Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Гринько Іллі Андрійовича*

академічної групи *125-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне впровадження інформації в цифрові зображення за допомогою систем нечіткого висновку*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Гринько Іллі Андрійовичу* **академічної групи** *125-19-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне впровадження інформації в цифрові зображення за допомогою систем нечіткого висновку*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз основних положень цифрової стеганографії, принципів приховування даних в зображеннях, основ нечіткої логіки і систем нечіткого висновку, а також існуючих підходів до вбудовування інформації з використанням нечіткої логіки.	25.02.2023 – 31.03.2023
Розділ 2	Розробка підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку та оцінка його ефективності.	01.04.2022 – 12.05.2023
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	13.05.2022 – 09.06.2023

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Гринько І.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 74 с., 16 рис., 2 табл., 4 додатки, 41 джерело.

Об’єкт розробки – цифрові зображення.

Предмет розробки – підхід до стеганографічного впровадження інформації у цифрові зображення із використанням нечіткої логіки.

Мета кваліфікаційної роботи – дослідження алгоритмів нечіткої логіки для вбудовування інформації у JPEG-зображення.

Наукова новизна результатів полягає у тому, що використання систем нечіткого висновку на основі алгоритмів Мамдані, Сугено, Цукамото і Ларсена дозволяє виконувати стеганографічне вбудовування інформації в цифрові зображення формату JPEG.

У першому розділі проаналізовано основні положення цифрової стеганографії, принципи приховування даних в зображеннях, основи нечіткої логіки і систем нечіткого висновку, а також існуючі підходи до вбудовування інформації в нерухомі зображення з використанням нечіткої логіки.

У спеціальній частині роботи запропоновано підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.

ДИСКРЕТНЕ КОСИНУСНЕ ПЕРЕТВОРЕННЯ, СИСТЕМА НЕЧІТКОГО ВИСНОВКУ, КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ, ЦИФРОВЕ ЗОБРАЖЕННЯ, ІНВАРІАНТНІСТЬ КОЛЬОРУ, ДИХРОМАТИЧНЕ ВІДБИТТЯ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

ABSTRACT

Explanatory note: p. 74, fig. 16, tab. 2, 4 additions, 41 sources.

The object of development is digital images.

The subject of development is an approach to steganographic introduction of information into digital images using fuzzy logic.

The purpose of the qualification work is to study algorithms of fuzzy logic for embedding information in JPEG images.

The scientific novelty of the results lies in the fact that the use of fuzzy inference systems based on Mamdani, Sugeno, Tsukamoto and Larsen algorithms allows steganographic embedding of information into JPEG digital images.

The first chapter analyzes the basic principles of digital steganography, the principles of hiding data in images, the basics of fuzzy logic and fuzzy inference systems, as well as existing approaches to embedding information in still images using fuzzy logic.

In a special part of the work, an approach to steganographic embedding of information in digital images using fuzzy inference systems is proposed and its effectiveness is evaluated. Based on the results of the research, conclusions were made regarding the solution to the problem.

In the economic section, calculations of capital costs, economic effect and payback period of capital investments are performed using the proposed solutions.

DISCRETE COSINE TRANSFORM, FUZZY INFERENCE SYSTEM, COMPUTER STEGANOGRAPHY, DIGITAL IMAGING, COLOR INVARIANCE, DICHROMATIC REFLECTANCE, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДКП – Дискретне косинусне перетворення;

ІС – Інформаційна система;

НЗБ – Найменш значущий біт;

ПЗ – Програмного забезпечення;

ЗСЛ – Зорова система людини;

ЦВЗ – Цифровий водяний знак;

DRM – Dichromatic Reflection Model – Модель дихроматичного відбиття;

MSE – Mean Squared Error – Середньоквадратичне відхилення;

PSNR – Peak Signal-to-Noise Ratio – Співвідношення між максимумом можливого значення сигналу і потужністю шуму, що спотворює значення сигналу.

ЗМІСТ

ВСТУП

Сучасні комп'ютерні технології обробки даних дозволили суттєво підвищити рівень інформаційної та кібербезпеки безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. Як відомо, на відміну від криптографічного захисту інформації, стеганографічні підходи намагаються в першу чергу приховати сам факт існування конфіденційної інформації [1-5].

Взагалі стеганографія давніша за криптографію, але активно розвиватись вона почала лише з появою комп'ютерних технологій. Саме в цей період стеганографія з мистецтва перетворилась на науку. Методи, які приховують інформацію в потоках оцифрованих сигналів і реалізуються на базі комп'ютерної техніки та програмного забезпечення в рамках окремих обчислювальних систем, корпоративних або глобальних мереж, становлять предмет вивчення досить молодої, але достатньо наукомісткої дисципліни – комп'ютерної стеганографії [1-5].

Наразі комп'ютерна стеганографія – самостійний науковий напрямок інформаційної безпеки, що вивчає проблеми створення компонент приховуваної інформації у відкритому інформаційному середовищі, яке може бути сформовано обчислювальними системами та мережами. Особливістю стеганографічного підходу є те, що він не передбачає прямого оголошення факту існування захищуваної інформації. Ця обставина дозволяє в рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати деякі важливі задачі захисту інформації ряду прикладних галузей.

Комп'ютерна стеганографія використовує результати з криптографії, теорії інформації, теорії складності, теорії ймовірностей і математичної статистики, загальної теорії оптимальних алгоритмів, цифрової обробки сигналів та зображень, теорії швидких ортогональних перетворень і т.п. Стеганографічні методи володіють унікальними властивостями, що робить їх незамінними при вирішенні певних задач захисту [1].

Більшість цифрових методів ґрунтуються, з одного боку, на тому, що файли, які не потребують абсолютної точності, можна дещо видозмінювати без втрати функціональності, а з іншого – на відсутності спеціального інструментарію або нездатності органів чуття людини надійно розрізняти незначні зміни в таких файлах.

Комп'ютерна стеганографія розвивається в декількох напрямах. Так, серед стеганографічних систем виділяють системи прихованого передавання даних, цифрових водяних знаків, ідентифікаційних номерів («відбитків пальців»). Завдання будь-якої стеганографічної системи – розмістити певне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити різниці між модифікованим контейнером та оригінальним методами візуального або статистичного аналізу.

Цифровим контейнером може слугувати будь-який файл чи потік даних. Через свою надлишковість найчастіше цифровими контейнерами виступають зображення, аудіо- чи відеосигнали [6-22].

В останні роки з'явилось багато публікацій щодо використання для стеганографічного вбудовування інформації різних методів систем штучного інтелекту (нейронних мереж, нечіткої логіки, еволюційних алгоритмів, агентських алгоритмів оптимізації) [23-28]. Цей напрямок наразі є дуже перспективним, оскільки зазначені інтелектуальні алгоритми реалізують надійні, недорогі, оптимальні та адаптивні рішення для задач приховування даних.

Взагалі актуальність методів систем штучного інтелекту при вирішенні різних питань в галузі кібербезпеки обумовлена здатністю інтелектуальних методів розв'язувати оптимізаційні задачі, які погано формалізуються, а також використанням для моделювання ефективних і універсальних апроксиматорів.

Таким чином, дослідження, розробка і вдосконалення підходів до вбудовування інформації у цифрові зображення із використанням методів систем штучного інтелекту наразі є актуальною задачею.

Метою роботи є дослідження алгоритмів нечіткої логіки для вбудовування інформації у JPEG-зображення.

Постановка задачі:

• проаналізувати основні положення цифрової стеганографії та принципи приховування даних в зображеннях;

• провести аналіз основ нечіткої логіки і систем нечіткого висновку, а також існуючих підходів до стеганографічного вбудовування інформації в нерухомі зображення з використанням нечіткої логіки;

• запропонувати підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Основні положення комп'ютерної стеганографії

1.1.1 Поняття стеганографічної системи

Стеганографічна система (стеганосистема) – це сукупність Σ= (X, M, K, Y, E, D) пустих контейнерів X, повідомлень M, ключів K, заповнених контейнерів Y і перетворень E та D, що їх пов'язують (алгоритмів вбудовування та вилучення) [1-5, 29-30].

Контейнер (носій) – це нетаємна інформація, в якій будуть приховані конфіденційні дані (повідомлення). В комп'ютерній стеганографії контейнером може слугувати будь-який файл чи потік даних. В силу своєї надлишковості найчастіше цифровими контейнерами виступають зображення, аудіо чи відеосигнали.

Повідомленням називається таємна інформація, наявність якої необхідно приховати.

Стеганоключ – елемент стеганосистеми, який параметризує алгоритми вбудовування і вилучення, та відомий тільки відправнику і одержувачу стеганоконтейнера. Стеганоключ зокрема може визначати область вбудовування (часова/просторова чи частотна), базис частотного розкладу, правила розбиття контейнера на сегменти, силу вбудовування, індекси задіяних коефіцієнтів, точки квантування, кодову книгу, вектор розширення та інше.

Пустим називають контейнер, який не містить прихованого стеганографічними методами повідомлення. Контейнер, що містить приховану інформацію, називають заповненим або стеганоконтейнером, або стеганограмою, або стего.

Отже, згідно рис. 1.1, де представлено узагальнену модель функціонування стеганосистеми, відправник ініціює роботу алгоритму вбудовування (вкраплення, впровадження) повідомлення M у контейнер X за

допомогою ключа K_{emb}. Результатом роботи алгоритму є стеганоконтейнер Y, що буде передаватися по відкритому каналу зв'язку.

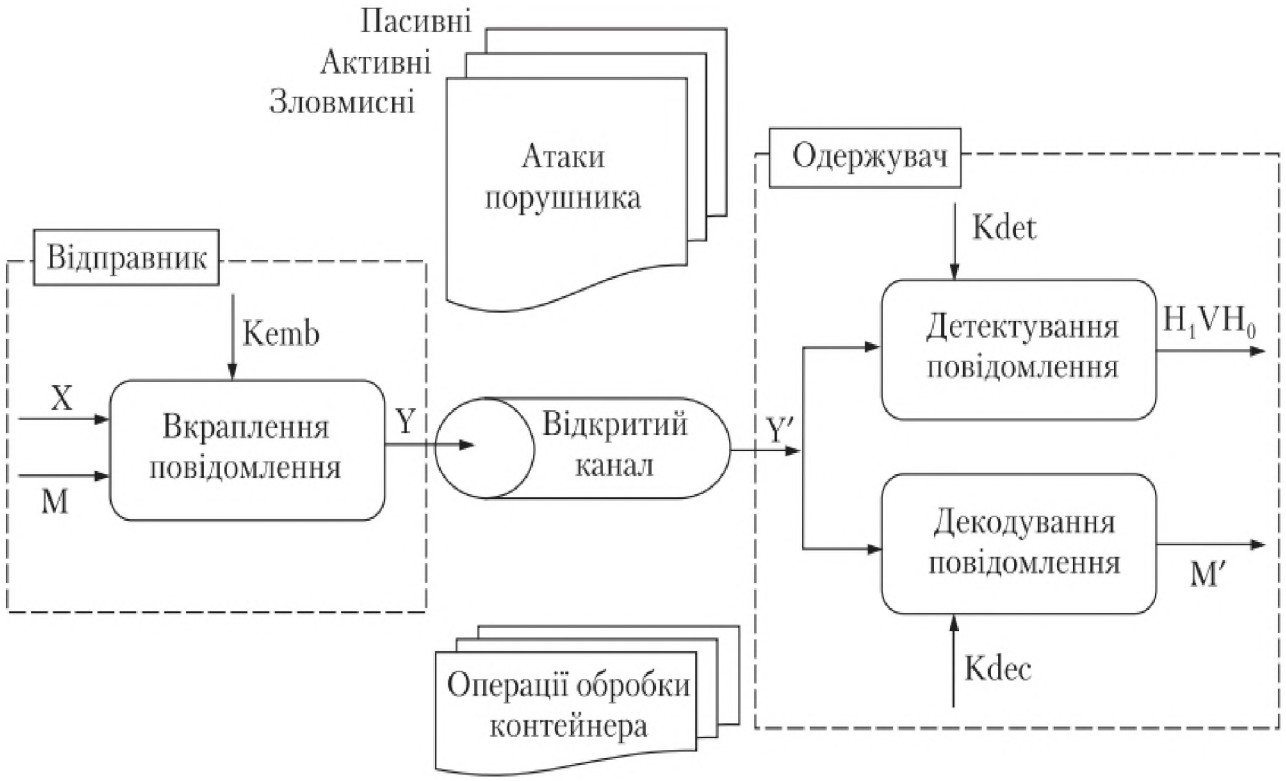


Рисунок 1.1 – Узагальнена модель функціонування стеганографічної системи [1-2]

Канал прихованої передачі повідомлення у контейнері, який утворюється всередині відкритого каналу, має назву стеганографічного каналу або стеганоканалу.

Першочергові вимоги для практичної придатності стеганосистем залежать від умов їх функціонування, що зокрема включають в себе множину можливих атак. В загальному випадку інформація, яка передається по стеганоканалу, може бути спотворена операціями обробки контейнера – так званими ненавмисними атаками.

Також потрібно враховувати, що крім легальних користувачів – відправника та одержувача, при експлуатації стеганосистеми можлива

наявність третього учасника інформаційної взаємодії – порушника, який здійснює навмисні атаки.

Порушник може мати можливість тільки спостерігати за інформацією у каналі зв'язку без можливості її змінювати, в такому випадку його називають пасивним.

Порушник може впливати на стеганоконтейнер з метою знищення вбудованого повідомлення, тоді він зветься активним. В деяких випадках знищення повідомлення можливе «всліпу», тобто за допомогою певного набору модифікацій контейнера, без знання методу й алгоритму вбудовування та секретів системи.

Порушник, мета якого достовірно оцінити таємний ключ і тим самим отримати можливість виконувати функції легального користувача, тобто створювати фальшиві стеганоконтейнери, є зловмисним.

Слід зазначити, що процес вилучення повідомлення легальним одержувачем може включати в себе детектування повідомлення, тобто підтвердження однієї з двох гіпотез H_1 чи H_0 про наявність або відсутність повідомлення в отриманому контейнері Y', та декодування повідомлення, тобто відновлення його змісту (див. рис. 1.1).

Задача будь-якої стеганографічної системи – вбудувати повідомлення в контейнер таким чином, щоб сторонній спостерігач не зміг помітити різниці між оригінальним контейнером та модифікованим.

1.1.2 Види стеганографічних систем

Наразі розділяють наступні види стеганографічних систем [1-3, 40]:

- системи прихованої передачі даних;
- системи цифрових водяних знаків (ЦВЗ);
- системи ідентифікаційних номерів;
- стеганосистеми заголовків.

Системи прихованої передачі даних застосовуються для організації таємної комунікації. Вони відрізняються від усіх інших тим, що у цьому випадку оригінальний вміст контейнера не грає ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача впровадженого повідомлення. Разом із тим потрібно обов'язково враховувати, що факт відправлення контейнера від відправника до одержувача не повинен виглядати дивним, а також не повинно спостерігатися помітних відхилень контейнера від норми.

