ПЛАН
ЛАБОРАТОРНИХ ЗАНЯТЬ

з дисципліни «ПРОГРАМНІ МЕТОДИ ОРГАНІЗАЦІЇ ПРИХОВАНОГО КАНАЛУ ЗВ'ЯЗКУ»

лабораторні заняття, годин – 30
Викладач – Кобозєва А.А.

Обсяг в годинах	Назва та стислий зміст практичного заняття	Мета роботи
ЗМІСТОВИЙ МОДУЛЬ 1. ВЛАСТИВОСТІ СТЕГАНОСИСТЕМ. ПОНЯТТЯ СТІЙКОСТІ СТЕГАНОСИСТЕМИ		
2	Заняття 1. **Метод модифікації найменшого значущого біта, його алгоритмічні реалізації.** 1. LSB-matching. 2. LSB-replacement. 3. Недоліки і переваги різних алгоритмічних реалізацій LSB-метода.	Вміти оцінювати результати стеганоперетворення цифрового зображення з точки зору збереження надійності сприйняття, стійкості до атак проти вбудованого повідомлення. Встановити на практиці шляхом обчислювального експерименту недоліки і переваги LSB-matching і LSB-replacement алгоритмічних реалізацій LSB-методу. Зіставити теоретично очікувані та практично отримані результати відносно властивостей алгоритмічних реалізацій LSB-методу.
6	Заняття 2,3,4. **Програмні реалізації стеганографічних алгоритмів, що використовують для вбудови додаткової інформації просторову та області перетворення контейнера.** 1. Переваги просторової області зображення для організації стеганоперетворення. 1.1. Практичне оцінювання обчислювальних витрат переходів «просторова область — область перетворення», «область перетворення — просторова область» у цифровому зображенні. 1.2. Практичне оцінювання обчислювальної похибка переходів «просторова область — область перетворення», «область перетворення — просторова область» для цифрового зображення. 2. Стеганоперетворення просторової області контейнера (метод псевдовипадкового інтервалу, метод псевдовипадкового переставлення, метод заміни палітри, метод квантування зображення та ін..) 3. Стеганоперетворення частотної області зображення (метод відносної заміни коефіцієнтів дискретного косинусного	Навчитися реалізовувати алгоритмічно різноманітні стеганоперетворення, порівнювати результати стеганоперетворення, виконані різними стеганоалгоритмами, використовуючи різноманітні критерії . Розвити навички прийняття рішень щодо вибору стеганоалгоритму з врахуванням вимог, що висуваються до формованого ним стеганоповідомлення. Оцінити переваги просторової області контейнера для її використання при стеганоперетворенні. Перевірити на практиці обмеженість/необмеженість області застосування конкретного стеганографічного алгоритму. Навчитися давати теоретичне обгрунтування отриманим практично результатам. Перевірити ефективність розглянутих стеганоалгоритмів для кольорових цифрових зображень, зображень в градаціях сірого, бінарних зображень.

	перетворення, метод Бенгама-Мемона-Юнга та ін..). 4. Методи розширення частотного спектру. 5. Статистичні методи. 6. Структурні методи.	
ЗМІСТОВИЙ МОДУЛЬ 2. ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СТЕГАНОСИСТЕМИ		
2	Заняття 5. **Метод підвищення стійкості стеганоалгоритму до атак проти вбудованого повідомлення, заснований на рішенні систем лінійних рівнянь.** 1. Практична реалізація зменшення числа обумовленості задачі декодування додаткової інформації. 2. Обчислювальна складність методу SYSTEMA та шляхи її зменшення.	Розуміти основні математичні принципи підвищення ефективності декодування стеганографічних методів. На прикладі метода модифікації найменшого значущого біта вміти підвищувати ефективність стеганографічного алгоритму шляхом зменшення числа обумовленості задачі декодування переданої інформації. На прикладі методу SYSTEMA розвивати здатність удосконалювати існуючі методи з врахуванням показнику їх стійкості до атак проти вбудованого повідомлення.
2	Заняття 6. **Експериментальне дослідження теоретичних основ забезпечення стійкості стеганоалгоритму до атак проти вбудованого повідомлення.** 1. Аналіз збурень сингулярних чисел і сингулярних векторів блоків матриці цифрового зображення для стеганоалгоритмів, оцінка стійкості яких до атак проти вбудованого повідомлення є відомою. 2. Співставлення для використаних алгоритмів теоретичних і практичних результатів їх стійкості.	Розуміти сутність теоретичних основ забезпечення стійкості стеганоалгоритму до атак проти вбудованого повідомлення. Навчитися застосовувати теоретичний підхід до практичної оцінки стійкості стеганоалгоритму до атак проти вбудованого повідомлення. Навчитися аналізувати отримані експериментальні оцінки властивості стеганоалгоритму та зіставляти їх с теоретично очікуваними, обґрунтовувати, пояснювати можливе неспівпадіння.
4	Заняття 7,8. **Стеганографічні перетворення, стійкі до стиску з втратами.** 1. Експериментальне дослідження стійкості до стиску з втратами сучасних стеганографічних алгоритмів. 2. Стиск зображення з використанням малорангових апроксимацій матриці (блоків матриці) зображення. Стеганоалгоритми, що використовують малорангові апроксимації контейнера. 3. Сучасні стеганоалгоритми, стійкі до стиску з втратами, які використовують для стеганоперетворення область сингулярного розкладання матриці (блоків матриці) контейнера. 4. Сучасні стеганоалгоритми, стійкі до стиску з втратами, які використовують для стеганоперетворення просторову область контейнера.	Розуміти сутність забезпечення стійкості стеганоалгоритму до стиску з втратами, незалежність існуючих достатніх умов стійкості від області стеганоперетворення (просторової, області перетворення). Вміти досліджувати довільний стеганоалгоритм на стійкість до стиску з втратами, аналізувати кількісні параметри стійкості. Вміти виконувати порівняльну оцінку стійкості кількох стеганоалгоритмів до стиску. Вміти давати пропозиції щодо підвищення стійкості існуючих стеганоалгоритмів до стиску.

