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 *Шило Олександр Валерійович*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Перевірка графічних зображень на наявність стеганографічно вбудованого водяного знака*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ас. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Шило Олександр Валерійович*** **академічної групи** ***125-17-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Перевірка графічних зображень на наявність стеганографічно вбудованого водяного знака***

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

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз технологій цифрового маркування графічних зображень і дискримінантного аналізу, а також існуючих підходів до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу та оцінка його ефективності.	01.04.2021 – 12.05.2021
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2021 – 09.06.2021

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Шило О.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 15 рис., 4 додатки, 35 джерел.

Об’єкт розробки – цифрові зображення.

Предмет розробки – підхід до ідентифікації цифрових зображень, що містять цифровий водяний знак.

Мета кваліфікаційної роботи – можливість ідентифікації цифрових зображень, що містять ЦВЗ в умовах відсутності апріорних відомостей про наявність ЦВЗ в даному зображенні і про закон вбудовування ЦВЗ.

Наукова новизна результатів полягає у тому, що ідентифікація цифрових зображень, відбувається шляхом побудови власних характеристичних векторів зображень з навчальної вибірки, що включають в себе статистичні характеристики, обчислені з розподілів вейвлет-коефіцієнтів і з розподілів похибки передбачення величин вейвлет-коефіцієнтів на різних піддіапазонах.

У першому розділі проаналізовано технології цифрового маркування графічних зображень і дискримінантного аналізу, а також існуючі підходи до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака.

У спеціальній частині роботи запропоновано підхід до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.

ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ, ДИСКРИМІНАНТНИЙ АНАЛІЗ, СТЕГАНОГРАФІЯ, ГРАФІЧНИЙ ФАЙЛ, КЛАСИФІКАЦІЯ, ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 76 с., 15 рис., 4 приложения, 35 источников.

Объект разработки – цифровые изображения.

Предмет разработки – подход к идентификации цифровых изображений, содержащих цифровой водяной знак.

Цель квалификационной работы – возможность идентификации цифровых изображений, содержащих ЦВЗ в условиях отсутствия априорных сведений о наличии ЦВЗ в данном изображении и о законе встраивания ЦВЗ.

Научная новизна заключается в том, что идентификация цифровых изображений, происходит путем построения собственных характеристических векторов изображений из обучающей выборки, включающих в себя статистические характеристики, вычисленные с распределений вейвлет-коэффициентов и с распределений погрешности предсказания величин вейвлет-коэффициентов на разных поддиапазонах.

В первой главе проанализированы технологии цифрового маркировки графических изображений и дискриминантного анализа, а также существующие подходы к проверке графических изображений на наличие стеганографической встроенного водяного знака.

В специальной части работы предложен подход к идентификации цифровых изображений, содержащих цифровой водяной знак, с использованием дискриминантного анализа и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, затрат на эксплуатацию системы безопасности и срок окупаемости инвестиций применения предложенного подхода.

ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЕ, ДИСКРИМИНАНТНЫЙ АНАЛИЗ, СТЕГАНОГРАФИЯ, ГРАФИЧЕСКИЙ ФАЙЛ, КЛАССИФИКАЦИЯ, ЦИФРОВОЙ ВОДЯНОЙ ЗНАК, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 76, fig. 15, 4 additions, 35 sources.

The object of development is digital images.

The subject of development is an approach to the identification of digital images containing a digital watermark.

The purpose of the qualification work is the possibility of identification of digital images containing CEV in the absence of a priori information about the presence of CEV in this image and the law of embedding CEC.

The scientific novelty of the results is that the identification of digital images occurs by constructing eigenvalue vectors of images from the training sample, which include statistical characteristics calculated from the distributions of wavelet coefficients and from the error prediction distributions of wavelet coefficients in different subbands.

The first section analyzes the technologies of digital labeling of graphic images and discriminant analysis, as well as existing approaches to the verification of graphic images for the presence of steganographically embedded watermark.

A special part of the paper proposes an approach to the identification of digital images containing digital watermark, using discriminant analysis and evaluates its effectiveness. Based on the results of research, conclusions were made regarding the solution of the problem.

In the economic section, calculations of capital costs, costs of operating the security system and the payback period of the application of the proposed approach.

WAVELET TRANSFORMATION, DISCRIMINATIVE ANALYSIS, STEGANOGRAPHY, GRAPHIC FILE, CLASSIFICATION, DIGITAL WATERMARK, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВП – Вейвлет-перетворення;

ВХВ – Власний характеристичний вектор;

ДКП – Дискретне косинусне перетворення;

ЦВЗ – Цифровий водяний знак;

ЦЗ – Цифрове зображення;

LDA – Linear Discriminant Analysis – Лінійний дискримінантний аналіз;

QDA – Quadratic Discriminant Analysis – Квадратичний дискримінантний аналіз.

ЗМІСТ

ВСТУП

З розвитком інформаційних технологій різко зросла проблема інформаційної безпеки. З використанням різних засобів обчислювальної техніки зловмисникові легко здійснити швидке незаконне розповсюдження і модифікацію мультимедійної інформації. Щороку в мережі Інтернет відбувається незаконне масове тиражування аудіо та відео продукції, а також нерухомих зображень. Тим самим власнику інформації завдається великої шкоди, як матеріальної, так і моральної.

Розвиток засобів обчислювальної техніки і широке поширення глобальної мережі Інтернет призвело до необхідності розробки нових засобів захисту мультимедійної інформації від незаконного поширення. На сьогоднішній день відомі дві ефективні технології забезпечення захисту безпеки мультимедійної інформації: стеганографія і криптографія.

Криптографічні методи піддають шифруванню об'єкт захисту за допомогою певного алгоритму з використанням ключа. При цьому зміст об'єкта захисту доступний тільки обмеженому колу осіб (власникам ключа) і тільки після дешифрування. Незважаючи на те, що на сьогоднішній день криптографічні методи досить надійні, шифрування інформації має ряд недоліків:

- зашифрований об'єкт може привернути увагу зловмисника;
- у ряді країн накладається ряд обмежень на використання криптографічних засобів.

На відміну від криптографії стеганографія приховує сам факт передачі інформації й, отже, не привертає уваги зловмисника. Крім того, на стеганографії не накладаються законодавчі обмеження, як у випадку криптографії. Тому використання методів даної науки в області захисту мультимедійної інформації має великий пріоритет.

Одним з напрямків стеганографії є цифрове маркування, яке здійснює непомітне вбудовування в об'єкт захисту невидимою для людського ока цифровий мітки – цифрового водяного знаку (ЦВЗ) [1-3]. Наявність

вбудованого в об'єкт захисту ЦВЗ дозволяє однозначно визначити автора документа, що утримує потенційного зловмисника від незаконного поширення мультимедійної інформації.

Наразі для захисту авторських прав на зображення віддається перевага впровадженню саме ЦВЗ в дані об'єкти через невисоку вартість, на відміну від інших відомих технічних і організаційних методів, а також можливості використання при реєстрації цифрових зображень, що недоступно для багатьох організаційних методів.

Нажаль, наразі, незважаючи на велику кількість існуючих методів і алгоритмів маркування, не існує універсального способу захисту зображень і визначення його автентичності, тому завдання розробки моделей і алгоритмів, що дозволяють забезпечити можливість докази автентичності та справжності захищених зображень, є актуальною.

Таким чином, вдосконалення підходів до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака наразі є актуальною задачею.

Метою роботи є можливість ідентифікації цифрових зображень, що містять ЦВЗ в умовах відсутності апріорних відомостей про наявність ЦВЗ в даному зображенні і про закон вбудовування ЦВЗ.

Постановка задачі:

• проаналізувати технології цифрового маркування графічних зображень, а також дискримінантного аналізу;

• провести аналіз існуючих підходів до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака;

• запропонувати підхід до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз технології цифрового маркування графічних зображень

Стеганографія – це наука, що вивчає методи приховування конфіденційної інформації [4]. Для захисту мультимедійної продукції активно використовується такий стеганографічний метод як цифрове маркування («digital watermarking»). Вперше термін «digital watermarking» застосовувався в роботі [5]. Цифрове маркування полягає у впровадженні в об'єкт захисту цифрового водяного знаку (ЦВЗ). Цифровий водяний знак – це цифрова мітка, непомітно вбудовується в зображення або інший сигнал для контролю його використання [4, 6, 7].

1.1.1 Місце цифрового маркування в стеганографії

Стеганографія – стародавня наука, що має декілька напрямків: класичний, комп'ютерний і цифровий.

Основне призначення класичної стеганографії – приховування інформації. Класична стеганографія зародилася дуже давно. Перші згадки датуються V ст. до нашої ери в історичних працях Геродота. З тих пір було винайдено безліч способів: від нанесення інформації на воскові дощечки або голову слуги у вигляді татуювання до застосування мікрокрапок і симпатичних чорнила різного складу.

З появою комп'ютерів з'явилося два нових напрямки в стеганографії: комп'ютерний і цифровий.

Основне призначення комп'ютерної стеганографії – скритна передача даних. Вона включає в себе безліч методів, які використовують комп'ютерні формати даних, особливості файлової системи, невикористовувані сектора тощо. Однак вони відрізняються низькою надійністю і продуктивністю.

Найбільшого поширення набули методи, які використовують цифрову обробку сигналів. Даний напрямок отримав назву – цифрова стеганографія. Вона має кілька напрямків використання [4, 5]:

- вбудовування інформації в цифровий носій з метою його прихованої передачі;

- вбудовування ідентифікаційних номерів (fingerprinting);

- приховане анотування документів (captioning)

- цифрове маркування мультимедійної продукції (watermarking).

Серед даних методів для захисту мультимедійної продукції використовуються цифрове маркування і вбудовування ідентифікаційних номерів.

Вбудовування ідентифікаційних номерів захищає мультимедійну продукцію від незаконного поширення. Оскільки кожен ідентифікаційний номер є унікальним, легко відстежити джерело витоку.

Вбудовування ЦВЗ на даний момент – один з найефективніших методів захисту зображень від незаконного поширення. Цифрове маркування нараховує велику кількість алгоритмів, що володіють різним ступенем ефективності.

1.1.2 Цифрове маркування нерухомих зображень

Більшість досліджень цифрового маркування присвячено маркуванню цифрових нерухомих зображень, що обумовлено наступними факторами [4, 5]:

- слабка чутливість людського ока до вмісту в зображенні шуму, незначним спотворенням зображення і незначною зміною таких його параметрів, як колірна складова, яскравість, контрастність;

- практична необхідність – існує величезна кількість фотографій, картин, відеопродукції, що потребують захисту;

- фіксований обсяг інформації для приховування, який усуває обмеження, що виникають при встановленні в реальному часі цифрового водяного знаку в потоковий контейнер (має заздалегідь невідомий розмір);

- можливість вбудовування відносно великої кількості інформації з огляду на досить великий розмір зображення;

- велика різноманітність добре опрацьованих методів цифрової обробки зображення.