Основна мета систем прихованої передачі даних – приховати наявність стеганоканалу, унеможливити розрізнення пустих і заповнених контейнерів без знання ключа. Для таких систем звичайно вважається, що контейнер не підлягає спотворенням в процесі його передачі по каналу зв'язку ($Y'=Y$), тому що таємна комунікація відбувається через відкритий канал інформаційно-комунікаційної мережі, наприклад, Інтернет, що забезпечує відсутність спотворень інформації при її передачі.

У першу чергу для цих систем характерна наявність пасивного порушника, який намагається виявити факт експлуатації стеганосистеми й прочитати таємну інформацію. Також слід зазначити, що пропускна здатність стеганоканалу, під якою розуміють відношення розміру контейнера до розміру повідомлення, для систем прихованої передачі даних повинна бути суттєво вищою, ніж для інших видів систем.

Слід зауважити, що задача прихованої передачі даних на практиці може трансформуватися в задачу їх прихованого зберігання. Тобто існують застосування, де роль відправника і одержувача виконує одна й та ж особа, але це не приводить до змін в принципах побудови та функціонування відповідних стеганографічних систем.

Системи ЦВЗ актуальні для широкого ряду практичних застосувань, таких як завадостійка аутентифікація аудіо та візуальних даних (зокрема контроль цілісності знімків камер спостереження, записів телефонних розмов), аутентифікація власника даних (захист авторських прав), аутентифікація

джерела даних, контроль розповсюдження та ідентифікація копій, контроль телевізійного та радіомовлення, контроль копіювання і т.д.

Стеганосистеми ЦВЗ мають на увазі два об'єкти інформаційного інтересу – вбудоване повідомлення та контейнер. Їх основна мета – зберегти цілісність вбудованого повідомлення після певного ряду можливих модифікацій стеганоконтейнера. Характерними атаками виступають активні та зловмисні атаки порушника, а також ненавмисні атаки, спричинені обробкою контейнера. Водяний знак має порівняно невеликий розмір, що дозволяє вбудувати його так, щоб забезпечити стійкість до ненавмисних та активних атак. Експлуатація системи ЦВЗ в більшості випадків не приховується, у той же час можливість читання вбудованих даних нелегальним користувачем, як правило, небажана, оскільки надає йому знання для подальших активних або зловмисних атак.

Процедуру вбудовування ЦВЗ в контейнер також прийнято називати маркуванням, а сигнал, що містить ЦВЗ – маркованим.

Системи ідентифікаційних номерів можна розглядати як частинний випадок систем ЦВЗ. Ідентифікаційні номери – це унікальні ЦВЗ, які, як правило, впроваджуються в набір копій цифрового контейнера з метою їх подальшої ідентифікації та контролю розповсюдження.

За допомогою стеганосистем ідентифікаційних номерів можна визначити, який з легальних користувачів контейнера порушує правила його використання. Небезпечною та специфічною для даного виду стеганосистем є атака змовою (коаліцією): декілька користувачів, кожен з яких отримав свій екземпляр контейнера з вбудованим у нього унікальним ідентифікаційним номером, стають порушниками та, погоджено діючи, намагаються побудувати досить близьку до оригіналу оцінку пустого контейнера, що зберігає його функціональність, але не містить ідентифікаційної інформації. На практиці це актуально, наприклад, для задач захисту авторських прав та прав власності на CD/DVD диски з музикою чи фільмами і т.п.

Стеганосистеми заголовків відрізняються від усіх попередніх у першу чергу відсутністю порушника. Їх основна мета – прихована анотація даних,

зберігання різнорідної інформації у єдиному цілому так, щоб різні типи даних не заважали одні одним з точки зору комфорту їх сприйняття. На практиці за допомогою таких систем зручно організовувати швидкий пошук по мультимедійним базам даних, анотування медичних знімків, музики, зображень тощо. Стеганосистеми заголовків будуються на основі методів і алгоритмів впровадження ЦВЗ із забезпеченням стійкості до операцій обробки контейнера у каналі, що не пов'язані з функціонуванням стеганосистеми.

Зазвичай стеганосистема будується так, щоб забезпечити певний компроміс її базових характеристик, до яких відносяться невідчутність, стійкість, безпеку, пропускну здатність створюваного стеганоканалу та обчислювальну складність реалізації. Першочергові вимоги для практичної придатності стеганосистем залежать від умов їх функціонування, що зокрема включають у себе множину можливих атак.

Взаємозв'язок між видами стеганосистем та характерними для них атаками наведено в табл. 1.1.

Таблиця 1.1 – Взаємозв'язок між видом стеганосистеми та характерними для неї атаками

Характерні атаки	Вид стеганосистеми
Ненавмисні	Системи ЦВЗ, ідентифікаційних номерів, заголовків
Пасивні	Системи прихованої передачі даних
Активні	Системи ЦВЗ, ідентифікаційних номерів
Зловмисні	Системи прихованої передачі даних, ЦВЗ, ідентифікаційних номерів

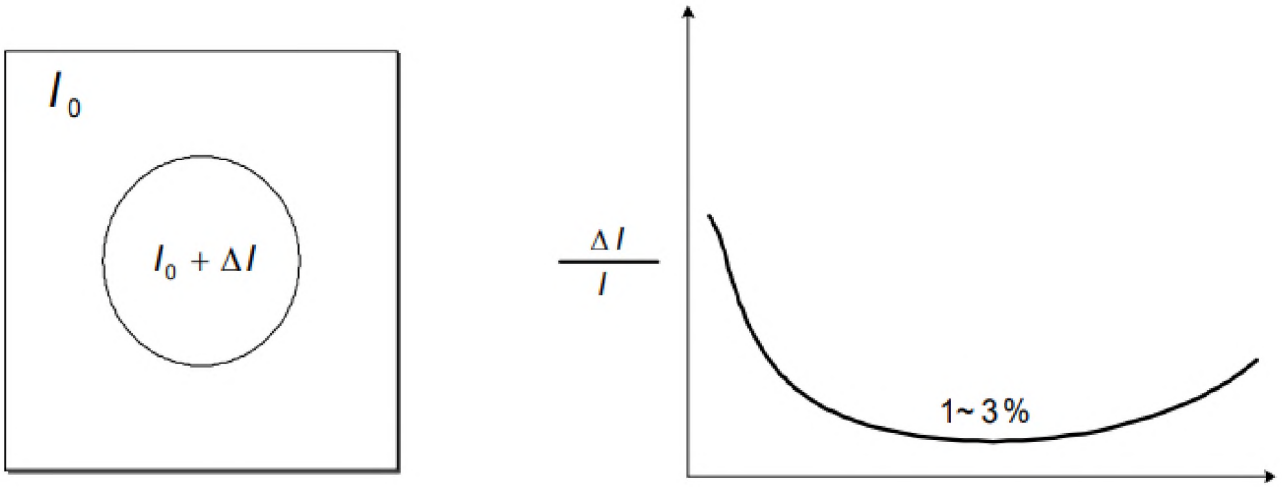
1.1.3 Властивості зорової системи людини, що використовуються при приховуванні даних

Властивості зорової системи людини (ЗСЛ) можна розділити на дві групи: низькорівневі («фізіологічні») і високорівневі («психофізіологічні»). Аж до

середини 1990-х рр. XX ст. дослідники брали до уваги, головним чином, низькорівневі властивості зору. В останні роки намітилася тенденція побудови стеганоалгоритмів з обліком і високорівневих характеристик ЗСЛ [40].

Найбільш важливі низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні – це чутливість до зміни яскравості зображення, частотна чутливість і ефект маскування.

Чутливість до зміни яскравості визначається у такий спосіб. Випробуваному показують деяку однотонну картинку (рис. 1.2,*а*). Після того, як око адаптувалося до її освітленості I, поступово змінюють яскравість навколо центральної плями. Зміну освітленості ΔI продовжують доти, доки вона не буде виявлена. На рис. 1.2,*б* показана залежність мінімального контрасту ΔI/I від яскравості I (для зручності поміняли звичне розташування осей).



а б

Рисунок 1.2 – Властивості зорової системи людини

Як видно з рис. 1.2, для середнього діапазону зміни яскравості контраст приблизно постійний, тоді як для малих і більших яскравостей значення порога нерозрізненості зростає. Було встановлено, що $\Delta I \approx 0.01-0.03\, I$ для середніх значень яскравості [40].

Результати новітніх досліджень суперечать «класичній» точці зору і показують, що при малих значеннях яскравості ЗСЛ поріг нерозрізненості зменшується, тобто ЗСЛ більш чутлива до шуму в цьому діапазоні.

Частотна чутливість ЗСЛ проявляється у тому, що людина набагато більш сприйнятлива до низькочастотного, ніж до високочастотного шуму. Це пов'язане з нерівномірністю амплітудно-частотної характеристики системи зору людини. Експериментально її можна визначити за допомогою того ж досвіду, що і при яскравій чутливості. Але цього разу в центральному квадраті змінюються просторові частоти доти, доки зміни не стануть помітними.

Елементи ЗСЛ розділяють відеосигнал, що надходить, на окремі компоненти. Кожна складова збуджує нервові закінчення ока через ряд підканалів. Вирізнювані оком компоненти мають різні просторові й частотні характеристики, а також різну орієнтацію (горизонтальну, вертикальну, діагональну). У випадку одночасного впливу на око двох компонентів з подібними характеристиками збуджуються ті самі підканали. Це приводить до ефекту маскування, що полягає в збільшенні порога виявлення відеосигналу в присутності іншого сигналу, що володіє аналогічними характеристиками. Тому адитивний шум набагато помітніше на гладких ділянках зображення, ніж на високочастотних, тобто в останньому випадку спостерігається маскування. Найбільш сильно ефект маскування проявляється, коли обидва сигнали мають однакову орієнтацію й місце розташування.

Можна показати, що частотна чутливість тісно пов'язана з яскравісною. Відомо також і вираз для визначення порога маскування на основі відомої яскравісної чутливості, що дозволяє знайти метрику перекручування зображення, що враховує властивості ЗСЛ. Такого типу математичні моделі добре розроблені для випадку квантування коефіцієнтів дискретного косинусного перетворення зображення, тому що саме воно застосовується в стандарті JPEG.

Ефект маскування в просторовій множині може бути пояснений шляхом побудови стохастичних моделей зображення. При цьому зображення

представляється у вигляді марківського випадкового поля, розподіл імовірностей якого підкоряється, наприклад, узагальненому гауссівському закону.

Таким чином, можна запропонувати таку узагальнену схему впровадження даних у зображення:

1. Виконати фільтрацію зображення за допомогою орієнтованих смугових фільтрів. При цьому одержимо розподіл енергії по частотно-просторових компонентах.

2. Обчислити поріг маскування на основі знання локальної величини енергії.

3. Масштабувати значення енергії впроваджуваного ЦВЗ у кожному компоненті так, щоб воно було менше порога маскування.

Слід зазначити, що багато алгоритмів вбудовування інформації так чи інакше використовують цю схему.

Високорівневі властивості ЗСЛ поки рідко враховуються при побудові стеганоалгоритмів. Їх відмінністю від низькорівневих є те, що ці властивості проявляються «удруге», обробивши первинну інформацію від ЗСЛ, мозок видає команди на її «підналаштовування» під зображення.

Основні високорівневі властивості ЗСЛ:

1. Чутливість до контрасту. Висококонтрастні ділянки зображення, перепади яскравості привертаються до себе значну увагу.

2. Чутливість до розміру. Більші ділянки зображення "помітніші" менших за розміром. Причому існує поріг насичення, коли подальше збільшення розміру не істотне.

3. Чутливість до форми. Довгі й тонкі об’єкти привертають більшу увагу, ніж круглі однорідні.

4. Чутливість до кольору. Деякі кольори (наприклад, червоний) "помітніші" інших. Цей ефект підсилюється, якщо тло заднього плану відрізняється від кольору фігур на ньому.

5. Чутливість до місця розташування. Людина схильна у першу чергу розглядати центр зображення.

6. Люди звичайно уважніше до зображень переднього плану, ніж заднього.

7. Якщо на зображенні є люди, у першу чергу людина зверне свою увагу на них. На фотографії людина звертає першочергову увагу на особу, очі, рот, руки.

8. Чутливість до зовнішніх подразників. Рух очей спостерігача залежить від конкретної обстановки, від отриманих їм перед переглядом або під час його інструкцій, додаткової інформації.

1.1.4 Стеганографічні методи приховування даних

Більшість методів комп'ютерної стеганографії базуються на наступних двох принципах [4]. Перший принцип полягає у тому, що файли, які не потребують абсолютної точності, можуть бути видозмінені (певною мірою) без втрати функціональності. Другий принцип полягає у тому, що органи відчуття людини не здатні розрізнити зміни в модифікованих таким чином файлах та відсутній спеціальний інструментарій для цього.

Відповідно до існуючих методів комп'ютерної стеганографії, запропоновано класифікацію, зображену на рис. 1.3.

За способом вибору контейнера вирізняють сурогатні, селективні та конструюючі методи. В сурогатних методах стеганографії можливість вибору контейнера відсутня, обирається перший наявний контейнер, який, у більшості випадків, не є оптимальним. Селективні методи дозволяють обирати оптимальний контейнер. Для цього генерують велику кількість альтернативних контейнерів, певна хеш-функція яких порівнюється із хеш-функцією повідомлення. В конструюючих методах стеганографії контейнер генерується сам.