	5. Порівняння стійкості стеганоалгоритмів, які використовують для стеганоперетворення просторову та області перетворення зображення контейнера.	
ЗМІСТОВИЙ МОДУЛЬ 3. ТРИЄДИНА ЗАДАЧА СТЕГАНОГРАФІЇ ТА МЕТОДИ ЇЇ ВИРІШЕННЯ		
4	Заняття 9,10. **Підвищення пропускної спроможності прихованого каналу зв'язку.** 1. Загальні принципи забезпечення високої пропускної спроможності прихованого каналу зв'язку. 2. Порівняння стійких до атак проти вбудованого повідомлення стеганоалгоритмів, що здійснюють стеганоперетворення в області сингулярного розкладання матриці контейнера, з точки зору величини прихованої пропускної спроможності. 3. Модифікації базового методу, стійкого до атак проти вбудованого повідомлення, що здійснює стеганоперетворення в просторовій області контейнера. 4. Порівняльний аналіз отриманих модифікацій.	Розуміти теоретичну сутність забезпечення високої пропускної спроможності прихованого каналу зв'язку. Вміти оцінювати величину пропускної спроможності прихованого каналу зв'язку. Вміти обґрунтовано обирати стеганографічний метод/алгоритм, який забезпечує достатню пропускну спроможність прихованого каналу зв'язку. Вміти досліджувати існуючий стеганоалгоритм для надання пропозицій по його удосконаленню з точки зору підвищення пропускної спроможности прихованого каналу зв'язку.
4	Заняття 11,12. **Розробка стеганоперетворень цифрового зображення, які забезпечують одночасну перевірку автентичності й цілісності переданої інформації**. 1. Вимоги до стеганографічних методів, що вирішують триєдину задачу стеганографії. 2. Забезпечення належності множині цілих чисел коефіцієнтів дискретного косинусного перетвореня блоків матриці зображення. 3. Використання методу модифікації найменшого значущого біта для організації стеганоперетворення.	Розуміння необхідності забезпечення можливості перевірки цілісності та автентичності переданої сучасним прихованим каналом зв'язку інформації. Вміти аналізувати збурення повного набору параметрів цифрового зображення для виявлення результатів порушення його цілісності. Практична перевірка доцільності забезпечення належності множині цілих чисел коефіцієнтів дискретного косинусного перетвореня блоків матриці зображення при організації стеганоперетворення в прихованому каналі зв'язку.
6	Заняття 13,14,15. **Організація перевірки автентичності й цілісності переданої прихованим каналом зв'язку інформації з/без наявності контейнера.** 1. Організація перевірки автентичності додаткової інформації для стеганографічного методу, який вирішує триєдину задачу стеганографії, що вимагає наявності контейнера.	Розуміння необхідності забезпечення можливості перевірки цілісності та автентичності переданої сучасним прихованим каналом зв'язку інформації. Вміти обґрунтовувати, передбачати область застосування стеганографічних алгоритмів, що вирішують триєдину задачу стеганографії. Вміти програмно реалізовувати, досліджувати властивості, проводити порівняльний аналіз стеганометодів що

	2. Стеганографічний метод, що вирішує триєдину задачу стеганографії з використанням контейнера для організація автентифікації додаткової інформації. 3. Організація автентифікації додаткової інформації без наявності контейнера. 4. Стеганографічний метод, що вирішує триєдину задачу стеганографії без використання контейнера для організація автентифікації додаткової інформації. 5. Удосконалення стеганографічного методу двухетапного декодування, заснованого на рішенні систем лінійних алгебраїчних рівнянь. 6. Стійкий до атак проти вбудованого повідомлення стеганометод, заснований на сингулярному розкладанні матриці.	вирішують триєдину задачу стеганографії.