Остання причина, як зазначено в [4] значно ускладнює впровадження ЦВЗ в нерухоме зображення, оскільки, чим ефективніше методи цифрової обробки зображень, тим ефективніше розробляються алгоритми стиснення. Отже, зі збільшенням ефективності алгоритмів стиснення буде зменшуватися кількість доступної інформації для вбудовування.

1.1.3 Вимоги, що пред'являються до алгоритмів цифрового маркування

Існує ряд обов'язкових вимог, що пред'являються до цифрових стеганографічним алгоритмам, основними з яких є [4-9]:

- стійкість (робастність);

- невиявленість;

- невидимість.

Стійкість стеганографічного алгоритму полягає в здатності ЦВЗ зберігати свій первісний вигляд після впливу на стеганоконтейнер атак різного типу.

Невиявленість полягає в здатності протистояти різним методам стеганоаналізу: [10-21], які використовує стеганоаналітік для виявлення факту присутності ЦВЗ в контейнері.

Невидимість характеризується здатністю алгоритму не вносити видимих людським оком змін у зовнішній вигляд контейнера. Отже, необхідно враховувати особливості зорової системи людини, які діляться на дві категорії [4]:

- низькочастотні, до яких відносяться чутливість людського ока до змін яскравості зображення, його частотної складової, а також ефекту маскування;

- високочастотні, які проявляються в підстроювання мозком низькочастотних властивостей під зображення (наприклад, чутливість до

контрасту, розміру, форми, кольору, розташуванню окремих об'єктів зображення).

Варто відзначити, що надійність стеганографічної системи залежить від обсягу вбудованого ЦВЗ [6]. Отже, необхідне дотримання компромісу між рівнем надійності вбудовування та обсягом ЦВЗ. На рис. 1.1 [6] відображена дана залежність при постійному розмірі контейнера.

Рисунок 1.1 – Залежність стійкості стеганографічної системи від обсягу вбудованого ЦВЗ

Крім перерахованих вище вимог стеганографічний алгоритм повинен володіти прийнятною обчислювальною складністю.

1.1.4 Класифікація цифрових водяних знаків, впроваджуваних в нерухомі зображення

За призначенням ЦВЗ діляться на [1-10]:

- тендітні;
- напівкрихкі;
- стійкі (робастні).

Головне призначення тендітних цифрових водяних знаків – перевірка справжності (аутентифікація) контейнера, в який вони вбудовані. Крім того,

тендітні ЦВЗ повинні визначати місце змін стеганоконтейнера і забезпечувати його відновлення. Тендітні ЦВЗ руйнуються при найменшому шкідливому впливі на контейнер.

Напівкрихкі ЦВЗ мають виборчу стійкість, наприклад стійкість до JPEG-стиску, в разі, якщо автору знадобиться стиснути зображення.

На відміну від вузькоспеціалізованого напрямку аутентифікації робастні ЦВЗ застосовуються для захисту від незаконного поширення і захисту авторських прав. Отже, вони повинні володіти стійкістю до атак різного типу.

По видимості ЦВЗ підрозділяються на видимі і невидимі. Переважно використання невидимих ЦВЗ, оскільки:

- ступінь погіршення якості зображення після їх вбудовування значно менше, ніж при цифровому маркуванні видимим ЦВЗ;

- видимі ЦВЗ не задовольняють вимозі непомітності.

1.1.5 Класифікація атак на системи цифрового маркування

Серед великої кількості робіт, присвячених класифікації атак зловмисників на системи цифрового маркування [1-10] найбільш повна приведена в літературі [21], схема з якої відображена на рис. 1.2.

Згідно з цією класифікацією всі атаки проти систем цифрового маркування можна розділити на два класи: системні атаки і неавторизований вплив.

Системні атаки використовують помилки в роботі стеганографічної системи. Прикладом шкідливого впливу даного типу є мозаїчна атака, що застосовується в мережі Інтернет. При використанні мозаїчної атаки стеганоконтейнер розбивається на окремі фрагменти, які занадто малі, щоб зберігати в собі ЦВЗ. На сторінці Інтернет-сайту дані фрагменти розміщуються поруч один з одним, візуально утворюючи початкове зображення.

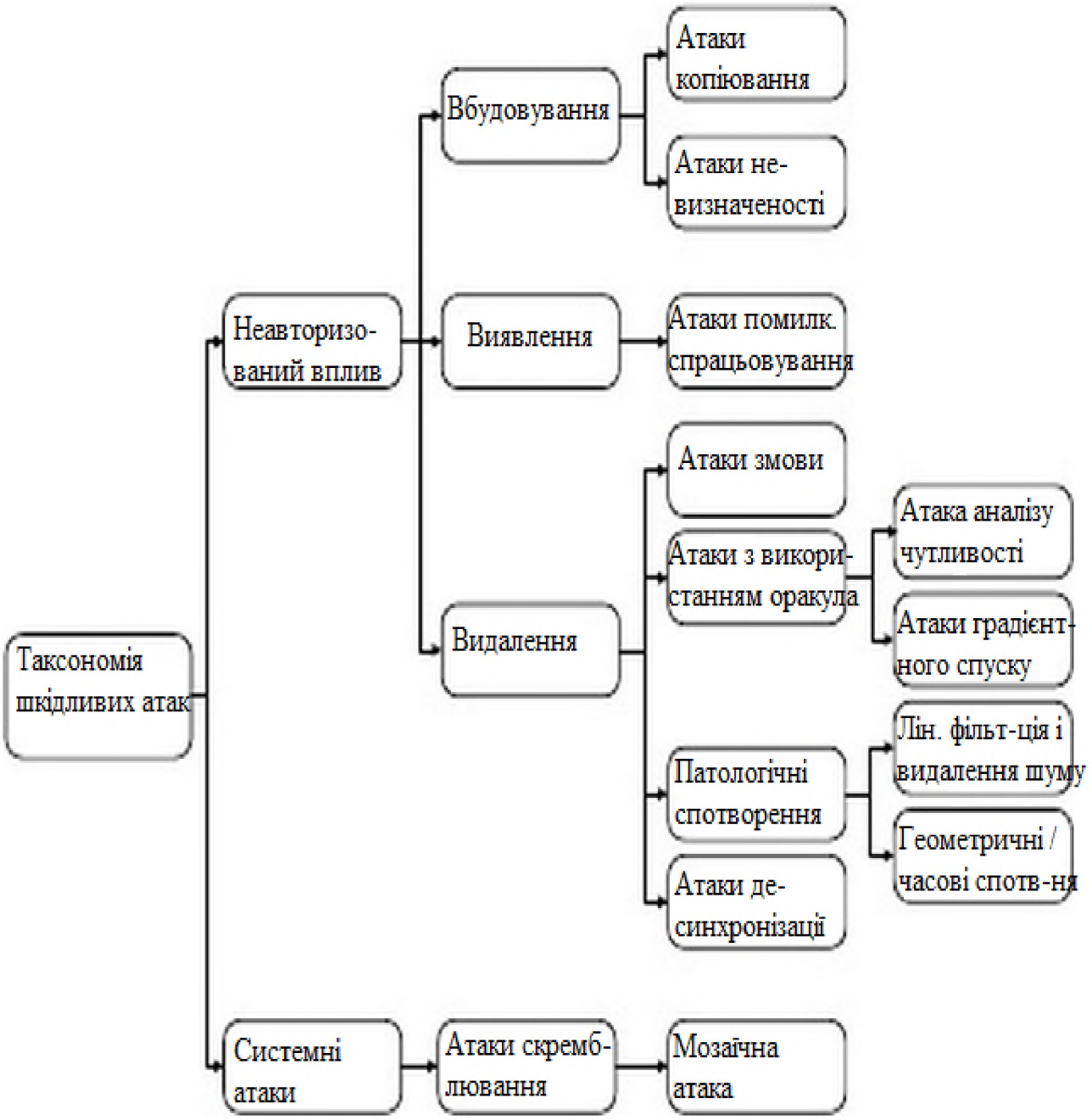


Рисунок 1.2 – Класифікація атак на системи цифрового маркування

Атаки неавторизованого впливу використовують уразливості в системі цифрового маркування і в свою чергу поділяються на атаки неавторизованого вбудовування, виявлення і видалення ЦВЗ відповідно.

При неавторизованому вбудовуванні зловмисник вбудовує свій ЦВЗ в стеганографічний контейнер.

Атаки неавторизованого виявлення спрямовані на встановлення факту присутності ЦВЗ в стеганоконтейнері або на імітацію присутності ЦВЗ в

контейнері (атака помилкового спрацьовування) при наявності детектора у зловмисника.

Використовуючи атаки неавторизованого видалення, зловмисник прагне повністю видалити ЦВЗ з стеганоконтейнера (наприклад, лінійна фільтрація) або зробити водяний знак невидимим для детектора (геометричні атаки).

Одним з найпоширеніших шкідливих впливів на системи цифрового маркування є компресія зображення у зв'язку з широким розповсюдженням в мережі Інтернет графічного формату JPEG, а також більш ефективного формату JPEG2000, що набирає популярність.

1.1.6 Алгоритми маркування цифрових зображень

Незважаючи на те, що цифрова стеганографія – молода наука, на сьогоднішній день вона налічує велику кількість алгоритмів впровадження ЦВЗ, що підрозділяються на кілька класів. Узагальнена класифікація алгоритмів представлена на рис. 1.3.

За ступенем оборотності ЦВЗ алгоритми цифрового маркування діляться на оборотні та необоротні. Необоротні алгоритми вбудовують ЦВЗ, викликаючи при цьому незворотні викривлення контейнера. Одна з головних задач при розробці подібних алгоритмів – максимально знизити рівень внесених спотворень [1-11]. На відміну від незворотних алгоритмів оборотні здатні крім вилучення ЦВЗ повністю відновити первісний вигляд зображення. Оборотні алгоритми особливо актуальні в області захисту військових і медичних зображень, що не допускають навіть незначного візуального спотворення.

За способом вбудовування алгоритми цифрового маркування діляться на [1-11]:

1. Лінійні алгоритми (адитивні алгоритми) – полягають в лінійній модифікації початкового зображення, а її витягання в декодері проводиться

кореляційними методами. При цьому ЦВЗ зазвичай складається із зображенням-контейнером, або «вплавляється» (fusion) до нього.

2. Нелінійні алгоритми на основі скалярного або векторного квантування, де під квантуванням розуміється процес зіставлення великої (можливо й нескінченної) безлічі значень з деякою кінцевою безліччю чисел.

3. Алгоритми, що використовують фрактальне кодування, особливістю якого є пошук послідовності афінних перетворень (поворот, зсув, масштабування), що дозволяють апроксимувати блоки зображення малого розміру (рангові) блоками більшого розміру (доменами).