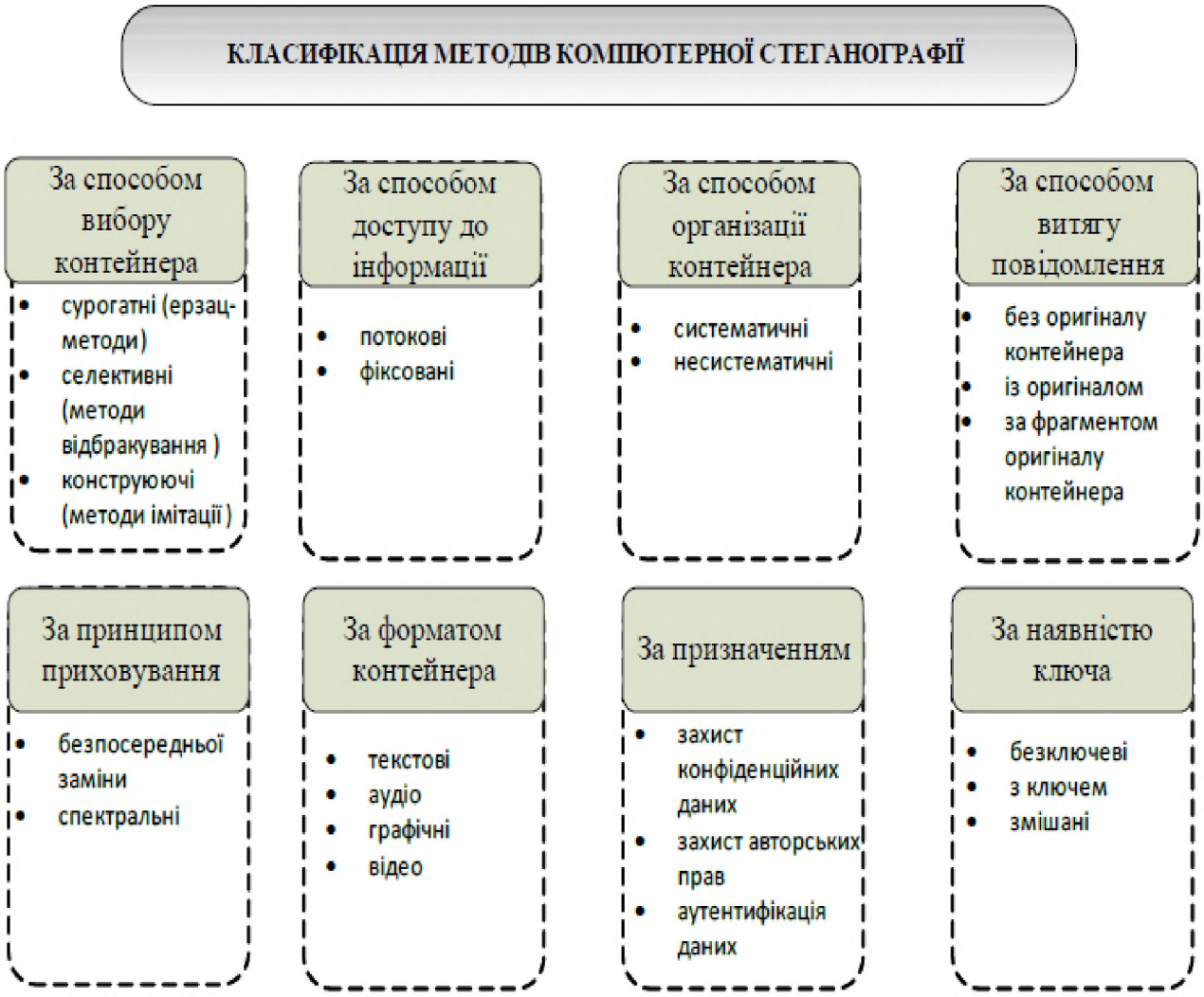


Рисунок 1.3 – Класифікація методів комп’ютерної стеганографії

За способом доступу до інформації, що приховується, розрізняють методи для потокових та фіксованих контейнерів.

За способом організації контейнера бувають систематичні та несистематичні методи комп’ютерної стеганографії. У систематичних методах можна точно сказати, де в контейнері знаходяться інформаційні біти, а де – біти шуму. У несистематичних методах для виділення повідомлення доводиться обробляти всю стеганограму.

За принципом приховування даних є методи безпосередньої заміни та спектральні методи. Методи безпосередньої заміни використовують надлишок інформації у малозначних частинах контейнера для вбудовування

повідомлення. Спектральні ж методи використовують спектральні представлення елементів контейнера для приховування повідомлення. В основному в стеганографії використовується саме надлишковість файлу-контейнера.

Слід також виділити методи, що використовують спеціальні властивості форматів файлів:

– зарезервовані поля форматів файлів, які зазвичай заповнюються нулями і не враховуються програмами;

– спеціальне форматування даних (зсув слів, речень, абзаців або шаблонний вибір символів);

– використання незадіяних частин оптичних та магнітних носіїв.

За типами контейнера виділяють стеганографічні методи із текстовими, графічними, аудіо- та відеофайлами-контейнерами.

За наявністю ключа виділяють безключові, з ключем та змішані стеганосистеми. Для функціонування безключової стеганосистеми, крім алгоритму графічного перетворення, відсутня необхідність в додаткових даних, на зразок стеганоключа. Таким чином, безпека безключової стеганосистеми базується тільки на секретності використовуваних стеганографічних перетворень.

Ключова стеганосистема поділяється на системи з відкритим та закритим ключами.

Система з відкритим ключем передбачає наявність закритого каналу зв'язку для передачі стеганоключа і забезпечує вищий рівень захисту повідомлення порівняно з безключовою, однак потребує затрат на передачу ключа. Стеганосистема з відкритим ключем працює по аналогії з криптографічними алгоритмами, однак потрібно зазначити, що стеганоключ не шифрує дані, а приховує місце їх вбудовування в контейнері.

Змішані стегосистеми використовують як відкритий, так і секретний ключ.

1.1.5 Принцип стиснення зображень JPEG

Наразі найбільшу практичну цінність представляють методи та алгоритми, що працюють зі стисненими зображеннями, оскільки в мережі Інтернет, а також у локальних комп'ютерних мережах цифрові зображення зберігаються і передаються насамперед у стисненому вигляді. Під стисненням розуміється зменшення числа біт, потрібних для цифрового представлення зображень. При цьому найпопулярнішим стандартом стиснення був і залишається JPEG, побудований на основі дискретного косинусного перетворення (ДКП) [1-5, 29-30].

На рис. 1.4 показано як відбувається стиснення зображень в алгоритмі JPEG.

Рисунок 1.4 – Етапи стиснення зображень згідно алгоритму JPEG

На першому етапі відбувається перетворення кольорової моделі RGB в іншу YUV. У зв'язку з тим, що більша частина візуальної інформації, сприймаюча людським оком, складається з компонентів яскравості Y, а до кольорових компонент U і V менш чутлива, то відкидаючи частину кольорових даних можна забезпечити стиснення зображення.

На другому етапі – дискретизація YUV кольорів, відбувається проріджуванням кольорових компонентів з коефіцієнтом 2. В результаті чого отримується в 2 рази стиснене зображення без будь-якого візуального погіршення.

Далі відбувається розбиття зображення на невеликі блоки розміром 8×8, над яким потім відбувається перетворення за допомогою ДКП. Тут відбувається деяка втрата інформації в зв'язку з неможливістю точного перетворення.

На четвертому етапі в результаті ДКП перетворення отримується матриці частотних коефіцієнтів. Для зменшення їх розрядності використовують матриці квантування. За допомогою яких більшість високочастотних та середньо частотних коефіцієнтів перетворюється на 0.

Далі відбувається зигзагоподібні сканування матриці для об'єднання нульових коефіцієнтів в групи. Потім – групове кодування, в результаті чого кожний не нульовий коефіцієнт вектора записується в вигляді пари двох чисел, де перше число це кількість нулів перед цим числом, а друге – значення даного елемента вектора.

На останньому етапі застосовується метод одноразового кодування Хафмана. За цим методом спочатку аналізується вся послідовність символів і часто повторювальним серіям біт ставиться у відповідність короткі маркери.

На кожному етапі компресії за ДКП може бути реалізоване приховування інформації.

Схема стеганографічного вбудовування додаткової інформації у процесі стиснення цифрового зображення методом JPEG представлена на рис. 1.5.

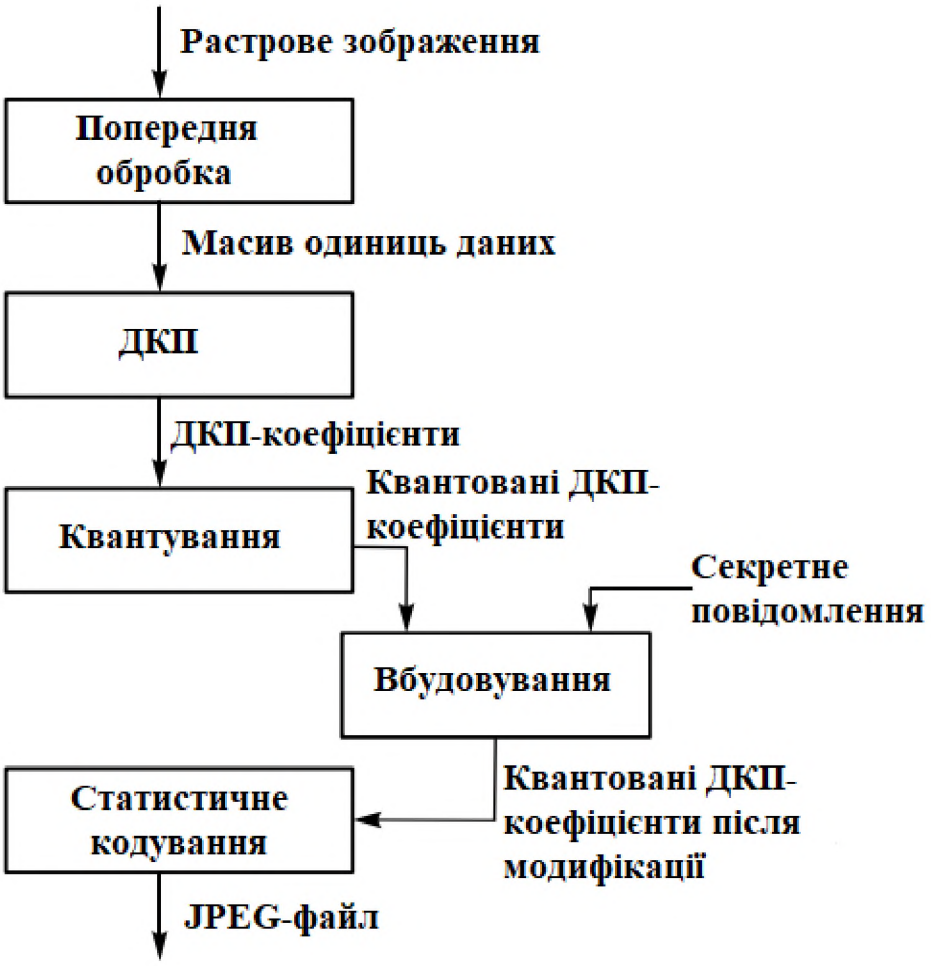


Рисунок 1.5 – Схема вбудовування інформації у процесі стиснення зображення методом JPEG

1.2 Існуючі підходи до стеганографічного вбудовування інформації в нерухомі зображення з використанням нечіткої логіки

Як вже зазначалось у вступі, в останні роки з’явилось багато публікацій щодо використання для стеганографічного вбудовування інформації різних методів систем штучного інтелекту (нейронних мереж, нечіткої логіки, еволюційних алгоритмів, агентських алгоритмів оптимізації). Цей напрямок наразі є дуже перспективним, оскільки зазначені інтелектуальні алгоритми реалізують надійні, недорогі, оптимальні та адаптивні рішення задач приховування даних.

Так, в роботі [6] запропоновано підхід для приховування секретного зображення в зображенні-контейнер, використання якого покращує візуальну якість стего-зображення, забезпечуючи при цьому велику ємність для вбудовування. В рамках підходу, як класифікатор використовується система нечіткого логічного висновку Мамдані, який приймає локальні особливості субобластей зображення-контейнера як чіткі вхідні значення та створює семантичні концепції, що відповідають корисному навантаженню субобластей зображення.

В роботі [7] запропоновано метод приховування секретних даних шляхом перетворення їх у нечітку область. У цьому методі для кожного нечіткого пікселя застосовуються дві методики, засновані на обробці зображень, такі як виявлення країв і виділення характеристик текстури. Потім для приховування інформації в іншому зображенні використовується метод стеганографічної заміни на основі найменшого значущого біта (НЗБ) [17-18].

Застосування алгоритму НЗБ у графічному процесорі (Graphics Processing Unit – GPU) було запропоновано у роботі [8]. В ній було запропоновано проводити виконання обчислень, паралельних за своєю природою до одного пікселя. Це можна зробити за допомогою нового методу передачі повідомлення та спільної пам'яті, щоб зменшити загальний час, потрібний для виконання стеганоалгоритму.

Основний підхід до обчислення похідних кольорових зображень полягає в окремому обчисленні похідних каналів і їх додаванні для отримання остаточного градієнта кольору. Однак похідні кольорового краю можуть бути в протилежних напрямках для окремих кольорових каналів. Таким чином, підсумовування похідних на канал відкине кореляцію між кольоровими каналами. Як рішення проблеми протилежного вектору у роботі [9] було запропоновано тензор кольору, отриманий від структурного тензора, для обчислення градієнта кольору. Адаптація тензора призводить до різноманітних локальних характеристик зображення, таких як детектори кіл, оцінка кривизни тощо [10-13]. Отже, використання, методів та прийомів комбінування похідних

різних кольорових каналів для обчислення структур локального зображення наразі є актуальним.

В роботі [14] запропоновано метод приховування секретних даних за допомогою нечіткого алгоритму зіставлення пікселів для підвищення надійності прихованих даних.

В роботі [15] запропоновано вдосконалений алгоритм для приховування секретних даних за допомогою концепції нечіткої логіки. Основна ідея цього методу полягає в використанні комбінації генетичного алгоритму і характеристик матриці суміщення рівнів сірого (Grey Level Co-Occurrence Matrix – GLCM). Використовуються такі характеристик текстури як кореляція, енергія, контраст і однорідність.

В роботах [16-17] запропоновано методи, засновані на нечіткій логіці, для приховування інформації в інших даних. У зазначених методах вбудовування інформації здійснюється в домен на основі нечіткої логіки. Перевагами автори вказують менші обчислювальні витрати порівняно з іншими методами перетворення домену.

В роботі [18] запропоновано новий метод приховування зображення за допомогою техніки нечіткого кодування та декодування. Нечіткий кодер стискає кожен блок у вигляді секретної інформації в менший блок і використовує стеганографію на основі моделі, щоб приховати все повідомлення від зображення носія. Основна перевага цього методу полягає у тому, що він забезпечує більш високу швидкість вбудовування даних і підвищену робастність до атак.

В роботі [19] запропоновано метод, заснований на поєднанні алгоритму нечіткої кластеризації С-середніх і класифікації на основі методу опорних векторів для реалізації стеганографії в зображеннях. Запропонована ними модель створює здатність приховувати секретні повідомлення, які можна конвертувати у зорову систему людини.

В роботі [20] запропоновано нову схему стеганографії на основі методу найменшого значущого біта для використання гібридного методу детектора

краю на основі нечіткої логіки. Цей метод є кращим у порівнянні з відомими (наприклад методом Фрідріха), а також не детектується системами на основі статистичного стеганоаналізу.

Слід зазначити, що кожен з представлених методів [6-20] має свої недоліки. З аналізу інших робіт [21-22, 29-33] було встановлено, що використання для стеганографічного впровадження інформації (секретних зображень) в цифрові зображення інших методів штучного інтелекту (насамперед нейронних мереж) знижувало якість стегозображення, у порівнянні з методами, які використовували нечітку логіку. До того ж, чим більше був розмір вбудовуваного зображення, тим гірша була якість стегозображення. Отже, слід віддати перевагу дослідженню і використовуванню алгоритмів нечіткої логіки для задач стеганографічного вбудовування інформації (секретних зображень) у цифрові зображення.

