wiley & Sons, Inc, 2015. – 410 p	https://www.pdfdrive.com/mathematical-structures-for-computer-graphics-d189113226.html

Додаткова

11.	Impractical Python Projects. Playful Programming Activities to Make You Smarter/ Edited by Lee Vaughan. – San Francisco, 2019. – 478 p.	https://www.pdfdrive.com/impractical-python-projects-playful-programming-activities-to-make-you-smarter-d183876561.html

12.	Multimedia Security: Watermarking, Steganography, and Forensics / Edited by Frank Y.Shih**.** – Taylor & Francis Group, 2013**.** – 411 p.	https://www.pdfdrive.com/multimedia-security-watermarking-steganography-and-forensics-d187856096.html
13.	Pro Processing for Images and Computer Vision with OpenCV Solutions for Media Artists and Creative Coders / Edited by Bryan WC Chung**.** – Academy of Visual Arts, Kowloon Tong, Hong Kong, 2017**.** – 301 p	https://www.pdfdrive.com/pro-processing-for-images-and-computer-vision-with-opencv-d54672394.html
14.	Secure Digital Documents Using Steganography and QR Code dissertation / Edited by Mohamed Sameh Hassanein. – Department of Computer Science, Brunel University, 2014. – 191 p	https://bura.brunel.ac.uk/bitstream/2438/10619/1/FulltextThesis.pdf
15.	Efficient And Robust Video Steganography Algorithms for Secure Data Communication; dissertation / Edited by Ramadhan J. Mstafa. – The school of engineering University of Bridgeport Connecticut, 2017. – 165 p	https://scholarworks.bridgeport.edu/xmlui/bitstream/handle/123456789/1964/EFFICIENT%20AND%20ROBUST%20VIDEO%20STEGANOGRAPHY%20ALGORITHMS%20FOR%20SECURE%20DATA%20COMMUNICATION.pdf?sequence=1&isAllowed=y
16.	Image Steganography Based on Discrete Wavelet Transform and Enhancing Resilient Backpropogation Neural Network dissertation / Edited by Ahmed Shihab Ahmed AL- Naima. – Middle East University Amman- Jordan, 2015. – 113 p	https://www.pdfdrive.com/image-steganography-based-on-discrete-wavelet-transform-and-enhancing-resilient-d46673622.html
17.	HTML Steganography Algorithms and Detection Methods dissertation / Edited by Iman Thannoon Sedeeq**.** – the University of Liverpool, 2018**.** – 140 p	https://cgi.csc.liv.ac.uk/~frans/CurrentResearch/Thessi/imanSedeeq_2018-6-12.pdf
18.	Глібко О. А. Комп'ютерна графіка. Створення моделей та сцен у тривимірному середовищі : навч . посіб. / О. А. Глібко, М. О. Максимова, І. П .Гречка. –Харків : НТУ «ХПІ», 2018. –132 с.	https://drive.google.com/file/d/1hZU8M1fsa4tvgGjnT7WZFeWG3TCMYOwg/view?usp=sharing
19.	Основи двовимірної комп'ютерної графіки : навчальний посібник / О. О. Сафронова, К. В. Донець. – К. : КНУТД, 2016. – 175 с.	https://er.knutd.edu.ua/bitstream/123456789/6598/2/20161212_103.pdf
20.	Пічугін М.Ф. Комп'ютерна графіка: навч. посіб. / М.Ф. Пічугін, І.О. Канкін, В.В. Вороьніков – К.: «Центр учбової літератури», 2013. – 346 с..	https://drive.google.com/file/d/1DPd7Zs1aKu-7aFQL_srAsh1Ntkn_Xkbz/view?usp=sharing
21.	Маценко В.Г. Комп'ютерна графіка: Навчальний посібник. – Чернівці: Рута, 2009 – 343 с.	https://drive.google.com/file/d/1JnFnTUOtGYa-lML3wskgpypUjfTnahHX/view?usp=sharing
22.	Муляр І. В. Шифрування звуку методом представлення його у вигляді спектрограми / І. В. Муляр, Є. С. Лєнков, Л. В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2016. – Вип. 51. – С. 177–185.	http://nbuv.gov.ua/UJRN/Znpviknu_2016_51_26
23.	Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.	https://drive.google.com/file/d/1-ZmFMuTkL5VnBgh1bXNfD6nODchxWI4U/view?usp=sharing
24.	Муляр І.В. Ітераційно-геометричний метод для стійкого перцептуального хешування зображення / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун // Вісник Хмельницького	http://elar.khnu.km.ua/jspui/handle/123456789/8940

	національного університету. Технічні науки. – 2020. – № 1. – С. 76–79	
25.	Муляр І.В. Використання розподілених хеш-таблиць надання доступу до хмарних сервісів / Ю. П. Кльоц, І. В. Муляр, В. М. Чешун, О. В. Бурдюг // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2020. – Вип. 67. – С. 85–95	http://elar.khnu.km.ua/jspui/handle/123456789/9620
26.	Муляр І.В. Симетрична криптосистема з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування / В. А. Анікін, В. М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 6. – С. 12-16.	http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: https://msn.khnu.km.ua/course/view.php?id=6189
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.