Рисунок 1.3 – Класифікація алгоритмів цифрового маркування нерухомих зображень

1.2 Цифрові формати нерухомих зображень. Особливості комп'ютерної обробки зображень

1.2.1 Формат BMP

За рішенням розроблювачів формат BMP-файла не прив'язаний до конкретної апаратної платформи [8]. Цей файл складається із чотирьох частин: заголовка, інформаційного заголовка, таблиці кольорів (палітри) і даних зображення. Якщо у файлі зберігається зображення із глибиною кольору 24 біти (16 млн. кольорів), то таблиця кольорів може бути відсутньою, однак у нашому 256-кольоровому випадку вона є. Структура кожної із частин файла, що зберігає 256-кольорове зображення, подана в табл. 1.1.

Заголовок файлу починається із сигнатури "BM", а потім іде довжина файлу, виражена в байтах. Наступні 4 байти зарезервовані для подальших розширень формату, а закінчується цей заголовок зсувом від початку файла до записаних у ньому даних зображення. При 256 кольорах цей зсув становить 1078 – саме стільки й доводиться пропустити, щоб добратися до даних.

Інформаційний заголовок починається із власної довжини (вона може змінюватися, але для 256-кольорового файлу становить 40 байтів) і містить розміри зображення, роздільну здатність, характеристики подання кольору й інших параметрів.

Ширина та висота зображення задаються в точках растра й пояснень, мабуть, не вимагають.

Кількість площин, що можуть застосовуватися у файлах, які мають невелику глибину кольору. При кількості кольорів 256 і більше вона завжди дорівнює 1, тому зараз це поле вже можна вважати застарілим, але для сумісності воно зберігається.

Глибина кольору вважається найважливішою характеристикою способу подання кольору у файлі й виміряється в бітах на точку. У цьому випадку вона дорівнює 8.

Таблиця 1.1 – Структура BMP-файлу

Ім'я	Довжина	Зсув	Опис
Заголовок файла (BitMapFileHeader)			
Type	2	0	Сигнатура "BM"
Size	4	2	Розмір файла
Reserved 1	2	6	Зарезервовано
Reserved 2	2	8	Зарезервовано
OffsetBits	4	10	Зсув зображення від початку файла
Інформаційний заголовок (BitMapInfoHeader)			
Size	4	14	Довжина заголовка
Width	4	18	Ширина зображення, точка
Height	4	22	Висота зображення, точка
Planes	2	26	Кількість площин
BitCount	2	28	Глибина кольору, бітів на точку
Compression	4	30	Тип компресії (0 – незжате зображення)
SizeImage	4	34	Розмір зображення, байт
XpelsPerMeter	4	38	Горизонтальна роздільна здатність, точка на метр
YpelsPerMeter	4	42	Вертикальна роздільна здатність, точка на метр
ColorsUsed	4	46	Кількість використовуваних кольорів (0 – максимально можливе для даної глибини кольору)
ColorsImportant	4	50	Кількість основних кольорів
Таблиця кольорів (палітра) (ColorTable)			
ColorTable	1024	54	256 елементів по 4 байти
Дані зображення (BitMap Array)			
Image	Size	1078	Зображення, записане рядками злава направо і знизу вгору

Компресія в BMP-файлах звичайно не використовується, але поле в заголовку для неї передбачено. Звичайно вона дорівнює 0, і це означає, що зображення не стисле. Надалі будемо використовувати тільки такі файли.

Розмір зображення – кількість байтів пам'яті, що вимагаються для зберігання цього зображення, не вважаючи даної палітри.

Горизонтальний і вертикальний роздільні здатності виміряються в точках растра на метр. Вони особливо важливі для збереження масштабу відсканованих картинок. Зображення, створені за допомогою графічних редакторів, як правило, мають у цих полях нулі.

Кількість кольорів дозволяє скоротити розмір таблиці палітри, якщо в зображенні реально присутньо менше кольорів, чим це допускає обрана глибина кольору. Однак на практиці такі файли майже не зустрічаються. Якщо кількість кольорів приймає значення, максимально припустиме глибиною кольору, наприклад 256 кольорів при 8 бітах, полі обнуляють.

Кількість основних кольорів – іде з початку палітри, і його бажано виводити без перекручувань. Дане поле буває важливе тоді, коли максимальна кількість кольорів дисплея була менше, ніж у палітрі BMP-файла. При розробці формату, мабуть, приймалося, що кольорі, які найбільш часто зустрічаються, будуть розташовуватися на початку таблиці. Зараз цієї вимоги практично не дотримуються, тобто кольори не впорядковуються по частоті, з якою вони зустрічаються у файлі. Це дуже важливо, оскільки палітри двох різних файлів, навіть складених з тих самих кольорів, містили б їх (кольори) у різному порядку, що могло істотно ускладнити одночасне виведення таких зображень на екран.

За інформаційним заголовком слідує таблиця кольорів, що становить масив з 256 (за кількістю кольорів) 4-байтових полів. Кожне поле відповідає своєму кольору в палітрі, а три байти із чотирьох – компонентам синьої, зеленої і червоної складових для цього кольору. Останній, найстарший байт кожного поля зарезервований і дорівнює 0.

Після таблиці кольорів знаходяться дані зображення, що по рядках растра записані знизу вгору, а усередині рядка – зліва направо. Оскільки на деяких платформах неможливо визначити одиницю даних, що менше 4 байтів, довжина кожного рядка вирівняна на границю в 4 байти, тобто при довжині рядка, некратній чотирьом, вона доповнюється нулями. Цю обставину

обов'язково треба враховувати при зчитуванні файла, хоча, можливо, краще заздалегідь подбати, щоб горизонтальні розміри всіх зображень були кратні 4.

Формат файлу був розроблений універсальним для різних платформ, тому немає нічого дивного в тому, що кольори палітри зберігаються в ньому інакше, чим прийнято для VGA. Під час виконання процедури читання виробляється необхідне перекодування.

1.2.2 Формат GIF

"GIF" – це стандарт фірми CompuServe для визначення растрових кольорових зображень [8]. Цей формат дозволяє висвічувати на різному встаткуванні графічні високоякісні зображення з більшою роздільною здатністю і має на увазі механізм обміну й висвічування зображень. Описаний у справжньому документі формат зображень був розроблений для підтримки теперішньої й майбутньої технології обробки зображень і буде надалі основою для майбутніх графічних продуктів CompuServe.

Головне завдання справжнього документа полягає в тому, щоб забезпечити програмістів необхідною технічною інформацією для написання декодерів і кодерів GIF. Тому в документі використовується термінологія, пов'язана із загальними питаннями графіків і програмування. Перший розділ справжнього документа описує формат даних GIF і його компоненти в додатку до декодерів GIF, поза залежністю від того чи є вони окремою програмою або частиною пакета зв'язку. Додаток В відноситься до декодерів, що є частиною пакетів зв'язку й описує протокол, необхідний для входу та існування режиму GIF, і відповідає на ряд специфічних питань. Загальний формат файлу GIF надано на рис. 1.4.

Наявність на початку файлу спеціального "підпису" указує, що наступні дані є дійсно потоком даних зображення у форматі GIF. Цей "підпис" складається з таких шести символів: GIF 87a. Три останніх символи "87a" можуть розглядатися як номер версії для даного конкретного визначення GIF.

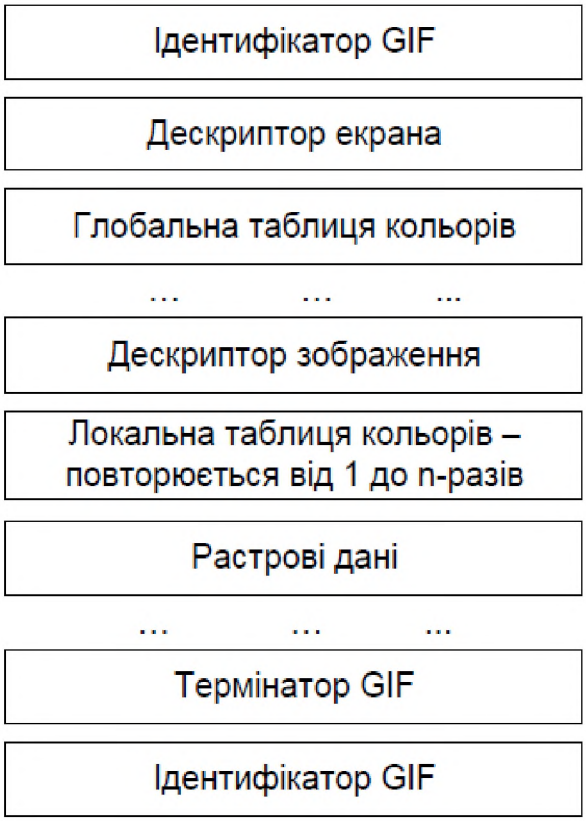


Рисунок 1.4 – Загальний формат файлу GIF

Дескриптор екрана описує загальні параметри для всіх наступних зображень у форматі GIF. Він визначає розміри простору зображення 30 або необхідного логічного екрана, існування інформації про таблицю кольорів і "глибину" екрана.

Глобальна таблиця кольорів є необов'язковою і рекомендується для зображень, де потрібна точна передача кольорів.

Дескриптор зображення визначає дійсне розташування та розміри наступного зображення усередині простору, визначеного в дескрипторі екрана. Також визначаються прапори, що вказують на присутність локальної таблиці для пошуку кольорів і визначення послідовності пікселів. Кожний дескриптор зображення починається із символу-роздільника зображень.

Растрові дані – формат самого зображення визначений як серія значень номерів пікселів, які утворять зображення. Пікселі запам'ятовуються зліва направо послідовно рядками зображення.

Термінатор GIF. Для того щоб забезпечити синхронізацію із закінченням файлу зображення GIF, декодер GIF повинен обробляти закінчення режиму GIF по символі шістнадцятирічне 0×3B або ";", знайденому після закінчення обробки зображення. За згодою декодувальні програми повинні робити паузу і чекати дій, які вказують, що користувач готовий до продовження. Це може бути повернення каретки, уведення із клавіатури або клацання кнопкою миші. Для інтерактивних додатків ці дії користувача повинні бути передані в ядро програми як переведення каретки, для того, щоб обчислювальний процес міг тривати. Звичайно декодувальна програма залишає графічний режим і вертається до попереднього процесу.

1.2.3 Формат JPEG

JPEG з'явився методом стиску, що дозволяє стискати дані повнокольорових багатоградаційних зображень із глибиною від 6 до 24 бітів/піксел з досить високою швидкістю та ефективністю. Сьогодні JPEG – це схема стиску зображень, що дозволяє досягти дуже високих коефіцієнтів стиску. Правда максимальний стиск графічної інформації, як правило, пов'язаний з певною втратою інформації. Тобто для досягнення високого ступеня стиску алгоритм так змінює вихідні дані, що одержуване після відновлення зображення буде відрізнятися від вихідного (стисливого). Цей метод стиску використовується для роботи з повнокольоровими зображеннями високої фотографічної якості. JPEG не був визначений як стандартний формат файлів зображень, однак на його основі були створені нові або модифіковані існуючі файлові формати.