Також відсутні роботи, у яких досліджується використання усіх систем нечіткого висновку для стеганографічного впровадження інформації у нерухомі зображення. Таким чином, у подальшій частині роботи, запропоновано дослідити використання алгоритмів нечіткої логіки (Мамдані, Сугено, Цукамото, Ларсена) для стеганографічного вбудовування інформації у цифрові зображення.

1.3 Нечітка логіка

Теорія нечітких множин (fuzzy sets theory) веде свій початок з 1965 р., коли професор Лотфі Заде (Lotfi Zadeh) з університету Берклі опублікував свою основну роботу «Fuzzy Sets» в журналі «Information and Control». Ця робота заклала основи моделювання інтелектуальної діяльності людини і стала початковим поштовхом у розвитку нової математичної теорії [23-29].

Прикметник «fuzzy», який можна перекласти як «нечіткий», «розмитий», «пухнастий», введено в назву нової теорії з метою дистанціювання від

традиційної чіткої математики і аристотелевої логіки, що оперують з чіткими поняттями: «належить – не належить», «істина – неправда».

Слід зазначити, що концепція нечіткої множини зародилася у Заде як «незадоволеність математичними методами класичної теорії систем, яка змушувала домагатися штучної точності, недоречної в багатьох системах реального світу, особливо в так званих гуманістичних системах, що включають людей».

Л. Заде розширив класичне поняття множини (по Г. Кантору), допустивши, що характеристична функція (функція належності елемента множині) може приймати будь-які значення в інтервалі [0; 1], а не тільки значення 0 або 1. Такі множини були названі їм нечіткими (fuzzy). Він визначив також ряд операцій над нечіткими множинами і запропонував узагальнення відомих методів логічного висновку modus ponens і modus tollens.

Ввівши поняття лінгвістичної змінної, і допустивши, що в якості її значень (термів) виступають нечіткі множини, Л. Заде створив апарат для опису процесів інтелектуальної діяльності, включаючи нечіткість і невизначеність виразів.

Поняття нечіткої множини – це спроба математичної формалізації нечіткої інформації для побудови математичних моделей. В основі цього поняття лежить уявлення про те, що елементи, які складають дану множину та володіють загальною властивістю, можуть володіти цією властивістю у різній мірі й, отже, належати до даної множини із різною мірою. У разі такого підходу вислови про те, що «елемент належить даній множині» втрачають сенс, оскільки необхідно вказати «наскільки сильно» цей елемент задовольняє властивостям даної множини.

1.3.1 Нечіткі множини

Підхід до формалізації поняття нечіткої множини складається в узагальненні поняття належності [23-29].

В теорії класичних множин існує декілька способів завдання множини. Одним з них вважається завдання за допомогою характеристичної функції, яка визначається таким чином (рис. 1.6) :

$$\chi(x) = \begin{cases} 1, x \in A, \\ 0, x \notin A. \end{cases} \tag{1.1}$$

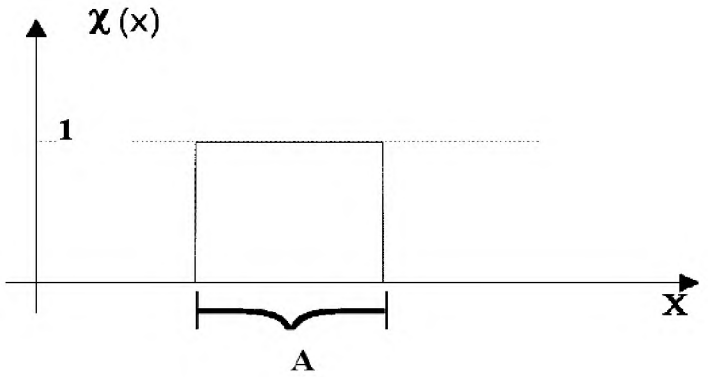
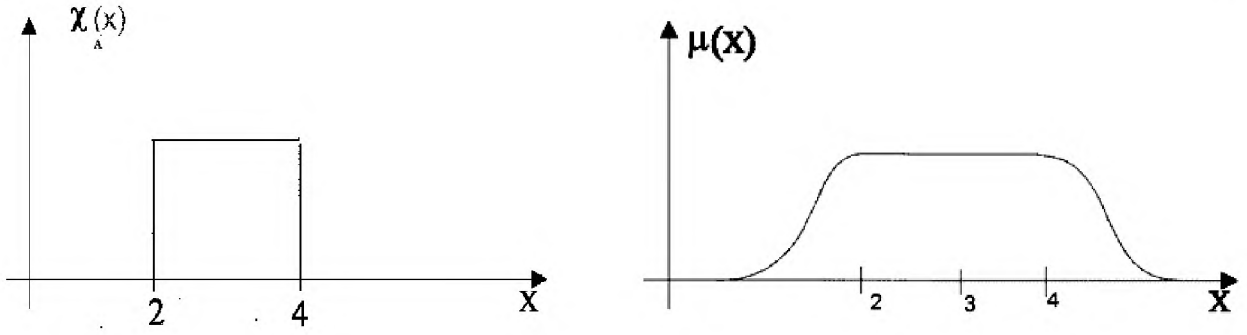


Рисунок 1.6 – Характеристична функція чіткої множини

Нехай E – універсальна множина, з елементів якого утворюються інші множини, що розглядаються в даному класі задач, наприклад, множини всіх цілих чисел, множини всіх гладких функцій, тощо. Характеристична функція множини $A \subseteq E$ – це функція, значення якої вказують, чи є елемент $x \in E$ елементом множини A. Особливістю цієї функції – в бінарному характері її значень.

Приклад. Для множини A чисел $2 \le x \le 4$ характеристична функція має вигляд, представлений рис. 1.7,*а*.

З точки зору характеристичної функції нечіткі множини є природним узагальненням звичайних множин, коли ми відмовляємося від бінарного характеру цієї функції і припускаємо, що вона може приймати будь-які значення на відрізку [0,1]. Множина значень x, на якому визначена функція належності, отримало назву нечіткої множини.



а *б*

Рисунок 1.7 – Приклад характеристичної функції чіткої (*а*) і нечіткої (*б*) множини

Нехай E – універсальна множина, x – елемент E, а R – деяка властивість. Нечітка підмножина відрізняється від звичайної тим, що для елементів x з E немає однозначної відповіді «так-ні» щодо властивості R.

У зв'язку з цим, нечітка підмножина A універсальної множини E, елементи якої задовольняють властивості R, визначається як множина впорядкованих пар

$$A=\{\mu_A(x)/x\}, \qquad (1.2)$$

де $\mu_A(x)$ – характеристична функція належності, що приймає значення в деякій цілком впорядкованій множині M (наприклад, M=[0,1]).

Функція належності вказує ступінь (або рівень) належності елемента x підмножині A. Множина M є множиною належностей. Якщо M={0,1}, то нечітка підмножина A може розглядатися як звичайна або чітка множина.

Тепер припущення, що «x приблизно лежить в межах від 2 до 4» (рис. 1.7,а), може бути представлено відповідною функцією належності (рис. 1.7,б).

1.3.2 Нечіткі та лінгвістичні змінні

При описі об’єктів і явищ за допомогою нечітких множин використовуються поняття нечіткої та лінгвістичної змінних [23-29].

Нечітка змінна характеризується набором (α, X, A), де

α – найменування змінної;

X – універсальна множина (область визначення α);

A – нечітка множина на X, що описує обмеження (тобто $\mu_A(x)$) на значення нечіткої змінної α.

Лінгвістична змінна характеризується набором (β, T, X, G, M), де

β – найменування лінгвістичної змінної;

T – множина її значень (терм-множина), що являє собою найменування нечітких змінних, областю визначення кожної з яких є множина X. Множина T є базовою терм-множиною лінгвістичної змінної;

G – синтаксична процедура, що дозволяє оперувати елементами терм-множини T, зокрема, генерувати нові терми (значення). Множина $T \cup G(T)$, де G(T) – множина згенерованих термів, є розширеною терм-множиною лінгвістичної змінної;

M – семантична процедура, що дозволяє перетворити кожне нове значення лінгвістичної змінної, утворене процедурою G, в нечітку змінну, тобто сформувати відповідну нечітку множину.

Слід зазначити, що для того, щоб уникнути великої кількості символів: символ β використовують як для назви самої змінної, так і для всіх її значень; а також користуються одним і тим же символом для позначення нечіткої множини і його назви, наприклад терм «Молодий», який є значенням лінгвістичної змінної β=«вік», одночасно є і нечіткою множиною M («Молодий»).

Присвоєння кількох значень символам передбачає, що контекст дозволяє вирішити можливі невизначеності.

1.3.3 Нечіткі висновки

Механізм нечітких висновків зазвичай використовується в експертних і керуючих системах. У своїй основі він має базу знань, що формується

фахівцями-експертами предметної області у вигляді сукупності нечітких предикатних правил виду [23-29]:

$$\begin{gathered}\text{Правило 1: якщо x є } A_1\text{, тоді y є } B_1,\\ \text{Правило 2: якщо x є } A_2\text{, тоді y є } B_2,\\ \ldots\\ \text{Правило N: якщо x є } A_n\text{, тоді y є } B_n,\end{gathered} \tag{1.3}$$

де x – вхідна змінна, y – змінна висновку (ім'я для значення даних, яке буде обчислено); A і B – функції належності, визначені відповідно на x і y.

Знання експерта $A \rightarrow B$, що відбиває нечітке причинне відношення передумови і висновків, можна назвати нечітким відношенням R:

$$R = A \rightarrow B, \tag{1.4}$$

де "→" називають нечіткою імплікацією.

Відношення R можна розглядати як нечітку підмножину прямого добутку $X \times Y$ повної множини передумов X і висновків Y.

Таким чином, процес отримання нечіткого результату виведення B' з використанням спостереження A' і знання $A \rightarrow B$ можна відобразити наступним чином:

$$B' = A' \; R = A' \; (A \rightarrow B). \tag{1.5}$$

Таким чином, у загальному випадку нечіткий логічний висновок здійснюється в наступні етапи.

1. Нечіткість (введення нечіткості, фаззифікація, fuzzification). Функції належності, що визначені на вхідних змінних, застосовуються до їх фактичних значень, для того щоб визначити ступінь істинності кожної передумови кожного правила.

2. Логічний висновок. Обчислення значення істинності для передумов кожного правила застосовується до висновків кожного правила. Це призводить до однієї нечіткої підмножини, що буде призначена кожній змінній висновку для кожного правила. За правила логічного висновку, зазвичай, використовуються тільки операції min (мінімум) або prod (множення). При операції min функція належності виведення «відсікається» по висоті, що

відповідає обчисленому ступеню істинності передумови правила (нечітка логічна операція «І»). При операції prod функція належності виведення масштабується за обчисленим ступенем істинності передумови правила.

3. Композиція. Всі нечіткі підмножини, призначені до кожної змінної висновку (у всіх правилах), об'єднуються разом, щоб сформувати одну нечітку підмножину для кожної змінної виводу. При подібному об'єднанні зазвичай використовуються операції max (максимум) або sum (сума). При операції max комбінований висновок нечіткої підмножини конструюється як поточний максимум за всіма нечітким підмножинами (нечітка логічна операція «АБО»). У разі операції sum комбінований висновок нечіткої підмножини конструюється як поточна сума за всіма нечіткими підмножинами, призначеними змінній виводу правилами логічного висновку.

4. Приведення до чіткості (дефаззифікація, defuzzification) використовується для перетворення нечіткого набору висновків в чітке число.

Слід зазначити, що вибір конкретних способів реалізації окремих етапів нечіткого висновку визначається тим або іншим алгоритмом нечіткого висновку.

1.3.4 Алгоритм Мамдані

Одним із перших алгоритмів, який знайшов застосування в системах нечіткого висновку є алгоритм Мамдані (Mamdani), що був запропонований у 1975 р. англійським математиком Е. Мамдані як метод для керування поршневим двигуном. Цей алгоритм, заснований на нечіткому логічному висновку, дозволив уникнути надмірно великого обсягу обчислень і був позитивно оцінений фахівцями [23-30].

Суть алгоритму Мамдані полягає у наступному. Припустимо, що в базі знань містяться тільки два нечітких правила виду:

$$\begin{aligned} &\text{Правило 1: якщо } x \in A_1 \text{ і } y \in B_1, \text{ тоді } z \in C_1, \\ &\text{Правило 2: якщо } x \in A_2 \text{ і } y \in B_2, \text{ тоді } z \in C_2, \end{aligned} \qquad (1.6)$$

де x, y – вхідні змінні, z – змінної виводу, A_1, A_2, B_1, B_2, C_1, C_2 – деякі задані функції належності. При цьому, на основі наведеної інформації та чітких значень x_0, y_0 необхідно визначити чітке значення z_0.

Алгоритм Мамдані може бути описаний наступним чином (рис. 1.8):

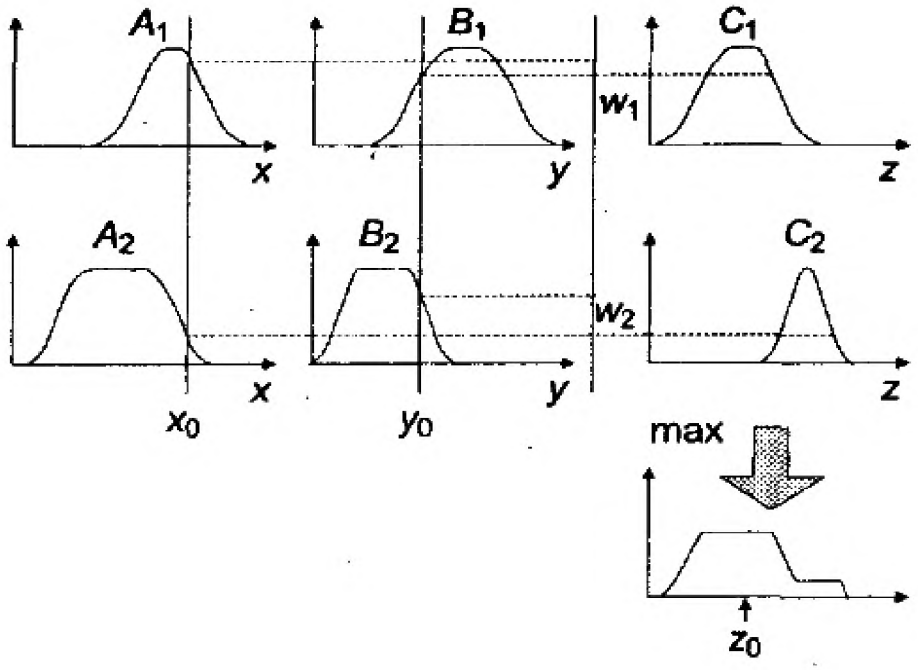


Рисунок 1.8 – Ілюстрація нечіткого висновку Мамдані

Етап 1. Нечіткість: знаходяться ступені істинності для передумов кожного правила: $A_1(x_0)$, $A_2(x_0)$, $B_1(y_0)$, $B_2(y_0)$.

Етап 2. Нечіткий висновок. Знаходяться рівні «відсікання» для передумов кожного з правил (з використанням операції min): $\alpha_1 = A_1(x_0) \wedge B_1(y_0)$, $\alpha_2 = A_2(x_0) \wedge B_2(y_0)$, де $\wedge$ – операція логічного мінімуму (min).

Далі знаходяться «усічені» функції належності: $C_1'(z) = (\alpha_1 \wedge C_1(z))$, $C_2'(z) = (\alpha_2 \wedge C_2(z))$.

Етап 3. Композиція: з використання операції максимум (max) проводиться об'єднання знайдених усічених функцій, що призводить до отримання підсумкової нечіткої підмножини для змінної виходу з функцією належності:

$$\mu_{\Sigma}(z) = C(z) = C_1'(z) \vee C_2'(z) = (\alpha_1 \wedge C_1(z)) \vee (\alpha_2 \wedge C_2(z)), \qquad (1.7)$$

де $\vee$ – операція логічного максимуму (max).

Етап 4. Приведення до чіткості (для знаходження z_0) проводиться, як правило, центроїдним методом: чітке значення вихідної змінної визначається як центр ваги для кривої $\mu_{\Sigma}(z)$:

$$z_0 = \frac{\int_{\Omega} z\mu_{\Sigma}(z)dz}{\int_{\Omega} \mu_{\Sigma}(z)dz}. \qquad (1.8)$$

1.3.5 Алгоритм Сугено

Суть алгоритму Сугено полягає у наступному. Припустимо, що в базі знань містяться тільки два нечітких правила виду [23-29, 31]:

Правило 1: якщо x є A_1 і y є B_1, тоді $z_1 = a_1 x + b_1 y$,

Правило 2: якщо x є A_2 і y є B_2, тоді $z_2 = a_2 x + b_2 y$. (1.9)

Алгоритм Сугено (Sugeno) може бути описаний таким чином (рис. 1.9):

Етап 1. Знаходяться ступені істинності для передумов кожного правила: $A_1(x_0)$, $A_2(x_0)$, $B_1(y_0)$, $B_2(y_0)$.

Етап 2. Знаходяться рівні «відсікання» для передумов кожного з правил (з використанням операції min): $\alpha_1 = A_1(x_0) \wedge B_1(y_0)$, $\alpha_2 = A_2(x_0) \wedge B_2(y_0)$,

а також індивідуальні виходи правил: $z_1^* = a_1 x_0 + b_1 y_0$, $z_2^* = a_2 x_0 + b_2 y_0$.

Етап 3. Визначається чітке значення вихідної змінної:

$$z_0 = \frac{\alpha_1 z_1^* + \alpha_2 z_2^*}{\alpha_1 + \alpha_2}. \qquad (1.10)$$

Наведене представлення відноситься до алгоритму Сугено 1-го порядку.

Разом з вищеописаним використовується також алгоритм Сугено 0-го порядку, у якому правила записані у формі:

Правило 1: якщо x є A_1 і y є B_1, тоді $z_1 = c_1$,

Правило 2: якщо x є A_2 і y є B_2, тоді $z_2 = c_2$. (1.11)

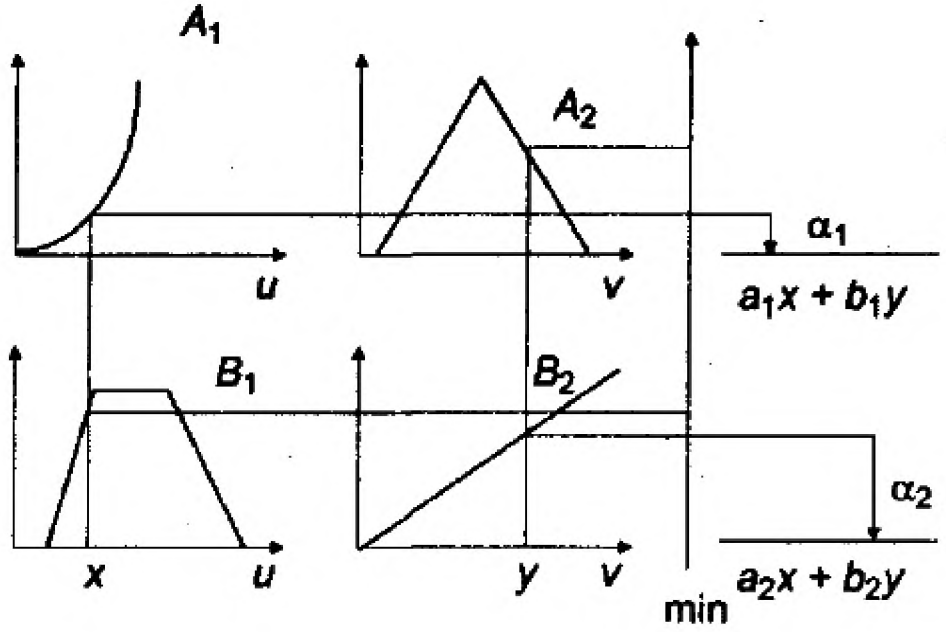


Рисунок 1.9 – Ілюстрація нечіткого висновку Сугено 1-го порядку

1.2.6 Алгоритм Цукамото

Суть алгоритму Цукамото полягає у наступному. Припустимо, що в базі знань містяться тільки два нечітких правила виду [23-29, 32]:

Правило 1: якщо x є A_1 і y є B_1, тоді z є C_1,

Правило 2: якщо x є A_2 і y є B_2, тоді z є C_2, (1.12)

але, на відміну від алгоритму Мамдані, тут функції $C_1(z)$, $C_2(z)$ є монотонними.

Алгоритм Цукамото (Tsukamoto) може бути описаний наступним чином (рис.1.10):

Етап 1. Знаходяться ступені істинності для передумов кожного правила: $A_1(x_0)$, $A_2(x_0)$, $B_1(y_0)$, $B_2(y_0)$.

Етап 2. Знаходяться рівні «відсікання» для передумов кожного з правил (з використанням операції min): $\alpha_1 = A_1(x_0) \wedge B_1(y_0)$, $\alpha_2 = A_2(x_0) \wedge B_2(y_0)$, а потім

– за допомогою вирішення рівнянь $\alpha_1=C_1(z)$, $\alpha_2=C_2(z)$ – чіткі значення (z_1 і z_2) для кожного з вихідних правил.

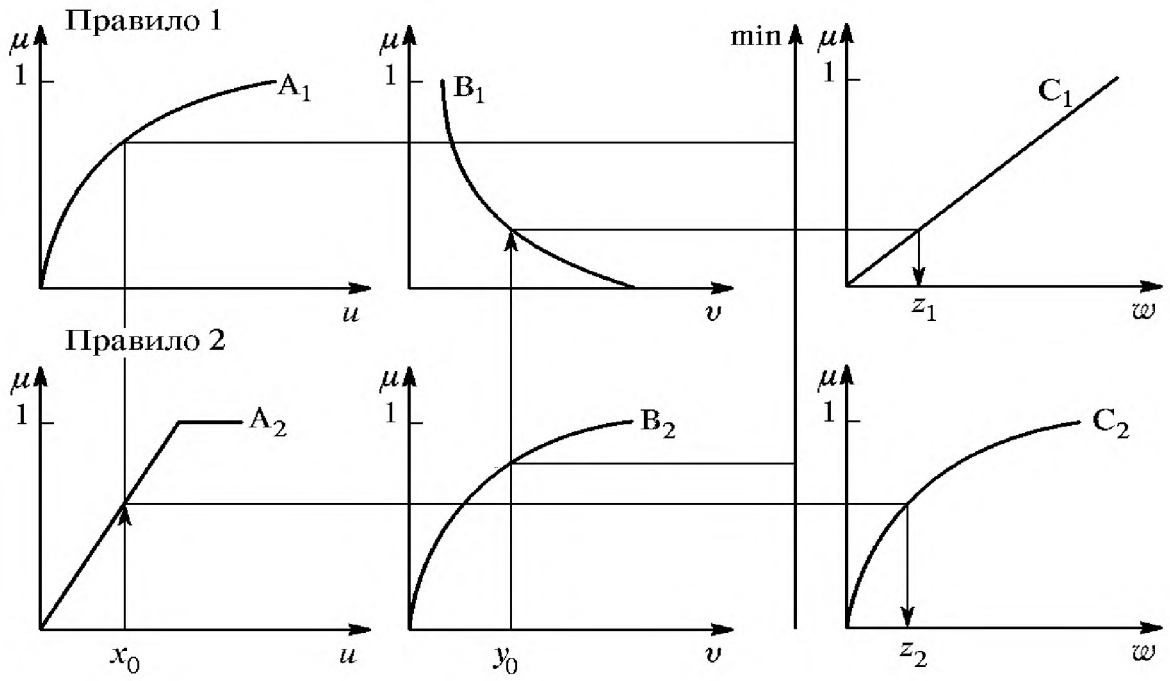


Рисунок 1.10 – Ілюстрація нечіткого висновку Цукамото

Етап 3. Визначається чітке значення змінної виводу (як зважене середнє z_1 і z_2):

$$z_0 = \frac{\alpha_1 z_1 + \alpha_2 z_2}{\alpha_1 + \alpha_2}; \tag{1.13}$$

або у загальному випадку (дискретний варіант центроїдного методу):

$$z_0 = \frac{\sum_{i=1}^{n} \alpha_i z_i}{\sum_{i=1}^{n} \alpha_i}. \tag{1.14}$$

1.3.7 Алгоритм Ларсена

В алгоритмі Ларсена нечітка імплікація моделюється з використанням оператора множення [23-29, 33].

Алгоритм Ларсена (Larsen) може бути описаний наступним чином (рис. 1.11):

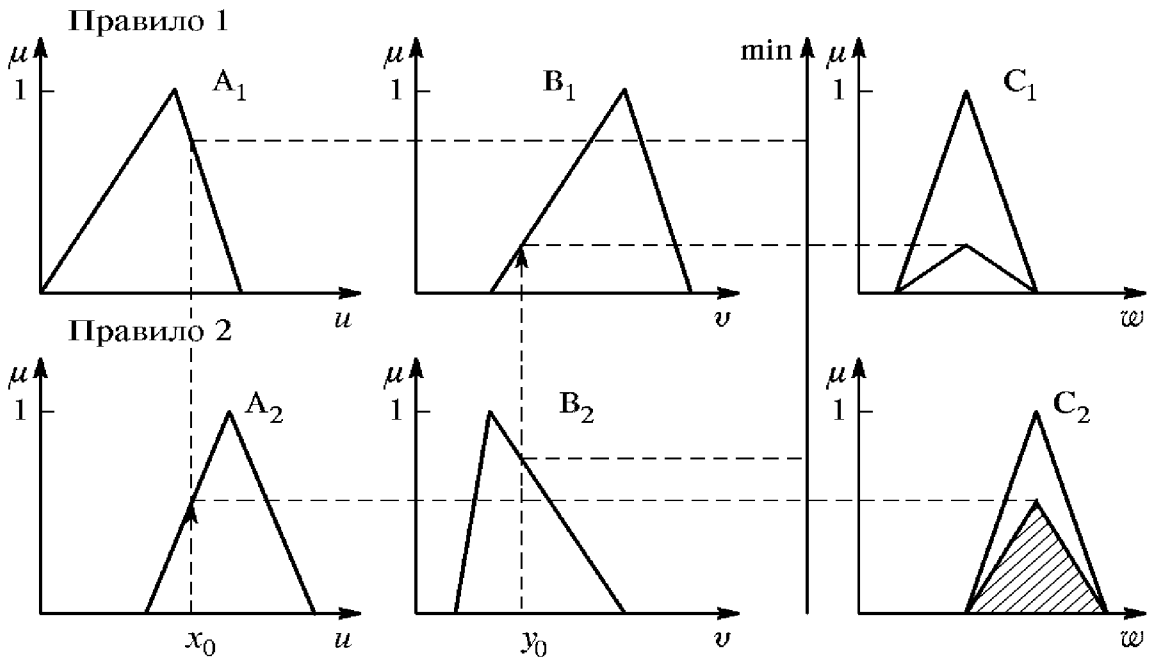


Рисунок 1.11 – Ілюстрація нечіткого висновку Ларсена

Етап 1. Знаходяться ступені істинності для передумов кожного правила: $A_1(x_0)$, $A_2(x_0)$, $B_1(y_0)$, $B_2(y_0)$.

Етап 2. Знаходяться рівні «відсікання» для передумов кожного з правил: $\alpha_1 = A_1(x_0) \wedge B_1(y_0)$, $\alpha_2 = A_2(x_0) \wedge B_2(y_0)$, а потім – приватні нечіткі підмножини $\alpha_1 C_1(z)$ та $\alpha_2 C_2(z)$.

Етап 3. Знаходиться підсумкова нечітка підмножина з функцією належності

$$\mu_\Sigma(z) = C(z) = (\alpha_1 C_1(z)) \vee (\alpha_2 C_2(z)), \qquad (1.15)$$

(у загальному випадку n правил $\mu_\Sigma(z) = C(z) = \bigvee_{i=1}^{n} (\alpha_i C_i(z))$).

Етап 4. Приведення до чіткості (аналогічно до розглянутих раніше алгоритмів).

Слід зазначити, що результати нечіткого висновку, які отримані за допомогою різних алгоритмів, можуть відрізнятися. Певної переваги того чи іншого методу дослідники в області нечітких систем не виділяють. Подібне можна сказати й про способи приведення до чіткості.