Алгоритм обробки даних JPEG. Специфікація JPEG визначає мінімальні вимоги стандарту, які повинні підтримуватися всіма програмами, що використовують цей метод. JPEG заснований на схемі кодування, що базується на дискретних косинус-перетвореннях (ДКП, DCT). ДКП – це загальне ім'я визначеного класу операцій, дані про які були опубліковані кілька років назад.

Алгоритми, що базуються на ДКП, стали основою різних методів стиску. Ці алгоритми стиску базуються не на пошуці однакових атрибутів пікселів (як в RLE і LZW), а на різниці між ними.

У силу своєї природи вони завжди кодують із втратами, але здатні забезпечити високий ступінь стиску при мінімальних втратах даних. Схема JPEG ефективна тільки при стиску багатоградаційних зображень, у яких розходження між сусідніми пікселями, як правило, досить незначні. Практично JPEG добре працює тільки із зображеннями, що мають глибину хоча б 4 або 5 бітів/піксел на колірний канал. Основи стандарту визначають глибину вхідного зразка в 8 бітів/піксел. Дані з меншою бітовою глибиною можуть бути оброблені за допомогою масштабування до 8 бітів/піксел, але результат для вихідних даних з низькою глибиною кольору може бути незадовільним, оскільки між атрибутами сусідніх пікселів будуть істотні розходження. За подібними причинами погано обробляються вихідні дані на основі кольорових таблиць, особливо якщо зображення представляється в розмитому вигляді.

Процес стиску за схемою JPEG представлено на рис. 1.5.

Процес стиску за схемою JPEG включає ряд етапів (рис. 1.5):

1. Перетворення зображення в оптимальний колірний простір.

2. Субдискретизація компонентів кольоровості усередненням груп пікселей.

3. Застосування дискретних косинус-перетворень для зменшення надмірності даних зображення.

4. Квантування кожного блоку коефіцієнтів ДКП із застосуванням вагових функцій, оптимізованих з урахуванням візуального сприйняття людиною.

5. Кодування результуючих коефіцієнтів (даних зображення) із застосуванням алгоритму Хаффмена для видалення надмірності інформації.

При цьому слід звернути увагу на те, що декодування JPEG здійснюється у зворотному порядку.

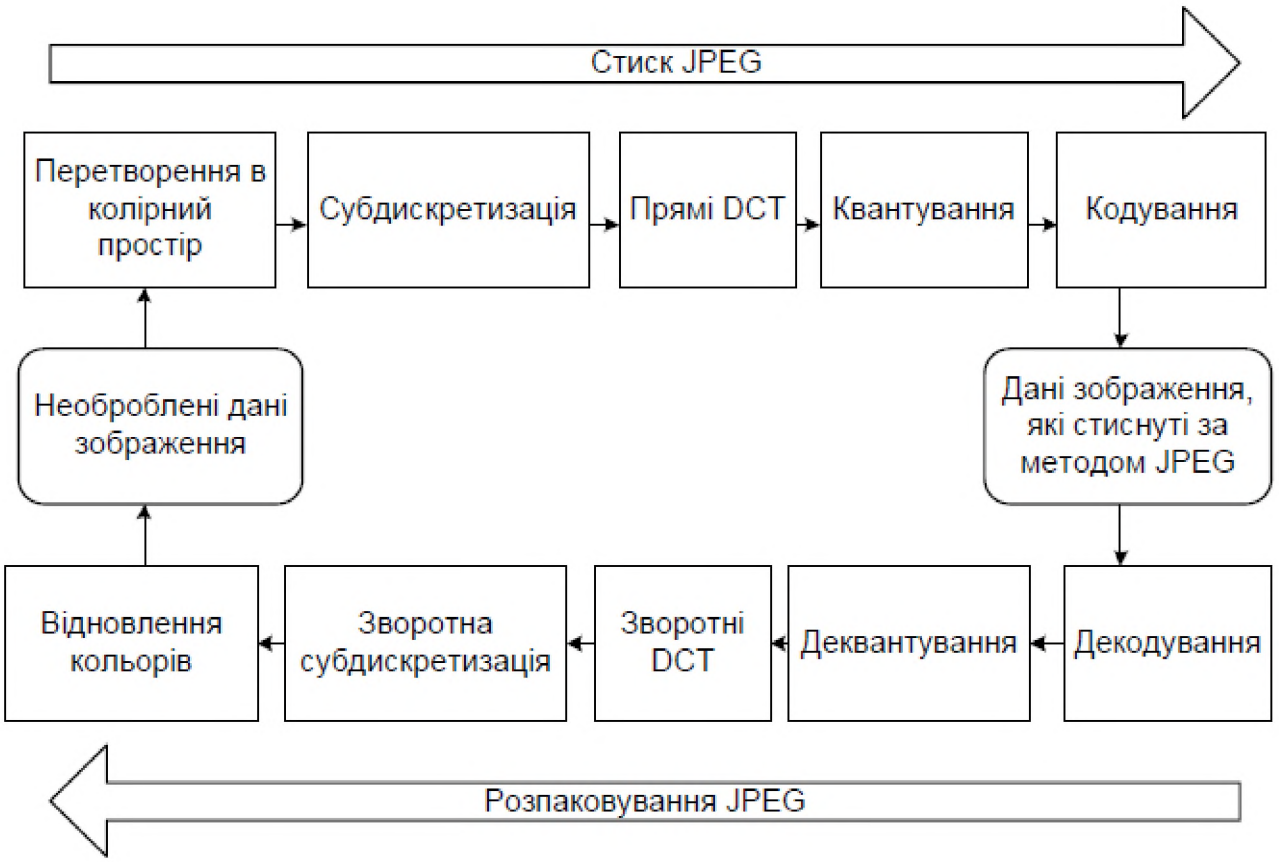


Рисунок 1.5 – Структура JPEG-перетворень

1.3 Дискримінантний аналіз

Дискримінантний аналіз – розділ обчислювальної математики, багатовимірного статистичного аналізу, що представляє набір методів статистичного аналізу для вирішення задач розпізнавання образів, класифікації багатовимірних спостережень за принципом максимальної схожості при наявності навчальних ознак [22-26]. Дискримінантний аналіз використовується для прийняття рішення про те, які змінні поділяють (тобто «дискримінують») вихідний набор даних, тобто виділяють так звані «групи». На відміну від кластерного аналізу в дискримінантному аналізі групи відомі апріорі. Головні завдання дискримінантного аналізу наведено на рис. 1.6.

Обмеження для використання дискримінантного аналізу наведено на рис. 1.7.

Рисунок 1.6 – Головні завдання дискримінантного аналізу

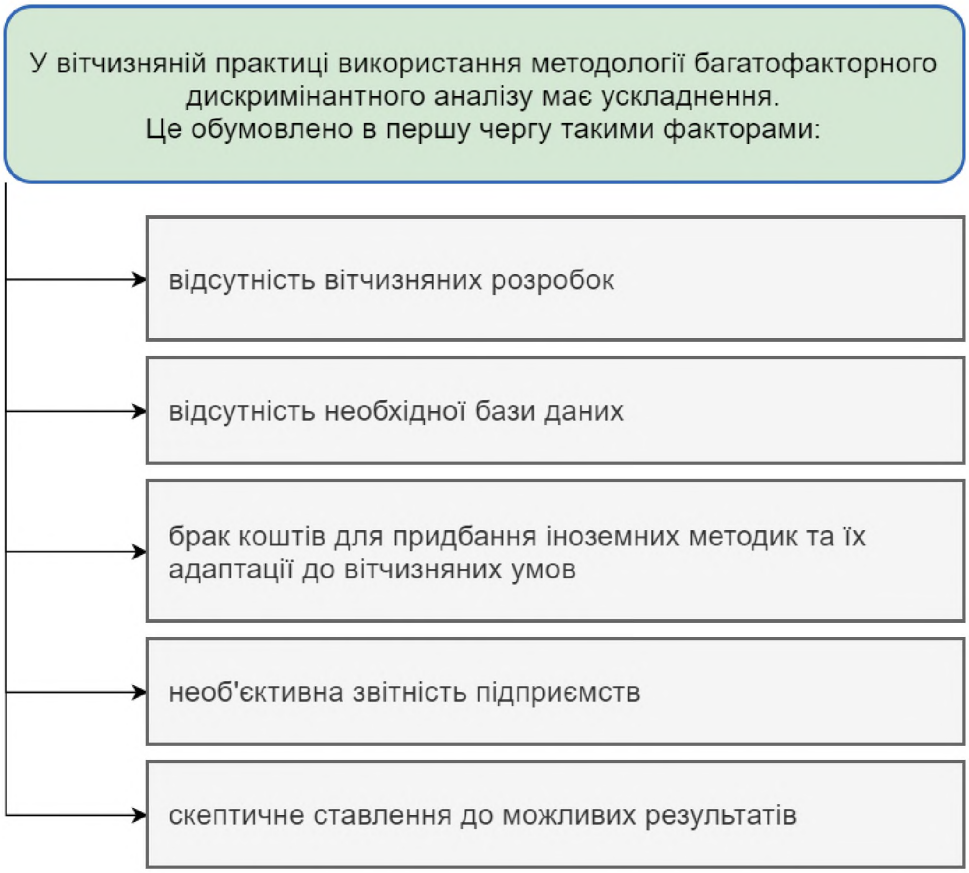


Рисунок 1.7 – Обмеження для використання дискримінантного аналізу

Основні положення дискримінантного аналізу легко зрозуміти з уявлення щодо досліджуваної області, яка складається з окремих сукупностей, кожна з яких характеризується змінними з багатовимірним нормальним розподілом.

Дискримінантний аналіз намагається знайти лінійні комбінації таких показників, які найкращим чином поділяють представлені сукупності.

Основні проблеми у використанні дискримінантного аналізу наведено на рис. 1.8.

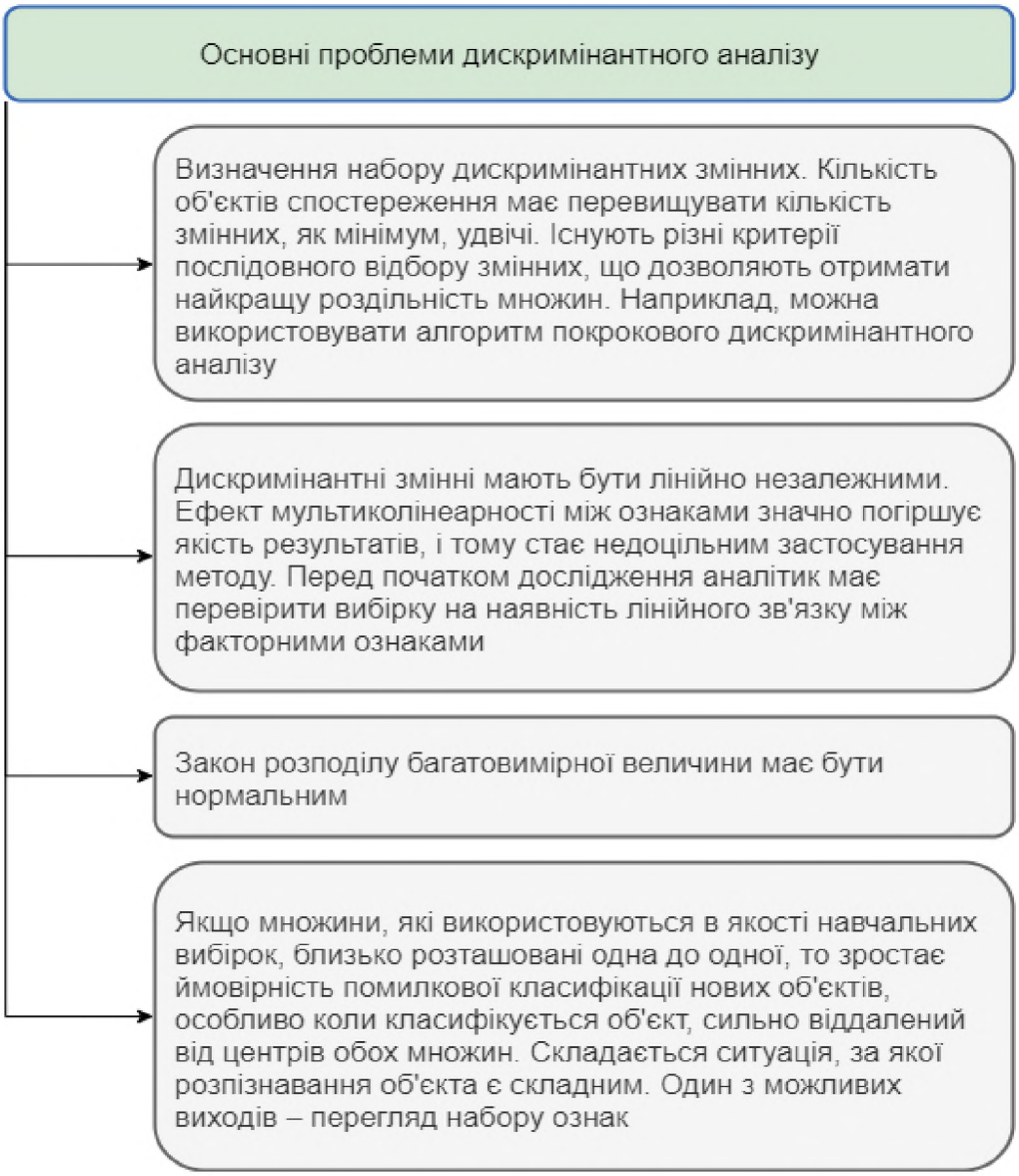


Рисунок 1.8 – Проблеми використання дискримінантного аналізу

При використанні методу дискримінантного аналізу головним показником є точність класифікації, і цей показник можна легко визначити, оцінивши частку правильно класифікованих елементів. Якщо дослідник працює з досить великою вибіркою, застосовується наступний підхід: виконується аналіз по частині даних (наприклад, по половині), а потім прогностичне

рівняння застосовується для класифікації спостережень у другій половині даних. Далі оцінюється точність прогнозу, тобто відбувається перехресна верифікація. У дискримінантному аналізі існують методи покрокового відбору змінних, які допомагають здійснити вибір прогностичних змінних.

У дискримінантному аналізі формулюється правило, за яким об'єкти підмножини підлягає класифікації відносяться до одного з уже існуючих (навчальних) підмножин (класів). У загальному випадку задача розрізнення (дискримінації) формулюється таким чином. Нехай результатом спостереження над об'єктом є реалізація k-мірного випадкового вектора $\vec{x} = (x_1, x_2, ..., x_k)$. Потрібно встановити правило, згідно з яким за спостереженнями значенням вектора $\vec{x}$ об'єкт відносять до однієї з можливих сукупностей c_i, i=1,..,*l*. Для побудови правила дискримінації простір R значень вектора $\vec{x}$ розбивається на області R_i, i=1,..,*l* так, що при попаданні $\vec{x}$ в R_i об'єкт відносять до сукупності X_i.

Правило дискримінації вибирається відповідно до визначеного принципом оптимальності на основі апріорної інформації щодо об'єкта з X_i. При цьому слід враховувати розмір збитку від неправильної дискримінації. Апріорна інформація може бути представлена як у вигляді деяких відомостей щодо функції розподілу ознак у кожної сукупності, так і у вигляді вибірок з цих сукупностей. Апріорні ймовірності можуть бути задані, або ні. Очевидно, що рекомендації будуть тим точніше, чим повніше вихідна інформація. З точки зору застосування дискримінантного аналізу найважливішою є ситуація, коли вихідна інформація щодо розподілу представлена вибірками.

У цьому випадку завдання дискримінації ставиться таким чином.

Нехай $x_1^{(i)}, ..., x_{ni}^{(i)}$ вибірка із сукупності π_i, i=1,..,*l*, причому кожен j-й об'єкт вибірки представлений k-мірним вектором параметрів $x_j^{(i)} = \left(x_{j1}^{(i)}, ..., x_{jk}^{(i)}\right)$. Проведено додаткове спостереження $x = (x_1, ..., x_k)$ над об'єктом, що належить до однієї із сукупностей X_i.

Потрібно побудувати правило віднесення спостереження *x* до однієї з цих сукупностей.

Зазвичай у завданні розрізнення переходять від вектора ознак, що характеризують об'єкт, до лінійної функції від них, дискримінантної функції, гіперплощини, що найкращим чином розділяє сукупність вибіркових точок.

Найбільш вивчений випадок, коли відомо, що розподіл векторів ознак у кожній сукупності нормальний, але немає інформації про параметри цих розподілів. Тут природно замінити невідомі параметри розподілу в дискримінантній функції їх найкращими оцінками. Правило дискримінації можна засновувати на відношенні правдоподібності. Непараметричні методи дискримінації не вимагають знань щодо точного функціонального вигляду розподілів і дозволяють вирішувати завдання дискримінації на основі незначної апріорної інформації щодо сукупностей, що особливо цінно для практичних застосувань.

У параметричних методах ці точки використовуються для оцінки параметрів статистичних функцій розподілу. При цьому, як правило, використовується нормальний розподіл.

1.3.1 Лінійний дискримінантний аналіз

Лінійний дискримінантний аналіз або LDA (Linear Discriminant Analysis) – це найстаріший з методів класифікації, розроблений Р. Фішером [22-26]. Лінійний дискримінантний аналіз – це метод пошуку лінійної комбінації змінних, що найкращим чином розділяє деяку множину об’єктів на два або більше класів.

Слід зазначити, що під загальною назвою LDA об'єднано декілька схожих методів, що розрізняються вимогами до властивостей вибірки. Нижче розглянуто один з цих методів, при якому висуваються лише дві вимоги до вибірки: 1) розмір вибірки повинен перевершувати число змінних; 2) класи можуть перетинатися, але їх центри повинні бути віддалені один від одного.

Висуваються припущення:

1. Є різні класи об'єктів.

2. Кожен клас має нормальну функцію щільності від n змінних:

$$f_i(x)_{rz} = (2\pi)^{-1/2} \left|\Sigma_i\right|^{-1/2} \exp\left(-\frac{1}{2}\left(x - \mu^{(i)}\right) \right)^T \Sigma_i^{-1} \left(x - \mu^{(i)}\right), \quad (1.1)$$

де μ(i) – вектор математичних очікувань змінних розмірності k; $\sum_i$ – коваріаційна матриця, позитивно визначена; $\sum_i^{-1}$ – обернена коваріаційна матриця.

Коваріаційна матриця – це матриця, утворена з попарних коваріацій кількох випадкових величин; точніше, для k-мірного випадкового вектора $X = (X_1,...,X_k)$ коваріаційна матриця – це квадратна матриця:

$$\sum = E(X - EX)(X - EX)^T \quad (1.2)$$

де $EX = (EX_1,...,EX_k)$ – вектор середніх значень.

Компоненти коваріаційної матриці дорівнюють:

$$\sigma_{ij} = E\left[(X_i - EX_i)(X_j - EX_j)\right] = cov(X_i, X_j), \quad i, j = 1 \ldots k, \quad (1.3)$$

і при $i=j$ збігаються з DX_i (тобто на головній діагоналі знаходяться дисперсії величин X_i).

Головною проблемою в методі LDA є звернення матриці ∑. Якщо вона вироджена, то метод використовувати не можна.

У разі, якщо параметри відомі, дискримінацію можна провести наступним чином.

Нехай існують функції щільності $f_1(x), f_2(x), \ldots, f_i(x)$ нормально розподілених класів. Задана точка *x* в просторі *k* вимірювань. Припускаючи, що точка *x* має найбільшу щільність, необхідно віднести цю точку до і-го класу. Існує теорема, яка доводить, що якщо апріорні ймовірності для визначених точок кожного класу однакові і втрати при неправильної класифікації *i*-ї групи в якості *j*-й не залежать від *i* та *j*, то вирішальна процедура мінімізує очікувані втрати при неправильної класифікації.

Нижче наведено приклад оцінки параметра багатовимірного нормального розподілу $\hat{\mu}^{(i)}$ і $\sum$, які можуть бути оцінені за вибірковими даними.

Нехай задано вибірку $\left(x_1^{(i)}, x_2^{(i)}, \ldots, x_m^{(i)}\right) = x_i, (i = 1, \ldots, l)$. Математичні очікування $\mu_1, \mu_2, \ldots, \mu_k$ можуть бути оцінені середніми значеннями:

$$\hat{\mu}_q^{(i)} = \frac{1}{n_i} \sum_{j=1}^{ni} x_{jq}^{(i)}, \; q = 1 \ldots k. \tag{1.4}$$

Незміщені оцінки елементів коваріаційної матриці $\sum$ є

$$\left(\hat{\sum}_i \right)_{rs} = \frac{1}{n_l - 1} \sum_{j=1}^{ni} \left(x_{jr}^{(i)} - \hat{\mu}_r^{(i)} \right) \left(x_{js}^{(i)} - \hat{\mu}_s^{(i)} \right); \;\; r, s = 1, \ldots, k \tag{1.5}$$

Отже, можна визначити $\hat{\mu}^{(i)}$ і $\hat{\sum}_i$ за вибірками у кожному класі, отримавши оцінки, точку *x* необхідно віднести до класу, для якої функція *f* максимальна.