1.3.8 Методи приведення до чіткості

1. Центроїдний метод (використовується в алгоритмі Мамдані) для безперервного варіанту має вигляд [23-29]:

$$z_0 = \frac{\int_{\Omega} z \cdot \mathrm{C}(z) dz}{\int_{\Omega} \mathrm{C}(z) dz}; \tag{1.16}$$

а для дискретного варіанту:

$$z_0 = \frac{\sum_{i=1}^{n} \alpha_i z_i}{\sum_{i=1}^{n} \alpha_i}. \tag{1.17}$$

2. Перший максимум. Чітка величина змінної висновку знаходиться як найменше значення, при якому досягається максимум підсумкової нечіткої множини (рис. 1.12,*а*):

$$z_0 = \min\{z \mid \mathrm{C}(z) = \max_u \mathrm{C}(u)\}. \tag{1.18}$$

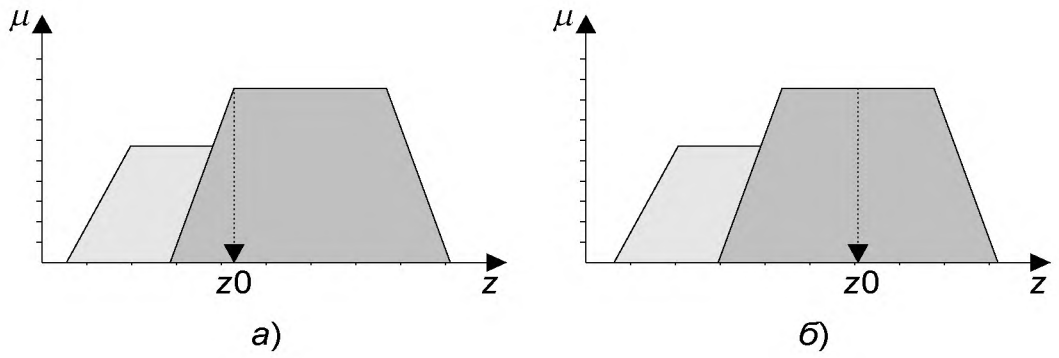
3. Середній максимум. Чітке значення знаходиться за формулою

$$\mathrm{z}_0 = \frac{\int_{\mathrm{G}} \mathrm{z} d\mathrm{z}}{\int_{\mathrm{G}} d\mathrm{z}}, \tag{1.19}$$

де G – підмножина елементів, що максимізують C (рис. 1.12,*б*).

Дискретний варіант (якщо C – дискретно):

$$z_0 = \frac{1}{N} \sum_{j=1}^{N} z_j. \tag{1.20}$$



а) *б*)

Рисунок 1.12 – Ілюстрація методів приведення до чіткості:
а – перший максимум; *б* – середній максимум

4. Критерій максимуму. Чітке значення обирається довільно серед множини елементів, що доставляють максимум C, тобто

$$z_0 \in \{z \mid \mathrm{C}(z) = \max_u \mathrm{C}(u)\}. \tag{1.21}$$

5. Висотна дефазифікація. Елементи області визначення Ω, для яких значення функції належності менше, ніж деякий рівень α, в розрахунок не приймаються і чітке значення розраховується за формулою:

$$z_0 = \frac{\int_{C\alpha} z \cdot \mathrm{C}(z)dz}{\int_{C\alpha} \mathrm{C}(z)dz}, \tag{1.22}$$

де $C\alpha$ – нечітка множина α-рівня.

1.3.9 Ефективність систем з нечіткою логікою

Ефективність використання апарату нечіткої логіки базується на наступних результатах [23-29].

1. У 1992 р. Ванг (Wang) показав, що нечітка система, яка використовує набір правил виду:

$$\textit{Правило } i\textit{: якщо } x_i \in A_i \textit{ і } y_i \in B_i, \textit{ то } z_i \in C_i, \quad i=1,2,\ldots,n \tag{1.23}$$

при гаусівських функціях належності, композиції у вигляді добутку, імплікації у формі Ларсена, а також центроїдного методу приведення до чіткості є універсальним апроксиматором, тобто може апроксимувати будь-яку безперервну функцію з довільною точністю (звісно, при $n \to \infty$).

Інакше кажучи, Ванг довів *теорему*:

для кожної речової безперервної функції g, заданої на компакті U і для довільного $\varepsilon > 0$ існує нечітка експертна система, що формує вихідну функцію $f(x)$ таку, що

$$\sup_{x \in U} \| g(x) - f(x) \| \le \varepsilon , \qquad (1.24)$$

де $\|\cdot\|$ – символ прийнятої відстані між функціями.

2. У 1995 р. Кастро (Castro) показав, що логічний контролер Мамдані при симетричних трикутних функціях належності, композиції з використанням операції min, імплікації у формі Мамдані, а також центроїдного методу приведення до чіткості також є універсальним апроксиматором.

Взагалі, системи з нечіткою логікою доцільно застосовувати для складних процесів, коли немає простої математичної моделі, а також якщо експертні знання про об'єкт або про процес можна сформулювати тільки в лінгвістичній формі.

Також слід відзначити, що системи з нечіткою логікою застосовувати недоцільно у випадках, коли необхідний результат може бути достатньо просто отриманий будь-яким іншим (наприклад, стандартним) шляхом, а також коли для об'єкта або процесу вже знайдена адекватна й легко досліджувана математична модель.

Основні недоліки систем з нечіткою логікою:

1. Вихідний набір нечітких правил-постулатів формулюється експертом-людиною і може виявитися неповним або суперечливим.

2. Вид і параметри функцій належності, що описують вхідні і вихідні змінні системи, обираються суб'єктивно і можуть виявитися такими, що не цілком відображають реальну дійсність.

1.4 Висновок. Постановка задачі

Комп'ютерна стеганографія – самостійний науковий напрямок інформаційної безпеки, що вивчає проблеми створення компонент приховуваної інформації у відкритому інформаційному середовищі, яке може бути сформовано обчислювальними системами та мережами. Особливістю стеганографічного підходу є те, що він не передбачає прямого оголошення факту існування захищуваної інформації. Ця обставина дозволяє в рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати деякі важливі задачі захисту інформації ряду прикладних галузей.

Завдання будь-якої стеганографічної системи – розмістити певне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити різниці між модифікованим контейнером та оригінальним методами візуального або статистичного аналізу.

Цифровим контейнером може слугувати будь-який файл чи потік даних. Через свою надлишковість найчастіше цифровими контейнерами виступають зображення, аудіо- чи відеосигнали.

Наразі найбільшу практичну цінність представляють методи та алгоритми, що працюють зі стисненими зображеннями, оскільки в мережі Інтернет, а також у локальних комп'ютерних мережах цифрові зображення зберігаються і передаються насамперед у стисненому вигляді. Під стисненням розуміється зменшення числа біт, потрібних для цифрового представлення зображень. При цьому найпопулярнішим стандартом стиснення був і залишається JPEG, побудований на основі дискретного косинусного перетворення.

В останні роки з’явилось багато публікацій щодо використання для стеганографічного вбудовування інформації різних методів систем штучного інтелекту (нейронних мереж, нечіткої логіки, еволюційних алгоритмів, агентських алгоритмів оптимізації) [6-22, 29-33]. Цей напрямок наразі є дуже перспективним.

Взагалі актуальність методів систем штучного інтелекту при вирішенні різних питань в галузі кібербезпеки обумовлена здатністю інтелектуальних методів розв’язувати оптимізаційні задачі, які погано формалізуються, а також використанням для моделювання ефективних і універсальних апроксиматорів.

В результаті аналізу існуючих підходів до стеганографічного вбудовування інформації в нерухомі зображення з використанням нечіткої логіки встановлено, що вони показують вищу якість стегозображення, у порівнянні із підходами, які використовують інші інтелектуальні методи, насамперед нейронні мережі. Також відсутні роботи, у яких досліджується використання усіх систем нечіткого висновку для стеганографічного впровадження інформації у нерухомі зображення.

Наразі найпопулярнішими алгоритмами нечіткої логіки є алгоритм Мамдані, Сугено, Цукамото та Ларсена.

Таким чином, для виконання мети кваліфікаційної роботи необхідно:

• запропонувати підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку

Узагальнена схема підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку (Мамдані, Сугено, Цукамото або Ларсена) представлена на рис. 2.1.

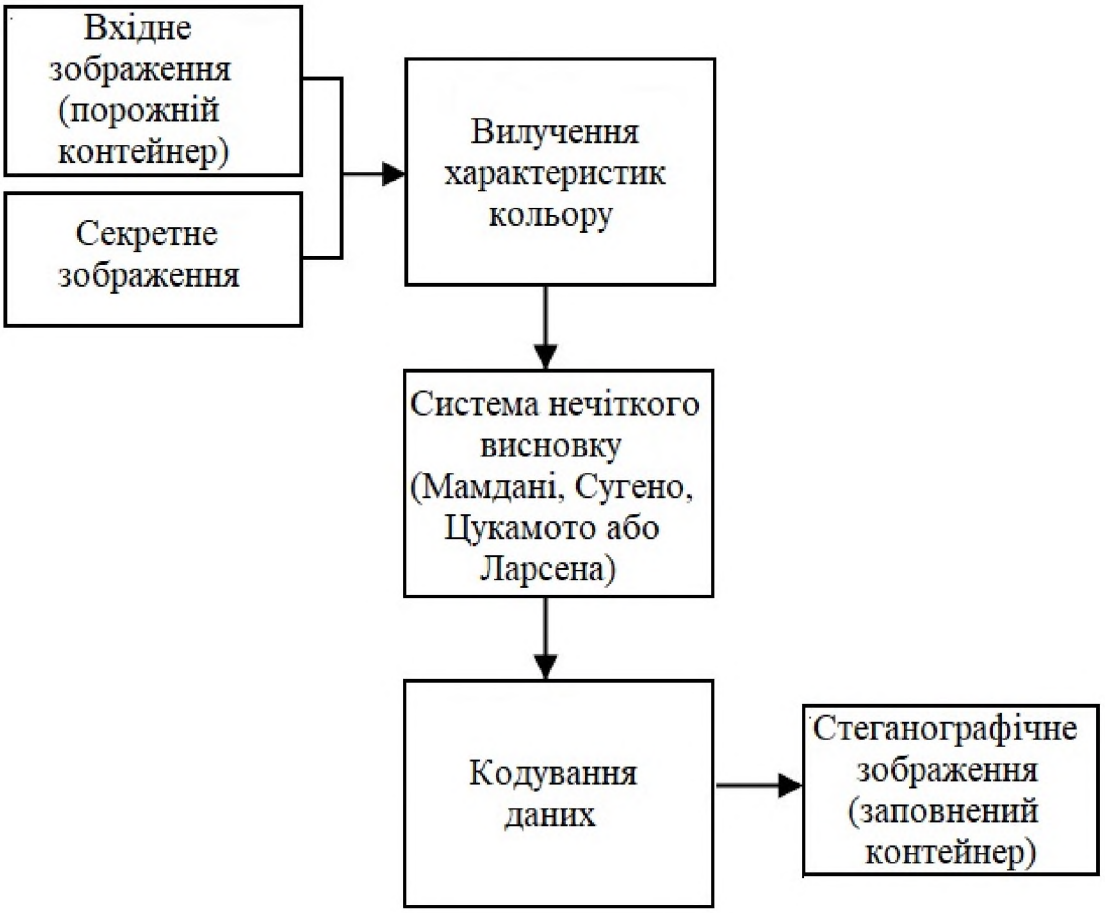


Рисунок 2.1 – Узагальнена схема підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку

На вхід подається вхідне зображення (порожній контейнер) та секретне зображення, яке потрібно впровадити. Далі вхідне зображення (порожній контейнер) розбивається на 9 блоків. У процесі вилучення характеристик кожен з блоків подаються на вхід системи нечіткого висновку (Мамдані, Сугено, Цукамото або Ларсена). Далі відбувається вилучення характеристик текстури, чутливість країв і чутливість яскравості. Формується система нечіткого логічного висновку за допомогою алгоритму Мамдані, Сугено, Цукамото або Ларсена.

Алгоритм вбудовування інформації має такий вигляд:

Крок 1. Зашифруйте секретні дані (зображення).

Крок 2. Розділіть вхідне зображення (порожній контейнер) на 9 блоків.

Крок 3. Виконайте вилучення характеристик з кожного блоку.

Крок 4. Надайте блоки як вхідні дані для системи нечіткого висновку (на основі алгоритму Мамдані, Сугено, Цукамото або Ларсена).

Крок 5. Виконайте процес вилучення характеристик.

Крок 5.1 Виконайте процес вилучення характеристик текстури.

Крок 5.2 Виконайте процес вилучення чутливості країв.

Крок 5.3 Виконайте процес вилучення чутливості до яскравості.

Крок 6. Обчисліть систему нечіткого висновку.

Вилучення кольорових характеристик у пікселях – це процес вилучення кольорових характеристик, які необхідні для ідентифікації кольорових символів кожного пікселя (такі характеристики, як RGB, CYANY, Monochrome).

В рамках розглянутого підходу використовуються наступні властивості кольору [34]:

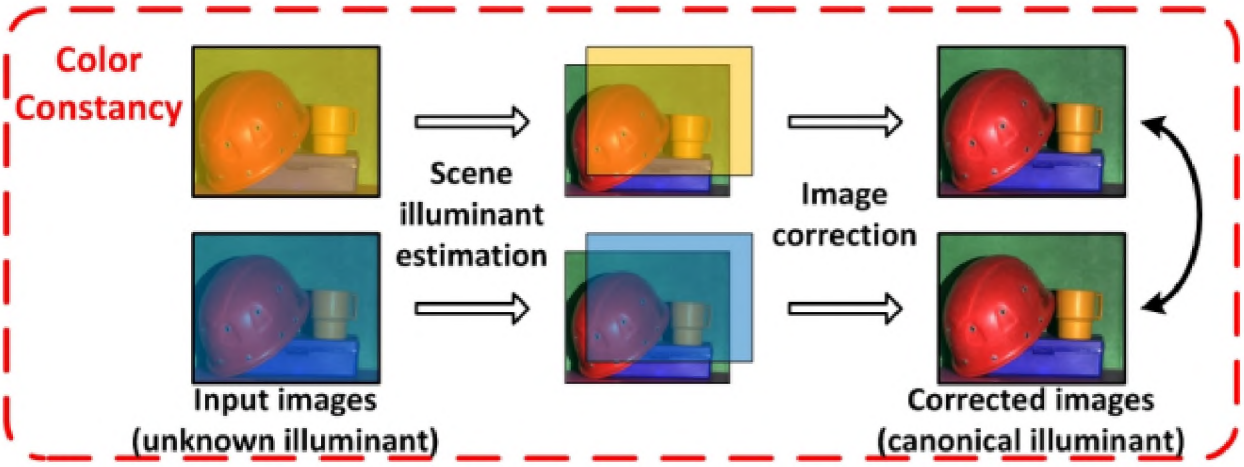
• характеристика інваріантності кольору;

• характеристика дихроматичного відбиття.

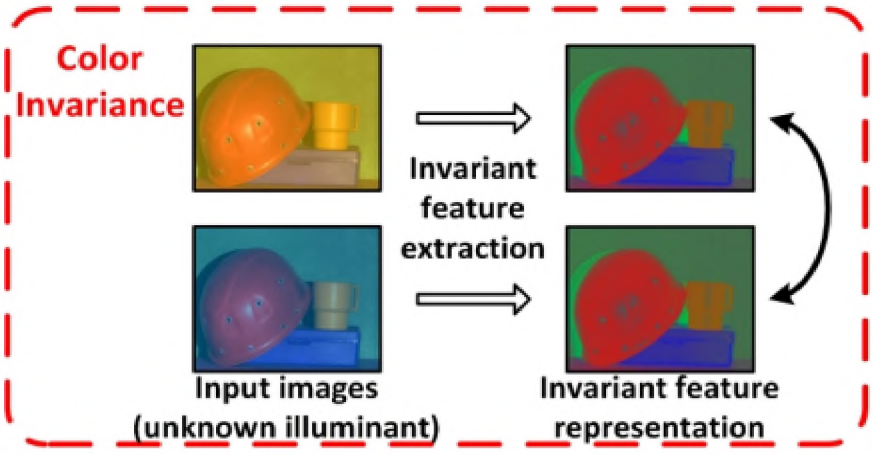
Зазначені характеристики розраховуються для всіх пікселів, присутніх у вхідному зображенні. Зловмисник, який має намір змінити приховані дані, не може передбачити або обчислити значення характеристик зображення, де б

інформація не була прихована. Це гарантує, що інформація не може бути зламана зловмисниками [34-39].

Взагалі, існує дві поширені методики для отримання надійного опису кольору зображення (рис. 2.2): обчислювальна постійність та інваріантність кольору. Методи інваріантності кольорів представляють зображення за характеристиками, які залишаються незмінними щодо конкретних умов зображення (наприклад, освітлення та зміни характеристик датчика).



а



б

Рисунок 2.2 – Порівняння постійності (а) та інваріантності кольору (б)

Існують три фактори, які тісно пов’язані між собою в процесі генерації кольорового зображення в пристроях формування зображення:

• фізичні властивості зображених поверхонь (об’єкта);

• природа джерела світла, що падає на ці поверхні;

• характеристики системи візуалізації.

Фундаментальне питання, пов’язане зі стабільним представленням кольору в даних цифрового зображення, полягає в тому, «як вивести процес формування кольорового зображення на пристроях отримання зображення, використовуючи фізичні закони світла?». Особливо цікаві кольорові зображення, записані в системі RGB через її домінуюче використання.

Стівен Шафер (Steven Shafer) створив просту фізичну модель процесу відбиття, яка називається моделлю дихроматичного відбиття (Dichromatic Reflection Model – DRM) [34], щоб зафіксувати важливий зв’язок між джерелами світла, коефіцієнтами відбиття поверхні та пристроями для формування зображення (рис. 2.3).

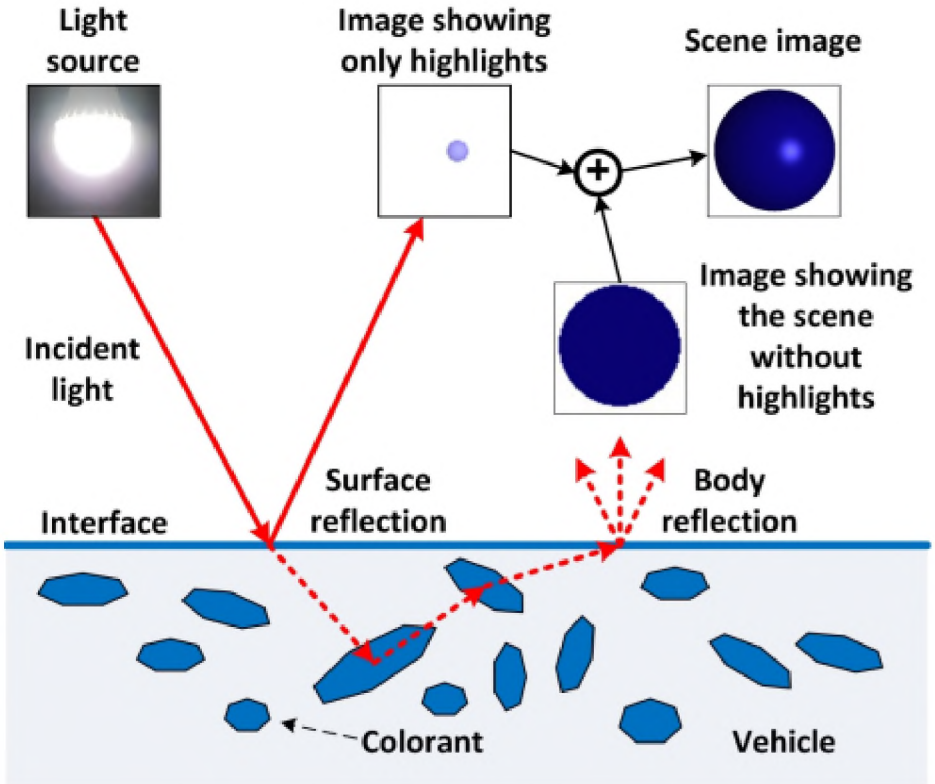


Рисунок 2.3 – Модель дихроматичного відбиття неоднорідного діелектричного матеріалу

Модель дихроматичного відбиття стала основою різноманітних методів постійності та інваріантності кольору. У цій моделі сцена сяйва складається з двох компонентів:

$$L(\lambda)=m_b c_b(\lambda)+m_s c_s(\lambda), \quad (2.1)$$

де λ – довжина хвилі; c_b – відбитий компонент тіла (дифузний); c_s – поверхня (межа розділу) відбитого компонента; m_b і m_s – масштабні коефіцієнти, значення яких змінюється в залежності від освітленості, напряму погляду та орієнтації поверхні.

У системі нечіткого висновку (Мамдані, Сугено, Цукамото або Ларсена) (рис. 2.1) всі входи є значеннями вилучених характеристик. Чотири функції належності з характеристик текстури, функції належності з чутливості до країв і функції належності з чутливості до яскравості надаються як вхідні дані для нечіткої системи.

Для того, щоб обчислити систему нечіткого висновку (Мамдані, Сугено, Цукамото або Ларсена), необхідно виконати наступні кроки з входами від процесу вилучення характеристик:

1. Визначення нечітких правил.

2. Система нечіткого висновку (Мамдані, Сугено, Цукамото або Ларсена) може бути фазифікована на основі вхідних даних, отриманих у процесі вилучення характеристик.

3. Комбінація нечітких вхідних даних на основі нечітких правил для визначення нечітких функцій.

4. Формування імплікації шляхом комбінування правила та виходу функції належності.

5. Формування агрегації шляхом поєднання нечітких правил та імплікації.

6. Виконання дефазифікації для отримання чіткого результату.

Таким чином, розглянутий підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку включає в себе процедуру вилучення кольорових характеристик зображень

(характеристики інваріантності кольору та характеристики дихроматичного відбиття), та їх подачі на вхід системи нечіткого висновку (на основі алгоритму Мамдані, Сугено, Цукамото або Ларсена).

2.2 Оцінка ефективності підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку була проведена шляхом моделювання в середовищі Matlab / Simulink.

Як джерело цифрових зображень використовувалась колекція зображень USC-SIPI, яка була створена на базі Університету Південної Каліфорнії (USC – University of Southern California) Інститутом обробки сигналів і зображень (SIPI – Signal and Image Processing Institute) [41].

Імітаційне моделювання проводилось на двох повнокольорових тестових JPEG-зображеннях роздільною здатністю 512×512 пікселів: «Peppers» і «Sailboat» (рис. 2.4,а-б), які використовувались як контейнери для подальшого вбудовування інформації. Як секретне зображення використовувалось JPEG-зображення «Tree» (рис. 2.4,в) з роздільною здатністю 128×128 та 256×256 пікселів.

Як системи нечіткого висновку досліджувались алгоритми Мамдані, Сугено, Цукамото та Ларсена.

Як критерій оцінки ефективності вбудовування використовувалась величина PSNR (Peak Signal-to-Noise Ratio) – співвідношення між максимумом можливого значення сигналу і потужністю шуму, що його спотворює (дБ):

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right) = 20\log_{10}\left(\frac{\mathrm{MAX}_I}{\sqrt{\mathrm{MSE}}}\right), \tag{2.1}$$

де MAX_I – максимальне значення, яке приймається пікселем цифрового зображення.

а

б

в

Рисунок 2.4 – Тестові зображення для оцінки ефективності підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку:
а – контейнер «Peppers»; б – контейнер «Sailboat»;
в – секретне зображення «Tree»

MSE (Mean Squared Error) – середньоквадратичне відхилення:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left| I(i, j) - K(i, j) \right|^2 \qquad (2.2)$$

де I(i, j) і K(i, j) – поточне й оцінюване цифрове зображення, відповідно; m×n – розмір цифрового зображення.

Результати імітаційного моделювання – значення оцінки якості величини PSNR (2.1) при використанні як системи нечіткого висновку алгоритмів Мамдані, Сугено, Цукамото та Ларсена при вбудовуванні секретного зображення «Tree» з роздільною здатністю 128×128 та 256×256 пікселів в зображення-контейнери «Peppers» і «Sailboat» представлені в табл. 2.1-2.2.

Таблиця 2.1 – Значення PSNR (дБ) при вбудовуванні інформації в зображення-контейнер «Peppers»

Роздільна здатність секретного зображення	Система нечіткого висновку			
	Мамдані	Сугено	Цукамото	Ларсена
128×128	61,14	61,08	57,95	58,67
256×256	55,62	55,67	52,94	53,42

Таблиця 2.2 – Значення PSNR (дБ) при вбудовуванні інформації в зображення-контейнер «Sailboat»

Роздільна здатність секретного зображення	Система нечіткого висновку			
	Мамдані	Сугено	Цукамото	Ларсена
128×128	60,89	60,84	57,78	58,44
256×256	56,03	56,06	53,19	53,81

Таким чином, в результаті імітаційного моделювання підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку було встановлено, що алгоритми Мамдані і Сугено показали кращі і приблизно однакові результати (див. табл.

2.1-2.2). При вбудовуванні секретного зображення роздільною здатністю 128×128 пікселів кращі результати показало використання алгоритму Мамдані – значення PSNR склало 61,14 дБ для зображення-контейнера «Peppers» і 60,89 дБ для зображення-контейнера «Sailboat». При вбудовуванні секретного зображення роздільною здатністю 256×256 пікселів кращі результати показало використання алгоритму Сугено – значення PSNR склало 55,67 дБ для зображення-контейнера «Peppers» і 56,06 дБ для зображення-контейнера «Sailboat».

Також було встановлено, що найгірші результати показало використання алгоритму Цукамото, у середньому на 5% гірше у порівнянні з алгоритмами Мамдані і Сугено. Використання ж алгоритму Ларсена показало результати у середньому на 4% гірше у порівнянні з алгоритмами Мамдані і Сугено.

Час вбудовування інформації на комп'ютері з процесором Pentium IV згідно запропонованого підходу із використанням алгоритмів Мамдані, Сугено, Цукамото та Ларсена становить 300-320 с при вбудовуванні секретного зображення роздільною здатністю 128×128 пікселів, та 550-600 с при вбудовуванні секретного зображення роздільною здатністю 256×256 пікселів, що у середньому на 10-15% менше у порівнянні з іншими підходами, які використовують послідовне вбудовування інформації (найпростіша варіація методу найменш значущого біта, структурні методи і т.д.).

Наукова новизна результатів полягає у тому, що використання систем нечіткого висновку на основі алгоритмів Мамдані, Сугено, Цукамото і Ларсена дозволяє виконувати стеганографічне вбудовування інформації в цифрові зображення формату JPEG.

Подальші дослідження можуть бути спрямовані на вдосконалення розглянутого підходу для стеганографічного вбудовування інформації в зображення інших форматів, таких як BMP, TIFF тощо. Також можна дослідити можливість використання й інших кольорових характеристик зображень (а не тільки характеристики інваріантності кольору та дихроматичного відображення).

2.3 Висновки

Запропонований підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку включає в себе процедуру вилучення кольорових характеристик зображень таких як характеристики інваріантності кольору та характеристики дихроматичного відбиття, а також їх подачі на вхід системи нечіткого висновку, яка побудована на основі алгоритму Мамдані, Сугено, Цукамото або Ларсена.

Оцінка ефективності підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку була проведена шляхом моделювання в середовищі Matlab / Simulink. Як джерело цифрових зображень використовувалась колекція зображень USC-SIPI, з якої було взято два повнокольорових тестових JPEG-зображення роздільною здатністю 512×512 пікселів: «Peppers» і «Sailboat», які використовувались як контейнери, а також JPEG-зображення «Tree» з роздільною здатністю 128×128 та 256×256 пікселів, що використовувалось як секретне зображення.

В результаті імітаційного моделювання було встановлено, що алгоритми Мамдані і Сугено показали кращі і приблизно однакові результати. При вбудовуванні секретного зображення роздільною здатністю 128×128 пікселів кращі результати показало використання алгоритму Мамдані – значення PSNR склало 61,14 дБ для зображення-контейнера «Peppers» і 60,89 дБ для зображення-контейнера «Sailboat». При вбудовуванні секретного зображення роздільною здатністю 256×256 пікселів кращі результати показало використання алгоритму Сугено – значення PSNR склало 55,67 дБ для зображення-контейнера «Peppers» і 56,06 дБ для зображення-контейнера «Sailboat».

Також було встановлено, що найгірші результати показало використання алгоритму Цукамото, у середньому на 6,5% гірше у порівнянні з алгоритмами

Мамдані і Сугено. Використання ж алгоритму Ларсена показало результати у середньому на 5% гірше у порівнянні з алгоритмами Мамдані і Сугено.

Час вбудовування інформації на комп'ютері з процесором Pentium IV згідно запропонованого підходу з використанням алгоритмів Мамдані, Сугено, Цукамото та Ларсена становить 300-320 с при вбудовуванні секретного зображення роздільною здатністю 128×128 пікселів, та 550-600 с при вбудовуванні секретного зображення роздільною здатністю 256×256 пікселів, що у середньому на 10-15% менше у порівнянні з іншими підходами, які використовують послідовне вбудовування інформації (найпростіша варіація методу найменш значущого біта, структурні методи і т.д.).

3 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є обґрунтування економічної доцільності стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку. Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок капітальних (фіксованих) витрат

Капітальними витрати називаються тому, що робляться, як правило, один раз, на початкових етапах створення інформаційної системи (ІС). До капітальних слід відносити наступні витрати: вартість розробки і впровадження проекту; залучення зовнішніх консультантів; первинні закупівлі основного програмного забезпечення (ПЗ); первинні закупівлі додаткового ПЗ; первинні закупівлі апаратного забезпечення тощо.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу щодо стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні операції:

де $t_{тз}$ – тривалість складання технічного завдання на стеганографічне вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку, $t_{тз}$=18;

$t_в$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо, $t_в$=*31*;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=*40*;

$t_р$ – тривалість імітаційного моделювання та оцінки ефективності підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку, $t_м$=*50*;

$t_д$ – тривалість підготовки технічної документації, $t_д$=*16*.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 18+31+40+50+16 = 155 \text{ годин.}$$

Розрахунок витрат на розробку підходу щодо стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}\ .$$

$$К_{рп} = З_{зп} + З_{мч} = 28675 + 1153{,}2 = 29828{,}2 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 155*185 = 28675 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч}= t*C_{мч}=155*7,44=1153,2 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0,9 \cdot 3 \cdot 1,68 + \frac{5800 \cdot 0,5}{1920} + \frac{6700 \cdot 0,4}{1920} = 7,44 \text{ грн.}$$

Оцінка ефективності підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку виконувалась за допомогою стандартних та розроблених програм в середовищі Matlab/Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Для розробки запропонованого підходу є потреба у залученні зовнішніх консультантів, що потребуватиме додаткових витрат величиною 4500 грн.