Вводиться припущення, що всі класи, серед яких повинна проводитися дискримінація, мають нормальний розподіл з однаковою коваріаційною матрицею $\sum$. У результаті істотно спрощується вираз для дискримінантної функції. Клас, до якого повинна належати точка *x*, можна визначити на основі нерівності

$$f_i(x) > f_{j(x)} \tag{1.6}$$

Необхідно скористатися наведеною вище формулою для випадку, коли їх коваріаційні матриці рівні: $\sum_i = \sum_j = \sum$, а $\mu^{(i)}$ – це вектор математичних очікувань класу *i*. Тоді наведену умову-нерівність можна представити у вигляді:

$$-\left[(x - \mu^{(i)})^T \Sigma^{-1} (x - \mu^{(i)}) \right] > -\left[(x - \mu^{(j)})^T \Sigma^{-1} (x - \mu^{(j)}) \right]. \tag{1.7}$$

Зауважимо, що якщо є два вектори M і W, то скалярний добуток можна записати у вигляді $Z^T W = W^T Z = (Z, W)$. У наведеному виразі-нерівності необхідно виключити $x^T \Sigma^{-1} x$ справа і зліва, поміняти у всіх членів суми знаки. Тоді вираз виглядає наступним чином:

$$(x, \Sigma^{-1} \mu^{(i)} - \frac{1}{2} (\mu^{(i)}, \Sigma^{-1} \mu^{(i)}) > (x, \Sigma^{-1} \mu^{(j)} - \frac{1}{2} (\mu^{(j)}, \Sigma^{-1} \mu^{(j)}) \tag{1.8}$$

Внесемо позначення:

$$v^{(i)} = \Sigma^{-1}\mu^{(i)}, \quad i = 1,\ldots,m, \tag{1.9}$$

$$\lambda_i = \frac{1}{2}\left(\mu^{(i)}, \Sigma^{-1}\mu^{(i)}\right), \quad i = 1,\ldots,m. \tag{1.10}$$

Тоді нерівність прийме остаточний вигляд:

$$\left(x, v^{(i)}\right) - \lambda_i > \left(x, v^{(j)}\right) - \lambda_j. \tag{1.11}$$

Наслідок: точка *x* належить до класу *i*, для якого лінійна функція:

$$h_i(x) = \left(x, v^{(i)}\right) - \lambda_i = max. \tag{1.12}$$

Перевага методу лінійної дискримінації Фішера полягає в лінійності дискримінантної функції і надійності оцінок коваріаційних матриць класів. Розглянемо частковий випадок, коли навчальний набір складається з двох матриць X_1 і X_2, в яких є по I_1 та I_2 рядків (зразків). Число змінних (стовпців) однаково – J. Вихідні припущення полягають у наступному:

1.Кожен клас (k=1 або 2) має нормальний розподіл $N(\mu_k, \sum_k)$.

2. Коваріаційні матриці цих класів однакові: $\sum_i = \sum_j = \sum$.

Класифікаційне правило в LDA дуже просте – новий зразок x відноситься до того класу, до якого він ближче по метриці Махаланобіса:

$$d_k = (x - \mu_k)\Sigma^{-1}(x - \mu_k)^T, \quad k = 1,2. \tag{1.13}$$

Як вже було показано, невідомі математичні очікування і коваріаційна матриця замінюються їхніми оцінками:

$$m_k = \frac{1}{I_k}\sum_{i=1}^{I_k} x_i, \quad S = \frac{1}{I_1 + I_2 - 2}\left(\tilde{X}_1^T\tilde{X}_1 + \tilde{X}_2^T\tilde{X}_2\right). \tag{1.14}$$

У цих формулах $\vec{X}_k$ позначає центровану матрицю X_k. Якщо прирівняти відстані $d_1 = d_2$, то можна знайти рівняння кривої, що розділяє класи. При цьому квадратичні члени $xS^{-1}x^t$ скорочуються, і рівняння стає лінійним

$$xw_1^t - v_1 = xw_2^t - v_2, \tag{1.15}$$

де

$$w_k = m_k S^{-1}, v_k = 0.5 m_k S^{-1} m_k^t. \tag{1.16}$$

Величини, що стоять в різних частинах рівняння називаються LDA-рахунками, f_1 і f_2. Зразок відноситься до класу 1, якщо $f_1 > f_2$, і, навпаки, до класу 2, якщо $f_1 < f_2$.

1.3.2 Алгоритм дискримінантного аналізу

Нехай є дві генеральні сукупності X і Y, що мають нормальний закон розподілу з невідомими, але рівними коваріаційними матрицями.

Алгоритм виконання дискримінантного аналізу включає наступні основні етапи.

Вихідні дані представляються або в табличній формі у вигляді q підмножин (навчальних вибірок) M_k і підмножини M_0 об'єктів, які підлягають дискримінації, або відразу у вигляді матриць $X^{(1)}, X^{(2)}, \ldots, X^{(q)}$, розміром $(n_k \times p)$:

$$X^{(1)} = \begin{pmatrix} x_{1,1}^{(1)} & x_{1,2}^{(1)} & \cdots & x_{1,p}^{(1)} \\ x_{2,1}^{(1)} & x_{2,2}^{(1)} & \cdots & x_{2,p}^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n_1,1}^{(1)} & x_{n_1,2}^{(1)} & \cdots & x_{n_1,p}^{(1)} \end{pmatrix} \tag{1.17}$$

$$X^{(2)} = \begin{pmatrix} x_{1,1}^{(2)} & x_{1,2}^{(2)} & \cdots & x_{1,p}^{(2)} \\ x_{2,1}^{(2)} & x_{2,2}^{(2)} & \cdots & x_{2,p}^{(2)} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n_2,1}^{(2)} & x_{n_2,2}^{(2)} & \cdots & x_{n_2,p}^{(2)} \end{pmatrix} \tag{1.18}$$

$$X^{(q)} = \begin{pmatrix} x_{1,1}^{(q)} & x_{1,2}^{(q)} & \cdots & x_{1,p}^{(q)} \\ x_{2,1}^{(q)} & x_{2,2}^{(q)} & \cdots & x_{2,p}^{(q)} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n_q,1}^{(q)} & x_{n_q,2}^{(q)} & \cdots & x_{n_q,p}^{(q)} \end{pmatrix} \tag{1.19}$$

$$X^{(0)} = \begin{pmatrix} x_{1,1}^{(0)} & x_{1,2}^{(0)} & \dots & x_{1,p}^{(0)} \\ x_{2,1}^{(0)} & x_{2,2}^{(0)} & \dots & x_{2,p}^{(0)} \\ \dots & \dots & \dots & \dots \\ x_{m,1}^{(0)} & x_{m,2}^{(0)} & \dots & x_{m,p}^{(0)} \end{pmatrix} \quad (1.20)$$

де $X^{(k)}$ – матриці з навчальними ознаками (k=1,2,...,q); $X^{(0)}$ – матриця нових m-об'єктів, що підлягають дискримінації (розміром m×p); p – кількість властивостей, якими характеризується кожен *i*-й об'єкт.

Тут повинна виконуватися умова: загальна кількість об'єктів N множини M має дорівнювати сумі кількості об'єктів m (в підмножині M_0), що підлягають дискримінації, і загальної кількості об'єктів у навчальних підмножинах:

$$N = m + \sum_{k=1}^{q} n_k, \quad (1.21)$$

де q – кількість навчальних підмножин (q≥2). У реальній практиці найбільш часто реалізується випадок q=2, тому і алгоритм дискримінантного аналізу наведемо для даного варіанту:

1. Визначаються $\overline{X}_j^k$ елементи векторів $\overline{X}^k$ середніх значень за кожної j-ї ознаки для і об'єктів всередині k-ї підмножини (k=1, 2):

$$\bar{X}_j^{(k)} = \frac{\sum_{i=1}^{n} x_{ij}^{(k)}}{n_k}, \quad j = 1 \dots p \quad (1.22)$$

2. Результати розрахунку представляються у вигляді векторів стовпців $\overline{X}^k$.

3. Для кожної навчальної підмножини розраховуються коваріаційні матриці S(k) (розміром p×p):

$$S^{(k)} = \left| \frac{1}{n_k} \sum_{k=1}^{n} (X_{ik}^{(k)} - \bar{X}_i^{(k)} \right| (X_{jk}^{(k)} - \bar{X}_j^{(k)})_{p \times p} \quad (1.23)$$

4. Розраховується об'єднана коваріаційна матриця $\breve{S}$ за формулою:

$$\breve{S} = \frac{1}{n_1 + n_2 - 2} (n_1 \times S^{(1)} + n_2 \times S^{(2)}) \quad (1.24)$$

5. Розраховується матриця $\breve{S}^{-1}$ обернена до $\breve{S}$:

$$\breve{S}^{-1} = \frac{1}{|\breve{S}|} \times \bar{\breve{S}} \tag{1.25}$$

де $|\breve{S}|$ – визначник матриці $\breve{S}$, (причому $|\breve{S}| \neq 0$), $\hat{S}$ – приєднувальна матриця, елементи якої є алгебраїчними доповненнями елементів матриці.

6. Розраховується вектор-стовпець

$$A = \begin{vmatrix} A_1 \\ A_2 \\ \dots \\ A_p \end{vmatrix} \tag{1.26}$$

дискримінантних множників з урахуванням всіх елементів навчальних підмножин за формулою:

$$A = \hat{S}^{-1}(\bar{X}^{(1)} - \bar{X}^{(2)}). \tag{1.27}$$

Наведена розрахункова формула отримана за допомогою методу найменших квадратів за умови забезпечення найбільшої відмінності між дискримінантними функціями. Найкращий поділ двох навчальних підмножин забезпечується поєднанням мінімальної внутрішньогрупової варіації і максимальної груповий варіації.

7. По кожному і-му об'єкту (i=1,2,...,N) множини M визначається відповідне значення дискримінантної функції:

$$F^{(k)} = A_1 x_{i,1}^{(k)} + A_2 x_{i,2}^{(k)} + \dots + A_p x_{i,p}^{(k)} \tag{1.28}$$

8. За сукупністю знайдених значень $F^{(k)}$ розраховуються середні значення для кожної підмножини M_k:

$$\bar{F}^{(k)} = \frac{\sum_{i=1}^{n_i} F_i^{(k)}}{n_k}, \quad k = 1,2,\dots \tag{1.29}$$

9. Визначається загальна середня (константа дискримінації) для дискримінантних функцій.

10. Виконується розподіл

$$\bar{F} = \frac{\sum_{k=1}^{q} \bar{F}^{(k)}}{q} \tag{1.30}$$

(дискримінація) об'єктів підмножини M_0 підлягають дискримінації за навчальними вибірками M_1 і M_2. З цією метою розраховані за п. 7 по кожному і-му об'єкту значення дискримінантних функцій

$$F_i^{(0)} = A_1 X_{i,1}^{(0)} + A_2 X_{i,2}^{(0)} + \cdots + A_p X_{i,p}^{(0)}, \quad i = 1,2,\ldots,m \tag{1.31}$$

порівнюються з величиною $\overline{F}$ загальної середньої. На основі порівняння даний об'єкт відносять до однієї з навчальних підмножин.

11. Далі робиться оцінка якості розподілу нових об'єктів, для чого оцінюється вклад змінних в дискримінантному функцію.