Витрати на налагодження системи інформаційної безпеки становитимуть 2000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$=29828,2+4500+2000=36328,2 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

де $С_в$ – вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки.

Оскільки середовище Matlab/Simulink, яке застосовувалося для оцінки ефективності підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку вже використовується, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 4000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18500 грн. Додаткова заробітна плата – 9% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту

інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки.

Отже,

$$С_з = (18500*12 + 18500*12*0,09)*0,1= 24198 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2022 р. складає 22%.

$$С_{єв} = 24198*0,22 = 5323,6 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,8*3*1920*1,68 = 7741,4 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1%

$$С_{тос} = 36328,2*0,01=363,28 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 4000+24198+5323,6 +7741,4+363,28 = 41626,28 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 10%.

Тому:

$$С_{ак} = 36328,2*0,10=3632,82 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$C = 0+41626,28 +3632,82 = 45259,1 \text{ грн.}$$

3.3 Оцінка можливого збитку

Запропонований підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку може бути використаний для організації прихованого зберігання і передачі інформації по відкритих каналах зв'язку.

Оцінка величини можливого збитку визначатиметься для умовного підприємства, яке може передавати інформацію по відкритих каналах зв'язку, вартість якої потенційно складає 550000 грн.

Вірогідність реалізації загроз (R) щодо цифрових зображень формату JPEG, які можуть порушити цілісності інформації, складає 20%.

Отже, можлива величина збитку (B) на рік від загроз щодо цифрових зображень формату JPEG, які можуть порушити цілісність інформації, становитиме:

$$B = 550000*0,2 = 110000 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації загрози;

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

Таким чином, загальний ефект від впровадження системи інформаційної безпеки визначається із урахуванням ризиків порушення інформаційної безпеки:

$$E = 110000 - 45259,1 = 64740,9 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 64740,9/36328,2 = 1,78 \text{ частки одиниці.}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (7%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,78 > (7 - 5)/100 = 1,78 > 0,02.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}$$

T_0= 1 / 1,78 = 0,56 року.

3.6 Висновок

Розробка підходу до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку є економічно доцільною відповідно до отриманих значень показників економічної ефективності, зокрема: коефіцієнт повернення інвестицій ROSI складає 1,78 грн./грн. (тобто на 1 гривню капітальних витрат припадає 1,78 грн. економічного ефекту). При цьому величина економічного ефекту складає 64740,90 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,56 року. Капітальні витрати визначено обсягом 36328,2 грн.

ВИСНОВКИ

1. Комп'ютерна стеганографія – самостійний науковий напрямок інформаційної безпеки, що вивчає проблеми створення компонент приховуваної інформації у відкритому інформаційному середовищі, яке може бути сформовано обчислювальними системами та мережами. Особливістю стеганографічного підходу є те, що він не передбачає прямого оголошення факту існування захищуваної інформації. Ця обставина дозволяє в рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати деякі важливі задачі захисту інформації ряду прикладних галузей.

Завдання будь-якої стеганографічної системи – розмістити певне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити різниці між модифікованим контейнером та оригінальним методами візуального або статистичного аналізу.

Цифровим контейнером може слугувати будь-який файл чи потік даних. Наразі найбільшу практичну цінність представляють методи та алгоритми, що працюють зі стисненими зображеннями, найпопулярнішим стандартом стиснення є JPEG, побудований на основі дискретного косинусного перетворення.

2. В останні роки з’явилось багато публікацій щодо використання для стеганографічного вбудовування інформації різних методів систем штучного інтелекту (нейронних мереж, нечіткої логіки, еволюційних алгоритмів, агентських алгоритмів оптимізації), актуальність яких обумовлена здатністю інтелектуальних методів розв’язувати оптимізаційні задачі, які погано формалізуються, а також використанням для моделювання ефективних і універсальних апроксиматорів.

В результаті аналізу існуючих підходів до стеганографічного вбудовування інформації в нерухомі зображення з використанням нечіткої логіки встановлено, що вони показують вищу якість стегозображення, у порівнянні із підходами, які використовують інші інтелектуальні методи,

насамперед нейронні мережі. Також відсутні роботи, у яких досліджується використання усіх систем нечіткого висновку для стеганографічного впровадження інформації у нерухомі зображення.

Наразі найпопулярнішими алгоритмами нечіткої логіки є алгоритм Мамдані, Сугено, Цукамото та Ларсена.

3. Запропоновано підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку, який включає в себе процедуру вилучення кольорових характеристик зображень таких як характеристики інваріантності кольору та характеристики дихроматичного відбиття, а також їх подачі на вхід системи нечіткого висновку, яка побудована на основі алгоритму Мамдані, Сугено, Цукамото або Ларсена.

4. Оцінка ефективності запропонованого підходу була проведена шляхом моделювання в середовищі Matlab / Simulink. Встановлено, що алгоритми Мамдані і Сугено показали кращі і приблизно однакові результати: при вбудовуванні секретного зображення роздільною здатністю 128×128 пікселів значення PSNR у середньому дорівнює 61 дБ, а при вбудовуванні зображення роздільною здатністю 256×256 пікселів – 55,9 дБ. Використання алгоритму Цукамото показало результати у середньому на 5% гірше у порівнянні з алгоритмами Мамдані і Сугено, а алгоритму Ларсена – на 4% гірше.

Час вбудовування інформації на комп'ютері з процесором Pentium IV згідно розглянутого підходу із використанням алгоритмів Мамдані, Сугено, Цукамото та Ларсена у середньому на 10-15% менше у порівнянні з іншими підходами, які використовують послідовне вбудовування інформації (найпростіша варіація методу найменш значущого біта, структурні методи і т.д.).

ПЕРЕЛІК ПОСИЛАНЬ

1. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки / В.К. Задірака // Вісник Національної академії наук України. – 2014. – № 5. – С. 65-69.

2. Кошкіна Н.В. Ефективні спектральні алгоритми для вирішення задач цифрової стеганографії : дис. канд. фіз.-мат. наук: 01.05.01 / Н.В. Кошкіна. – НАН України, Інститут кібернетики ім. В. М. Глушкова. – Київ, 2005. – 139 с.

3. Конахович Г.Ф. Компьютерная стеганография : теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

4. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О.К. Юдін, Р.В. Зюбіна, О.В. Фролов // Радиоэлектроника и информатика. – 2015. – № 3. – С. 13-21.

5. Основи комп'ютерної стеганографії : Навч. посіб. для студентів і аспірантів / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця: ВДТУ, 2003. – 427 с.

6. Sajasi S. A high quality image steganography scheme based on Fuzzy Inference System / S. Sajasi, A.M. Moghadam // Indian Journal of Science and Technology. – 2013. – № 4(15).– P. 1-6.

7. Alvi A.K. Image steganography using fuzzy domain transformation and pixel classification / A.K. Alvi, R. Dawes // 25th International Conference on Software Engineering and Knowledge Engineering (SEKE'13). – 2013. – P. 277-282.

8. Darshan R. Acceleration of LSB algorithm in GPU / R. Darshan, R. Prabu, M. Divya // International Journal of Computer Science and Information Technologies. – 2014. – № 5(3). – P. 2865-2867.

9. Forrest S. Genetic algorithms: Principles of natural selection applied to computation / S. Forrest // International Journal of Computer Science and Information Technologies. – 1993. – № 261(5123). – P. 872-878.

10. Long J. Fully convolutional networks for semantic segmentation / J. Long, E. Shelhamer, T. Darrell // IEEE Conference on Computer Vision and Pattern Recognition, 2015. – Boston, MA, USA. – P. 3431-3440.

11. Noh H. Learning deconvolution network for semantic segmentation / H. Noh, S. Hong, B. Han // IEEE International Conference on Computer Vision. – 2015. – Santiago, Chile. – P. 1520-1528.

12. Badrinarayanan V. Segnet: A deep convolutional encoder-decoder architecture for image segmentation / V. Badrinarayanan, A. Kendall, R. Cipolla. // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2017. – № 39 (12). – P. 2481-2495.

13. Kendall A. Bayesian segnet: Model uncertainty in deep convolutional encoder-decoder architectures for scene understanding / A. Kendall, V. Badrinarayanan, R. Cipolla // IEEE Conference on Computer Vision and Pattern Recognition, 2015. – Boston, MA, USA. – P. 1511-1520.

14. Al-Rubbaiy F.H. Concealment of information and encryption by using fuzzy technique / F.H. Al-Rubbaiy // Journal of the College of Basic Education. – 2011. – № 16(69). – P. 25-34.

15. Alghamdi A.A. Information security using steganographic method: Genetic algorithm and texture features / A.A. Alghamdi // Indian Journal of Science and Technology. – 2018. – № 11(34). – P. 1-6.

16. Khursheed F. Fuzzy logic-based data hiding / F. Khursheed, A.H. Mir // Proceeding of Cyber Security, Cyber Crime, and Cyber Forensics. – Department of Electronics and Communication, National Institute of Technology, Srinagar, India. – 2009.

17. Mir A.H. Fuzzy entropy based interactive enhancement of radiographic images / A.H. Mir // In Journal of Medical Engineering and Technology. – 2007. – Vol.31, no.3. – P.220–231.

18. Toony Z. A high capacity image hiding method based on fuzzy image coding/decoding / Z. Toony, H. Sajedi, M. Jamzad // 6th International Conference on Information Hiding, Toronto, Canada. – 2009. – P. 518-523.

19. A novel hybrid fuzzy-SVM image steganographic model / H.S. Hussain, S.A. Aljunid, S. Yahya, F.H.M. Ali // In Proceeding of International Symposium in Information Technology. – 2010. – Vol.1. – P.1-6.

20. Goodarzi M.H. Convergence between fuzzy logic and steganography for high payload data embedding and more security / M.H. Goodarzi, A. Zaeim, A.S. Shahabi // Proceedings of 6th International Conference on Telecommunication Systems, Services, and Applications. – 2011. – P.130-138.

21. Silman J. Steganography and steganalysis: An overview. / J. Silman. – Sans Institute, 2001. – Vol. 3. – P. 61-76.

22. Katzenbeisser S. Information hiding techniques for steganography and digital watermarking / Katzenbeisser S., Petitcolas F. // Artech house, Norwood, Massachusetts, USA. – 2000.

23. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с.

23. Глибовець М.М. Штучний інтелект : підручник для студ. вищих навч.закладів / М. М. Глибовець, О.В. Олецький. – К. : КМ Академія, 2002. – 369 с.

25. Ланде Д.В. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. / Д.В. Ланде, І.Ю. Субач, Ю.Є. Бояринова. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. – 297 с.

26. Зайченко Ю.П. Нечіткі моделі і методи в інтелектуальних системах. / Ю.П. Зайченко. – К: Слово, 2008. – 344 с.

27. Nelles O. Nonlinear System Identification: From Classical Approaches to Neural and Fuzzy Models / O. Nelles. – Berlin: Springer, 2001. – 785 pp.

28. Нейрокомпьютеры и интеллектуальные роботы / Под ред. Н. М. Амосова. – Киев.: Наукова думка, 1991. – 412 с.

29. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница: «УНІВЕРСУМ-Вінниця», 1999. – 320 с.

30. Mamdani E.H. An experiment in linguistic synthesis with a fuzzy logic controller / E.H. Mamdani, S. Assilian // International Journal of Man-Machine Studies. – 1975. – Vol. 7(1). – P. 1-13.

31. Takagi T. Fuzzy identification of systems and its applications to modeling and control / T. Takagi, M. Sugeno // IEEE Transactions on Systems, Man and Cybernetics. – 1985. – Vol. 15. – P. 116-132.

32. Tsukamoto Y. An approach to fuzzy reasoning method / Y. Tsukamoto // Advances in Fuzzy Set Theory and Applications. – Edited by M.M. Gupta, R.K. Ragade, R.R. Yager. – Amsterdam: North-Holland, – 1979.

33. Larsen M. Industrial applications of fuzzy logic control / M. Larsen // International Journal of Man-Machine Studies. – 1980. – Vol. 12. – No. 1. – P. 3-10.

34. Lee D. A Taxonomy of Color Constancy and Invariance Algorithm / D. Lee, K. Plataniotis. – Advances in Low-Level Color Image Processing. – Chapter: 3. – Publisher: Springer Netherlands. – P. 55-94.

35. Alghamdi A.A. Computerized steganographic technique using fuzzy logic. / A.A. Alghamdi // International Journal of Advanced Computer Science and Applications. – 2018. – Vol. 9(3). – P. 155-159.

36. Provos N. Hide and seek: an introduction to steganography / N. Provos, P. Honeyman // IEEE International Journal of Security and Privacy. – 2003. – Vol. 1., no.3. – P. 32–44.

37. Petitcolas F.A.P. Introduction to information hiding / F.A.P. Petitcolas // Information Hiding Techniques for Steganography and Digital Watermarking. – Artech House, Inc., Norwood. – 2000.

38. Ковтун В.Ю. Систематизація сучасних методів комп'ютерної стеганографії / В.Ю. Ковтун, С.А. Гнатюк, А.Н. Кинзерявий // Ukrainian Scientific Journal of Information Security. – 2013. – Vol. 19, issue 3. – P. 209-217.

39. Cheddad A. Digital image steganography: Survey and analysis of current methods / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // Signal Processing. – 2010. – Vol. 90(3). – P. 727-752.

40. Кузнецов О.О. Стеганографія: навчальний посібник / О.О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

41. The USC-SIPI image database. [Електронний ресурс]. – Режим доступу: http://sipi.usc.edu/database/.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	34	
6	А4	Спеціальна частина	11	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Гринько.ppt

2 Диплом Гринько.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-1 Гринько І.А.

на тему: «Стеганографічне впровадження інформації в цифрові зображення за допомогою систем нечіткого висновку»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 74 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на дослідження алгоритмів нечіткої логіки для вбудовування інформації у JPEG-зображення.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу основних положень цифрової стеганографії, принципів приховування даних в зображеннях, основ нечіткої логіки і систем нечіткого висновку, а також існуючих підходів до вбудовування інформації в нерухомі зображення з використанням нечіткої логіки в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до стеганографічного вбудовування інформації у цифрові зображення із використанням систем нечіткого висновку та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропоновані рішення можуть бути використані для організації прихованого зберігання і передачі даних по відкритих каналах зв'язку.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Гринько І.А. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**