Вплив ознак на значення дискримінантної функції і результати класифікації може оцінюватися за дискримінантними множниками (коефіцієнтам дискримінації), по дискримінантному навантаженню ознак або по дискримінантної матриці. Дискримінантні множники залежать від масштабів одиниць виміру ознак, тому вони не завжди зручні для оцінки.

Дискримінантні навантаження більш надійні в оцінці ознак, вони обчислюються як парні лінійні коефіцієнти кореляції між розрахованими рівнями дискримінантної функції F і ознаками, взятими для її побудови.

Дискримінантна матриця характеризує міру відповідності результатів класифікації фактичному розподілу об'єктів на підмножини і використовується для оцінки якості аналізу. В цьому випадку дискримінантна функція F формується за даними об'єктів (з вимірюваними ознаками) навчальних підмножин, а потім перевіряється якість цієї функції шляхом зіставлення фактичної приналежності об'єктів до класів з тією, що отримана в результаті формальної дискримінації.

1.3.3 Квадратичний дискримінантний аналіз

Квадратичний дискримінантний аналіз (QDA – Quadratic Discriminant Analysis) є природним узагальненням методу LDA. QDA – багатокласовий

метод і він може використовуватися для одночасної класифікації декількох класів k=1,…,K.

Нехай навчальний набір складається з K матриць $X_1,\ldots,X_k$, у яких є $I_1,\ldots,I_K$ рядків (зразків). Кількість змінних (стовпців) однакова. Зберігаючи перше припущення LDA, відмовимось від другого, тобто допустимо, що коваріаційні матриці в кожному класі різні. Тоді QDA-рахунки обчислюються за формулою

$$f_k = (x-\mu_k)\Sigma_k^{-1}(x-\mu_k)^t + \log(\det(\Sigma_k^{-1})),\ \ k = 1\ldots K \qquad (1.32)$$

Класифікаційне правило QDA таке – новий зразок x відноситься до того класу, для якого значення критерію QDA найменше. На практиці, так само, як і в LDA, невідомі математичні очікування і коваріаційні матриці замінюються їх оцінками:

$$m_k = \frac{1}{I_k}\sum_{i=1}^{I_k} x_i,\quad S_k = \frac{1}{I_k}\tilde{X}_k^t\tilde{X}_k, \qquad (1.33)$$

У цих формулах $\overline{X}^k$ позначає центровану матрицю X^k. Поверхня, що розділяє класи k і l визначається квадратним рівнянням $f_k=f_l$ тому метод і називається квадратичним.

1.4 Існуючі підходи до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака

Відомий підхід і система до декодування ЦВЗ, що міститься в зображенні формату JPEG [27], заснований на оцінці місцевих геометричних спотворень, що відбулися в зображенні через вбудовування еталонного повідомлення X. Цей підхід включає наступні кроки: моделювання локальних спотворень за допомогою індексної змінної J, що дозволяє визначити відмінності перекручених даних від початкових, оцінювання геометричних спотворень за допомогою еталонного повідомлення X, моделі локальних спотворень і моделі перекручених даних.

На рис. 1.9 представлена схема пристрою для зчитування водяних знаків згідно відомого підходу до декодування ЦВЗ, що міститься в зображенні формату JPEG [27].

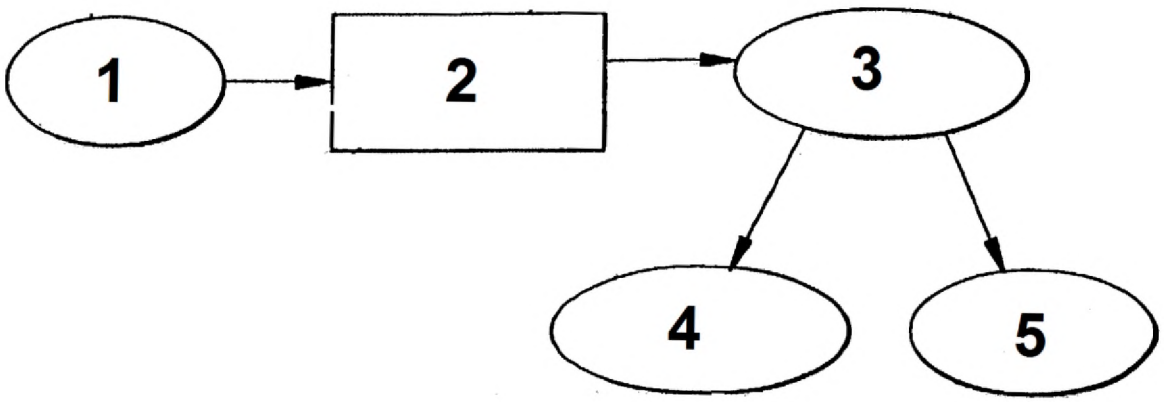


Рисунок 1.9 – Схема пристрою для зчитування водяних знаків згідно відомого підходу до декодування ЦВЗ, що міститься в зображенні формату JPEG [27]

На рис. 1.9 введено такі позначення:

1 – спотворені дані;

2 – процесор, пристосований для оцінки спотворень, що вводяться в дані;

3 – оцінені спотворення;

4 – блок виведення частини інформації на ЦВЗ, що несе повідомлення;

5 – блок виправлення спотворень.

Спотворені дані 1 надходять у зчитувач або приймач водяних знаків, відомий фахівцям в даній галузі. Цей приймач має процесор 2, пристосований для оцінки спотворень, що вводяться в дані. Наприклад, він запрограмований на реалізацію кроків різних варіантів відомого підходу [27]. Потім оцінені спотворення 3 використовуються, наприклад, або для виведення частини інформації 4 на сам водяний знак, що несе повідомлення, або для виправлення 5 спотворень.

Також відомий підхід і система для ідентифікації даних зображення JPEG [28], що дозволяє встановити, чи дійсно отримане зображення відправлено відомим джерелом і чи не був вміст файлу незначно модифікований під час передачі. Для кодування перевірочної інформації унікальна хеш-функція

отримається з першої частини даних зображення, що містяться в стислому зображенні JPEG таким чином, що будь-які спотворення зазначеної частини даних зображення в подальшому були б відображені в інший хеш-функції, отриманій на основі прийнятого файлу. Хеш-функція дає значення перевірки цілісності, що записується в першу частину даних зображення. Далі це значення шифрується в рядок підпису. Рядок підпису вбудовується в наступну частину даних зображення. Процес повторюється до тих пір, поки всі частини даних зображення не будуть оброблені. Рядок підпису, відповідний останній частини даних, вбудовується в цю частину. Оскільки впровадження значення перевірки цілісності не змінює послідовності даних файлу JPEG, будь-який декодер після цього може декодувати зображення. Далі файл зображення передається призначеному одержувачу. Для декодування одержувачем впровадженої перевірочної інформації щодо справжності відправника файлу JPEG хеш-функція обчислюється на основі першої частини даних отриманого зображення. Друга частина даних характеризує місце розташування, де було запроваджено рядок підпису для першої частини даних. У цьому випадку підпис витягується з даних. Після чого рядок підпису дешифрується в вигляді результату хеш-функції (перевірки цілісності), що міститься в самих даних. Ці два числа порівнюються один з одним. Якщо перше перевірочне число відповідає числу, що міститься в знайденому рядку підпису, яка була раніше впроваджена автором, то приймається рішення, що дані першої частини зображення справжні. Процес повторюється для кожної наступної частини даних, поки не будуть оброблені всі частини даних зображення.

Рис. 1.10 ілюструє етапи хешування, шифрування та вбудовування системи і способу автентифікації згідно з відомим підходом для ідентифікації даних зображення JPEG [28].

Рис. 1.11 ілюструє етапи автентифікації автора згідно з відомим підходом для ідентифікації даних зображення JPEG [28].

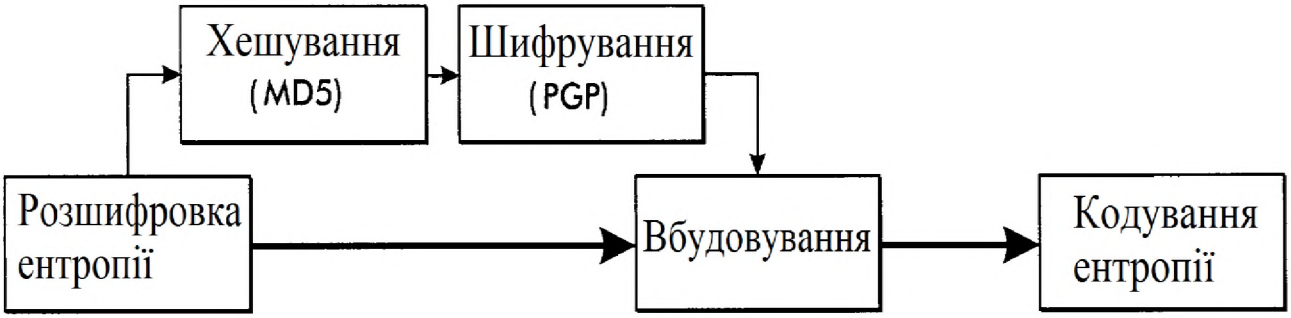


Рисунок 1.10 – Етапи хешування, шифрування та вбудовування системи і способу автентифікації згідно з відомим підходом для ідентифікації даних зображення JPEG [28]

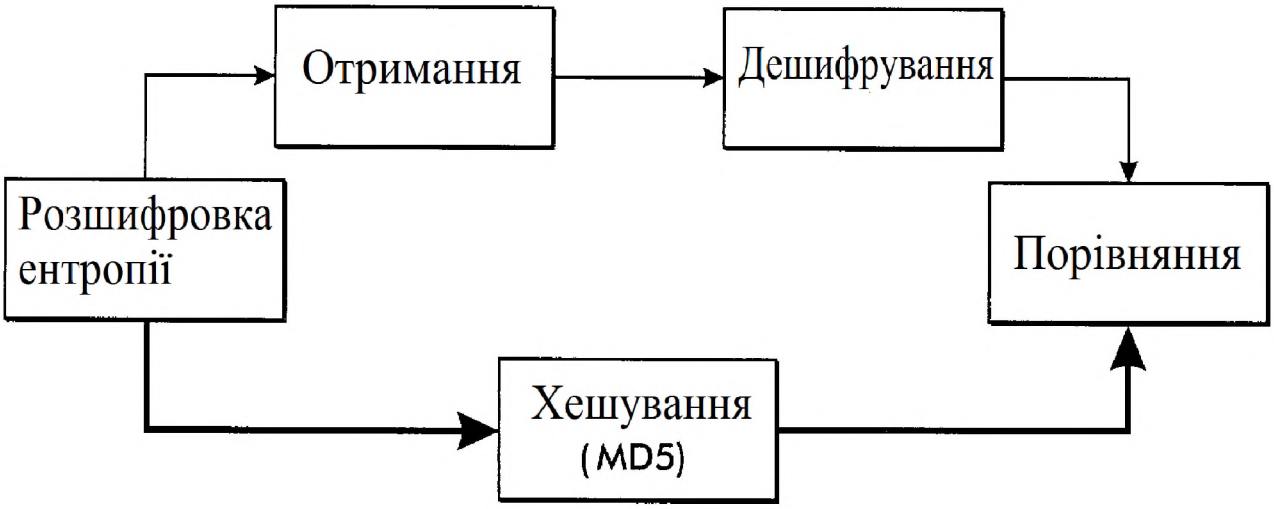
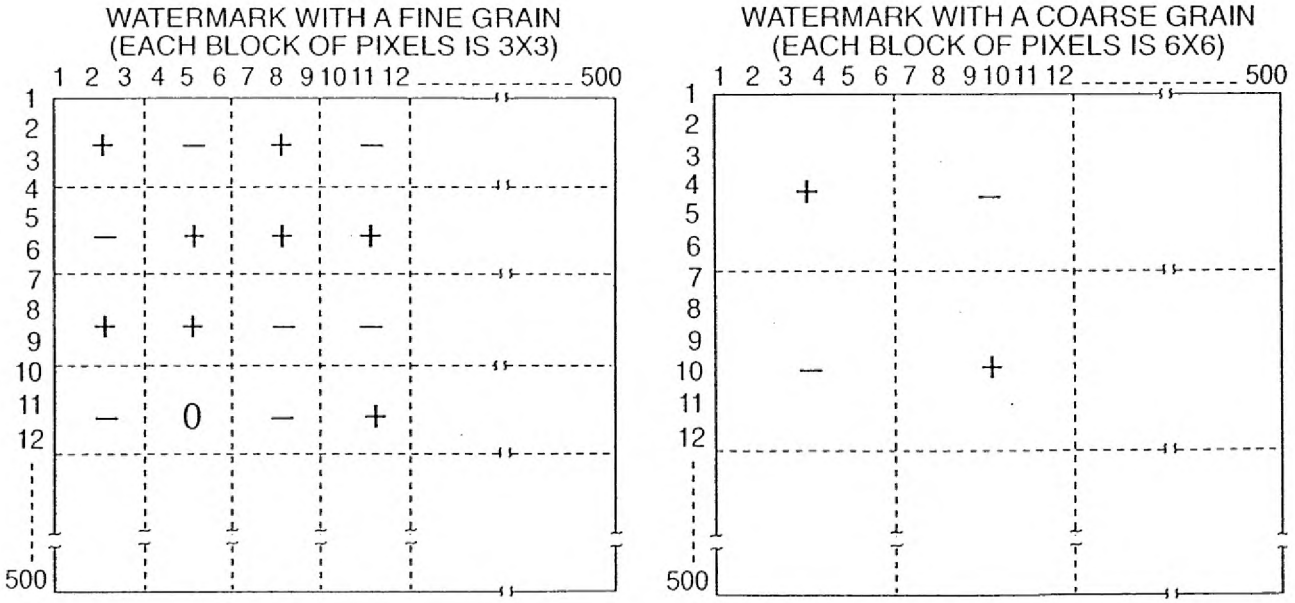


Рисунок 1.11 – Етапи автентифікації автора згідно з відомим підходом для ідентифікації даних зображення JPEG [28]

Відомий підхід і система до декодування ЦВЗ, що міститься в зображенні формату JPEG [27] та відомий підхід і система для ідентифікації даних зображення JPEG [28] (аналоги) застосовуються в області захисту авторських прав для пошуку зображень формату JPEG, що містять ЦВЗ, які можуть бути спотворені в результаті спроб їх видалення з зображення. Недоліками відомого підходу до декодування ЦВЗ, що міститься в зображенні формату JPEG [27] та підходу для ідентифікації даних зображення JPEG [28] є те, що вони можуть бути застосовані тільки в разі апріорного знання про присутність ЦВЗ в уже згадуваному зображенні формату JPEG і про закон його вбудовування, при цьому підходи застосовні тільки для ЦЗ формату JPEG.

Найбільш близьким за своєю сутністю до запропонованого підходу (прототипом) є відомий підхід до ідентифікації зображення, що містить багаторазовий ЦВЗ [29], що включає етап вбудовування в документ (оригінал) додаткової інформації, яка складається з двох типів ЦВЗ, з'єднаний з етапом зчитування вбудованих ЦВЗ з ідентифікованого документа (зображення), який в свою чергу з'єднаний з етапом порівняння отриманих енергетичних характеристик зчитаних ЦВЗ двох типів зі зразком, з'єднаним з етапом прийняття рішення про несанкціоноване копіювання ідентифікованого документа (зображення).

Як вже було сказано, документ (оригінал) включає зображення, яке має два цифрові водяні знаки, вставлені в нього. Зерно двох водяних знаків показано на рис. 1.12.



а б

Рисунок 1.12 – Зерно першого (а) та другого (б) водяного знака, які вбудовуються в документ згідно відомого підходу-прототипу до ідентифікації зображення, що містить багаторазовий ЦВЗ [29]

Перший водяний знак використовує блоки по 9 пікселів (блок 3×3). Кожен з пікселів у кожному блоці з 9 пікселів має значення сірого, змінене на

однакову величину. Наприклад, рис. 1.12,а показує, що для першого 9-піксельного блоку значення сірого збільшується, а для другого 9-піксельного блоку зменшується значення сірого. Величина збільшення та відбору блоків, яка збільшується та зменшується, є загальноприйнятою. Як показано на рис. 1.12,б, зернистість другого водяного знака знаходиться в блоках, які мають розмір 6×6 пікселів або 36 пікселів. Усі пікселі в кожному блоці з 36 пікселів змінюються на однакову величину.

Відомий підхід-прототип до ідентифікації зображення, що містить багаторазовий ЦВЗ [29] використовується в області захисту авторських прав і забезпечує розрізнення документів-оригіналів (зображень-оригіналів) від їх копій, отриманих шляхом роздруківки і сканування. Проте недоліком відомого підходу-прототипу до ідентифікації зображення, що містить багаторазовий ЦВЗ [29] є те, що він застосовується тільки в умовах присутності апріорних відомостей про закон вбудовування ЦВЗ, в іншому випадку підхід стає неефективним і розрізнити, чи є ідентифікований документ (оригінал) копією або оригіналом, не представляється можливим.

1.5 Висновок. Постановка задачі

В розділі проаналізовано технології цифрового маркування графічних зображень, а також дискримінантного аналізу. Встановлено, що стеганографія має багато областей застосування, одним з яких є вбудовування цифрових водяних знаків. Даний напрямок прекрасно підходить для вирішення завдань запобігання незаконному копіюванню і модифікації мультимедійної інформації, захисту авторських прав. Дискримінантний аналіз – набір методів статистичного аналізу для вирішення задач розпізнавання образів, класифікації багатовимірних спостережень за принципом максимальної схожості при наявності навчальних ознак.

В розділі проаналізовано існуючі підходи до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака.

Встановлено, що недоліками відомого підходу до декодування ЦВЗ, що міститься в зображенні формату JPEG [27] та підходу для ідентифікації даних зображення JPEG [28] є те, що вони можуть бути застосовані тільки в разі апріорного знання про присутність ЦВЗ в уже згадуваному зображенні формату JPEG і про закон його вбудовування, при цьому підходи застосовні тільки для ЦЗ формату JPEG.

Встановлено, що недоліком відомого підходу-прототипу до ідентифікації зображення, що містить багаторазовий ЦВЗ [29] є те, що він застосовується тільки в умовах присутності апріорних відомостей про закон вбудовування ЦВЗ, в іншому випадку підхід стає неефективним і розрізнити, чи є ідентифікований документ (оригінал) копією або оригіналом, не представляється можливим.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу

Запропонований підхід відноситься до області стеганографії, а саме до способів ідентифікації цифрових зображень (ЦЗ), що містять цифровий водяний знак (ЦВЗ), і може бути використаний для розрізнення оригінального ЦЗ, захищеного авторськими правами за допомогою впровадженого в нього ЦВЗ, від його копій, а також для пошуку ЦЗ різних форматів, що містять додаткову цифрову інформацію в умовах відсутності апріорних відомостей про закон її вбудовування та присутності в зображенні.

Технічний результат запропонованого підходу полягає в можливості ідентифікації ЦЗ, що містять ЦВЗ в умовах відсутності апріорних відомостей про наявність ЦВЗ в даному зображенні і про закон вбудовування ЦВЗ. Технічний результат досягається за рахунок побудови власних характеристичних векторів зображень з навчальної вибірки, що включають в себе статистичні характеристики, обчислені з розподілів вейвлет-коефіцієнтів і з розподілів похибки передбачення величин вейвлет-коефіцієнтів на різних піддіапазонах. У навчальну вибірку включаються два класи зображень: ЦЗ, що містять ЦВЗ і ЦЗ, що не містять ЦВЗ. Після навчання класифікатора, заснованого на дискримінантному аналізі, проводиться класифікація аналізованого зображення, тобто віднесення його до одного з класів. Завдяки цьому існує можливість ідентифікації ЦЗ, що містить ЦВЗ, тобто розрізнення зображення-оригіналу, захищеного авторськими правами від його копій, отриманих шляхом роздруківки і сканування.

Метою роботи є розробка підходу до ідентифікації цифрових зображень, які містять цифровий водяний знак, що забезпечує роботу в умовах відсутності апріорних відомостей про закон вбудовування ЦВЗ, при цьому підхід повинен

бути застосовний для аналізу зображень різних форматів (BMP, JPEG, GIF, PNG).

Поставлена мета досягається за рахунок того, що в відомий підхід до ідентифікації документа (зображення), який містить багаторазовий ЦВЗ, що включає етап вбудовування в документ (оригінал) додаткової інформації, яка складається з двох типів ЦВЗ, з'єднаний з етапом зчитування вбудованих ЦВЗ з ідентифікованого документа (зображення). Останній, в свою чергу, з'єднаний з етапом порівняння отриманих енергетичних характеристик зчитаних ЦВЗ двох типів зі зразком, сполученим з етапом прийняття рішення про несанкціоноване копіюванні ідентифікованого документа (зображення). Після етапу вбудовування замість етапу зчитування вбудованих ЦВЗ з ідентифікованого документа (зображення) і наступних за ним етапів порівняння і прийняття рішення введені етап формування тривимірного масиву значень інтенсивності точок зображення, етап формування масиву значень інтенсивності точок червоної кольорової складової зображення, етап формування масиву значень інтенсивності точок зеленої кольорової складової зображення, етап формування масиву значень інтенсивності точок синьої кольорової складової зображення, етап багаторівневого дискретного двовимірного вейвлет-перетворення, етап обчислення статистичних характеристик високих порядків з розподілу вейвлет-коефіцієнтів на окремих піддіапазонах вейвлет-перетворення, етап обчислення похибки передбачення значень коефіцієнтів на різних піддіапазонах вейвлет-перетворення, етап обчислення статистичних характеристик високих порядків з розподілу похибки передбачення значень вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення, етап формування власного характеристичного вектора зображення, етап формування масиву власних характеристичних векторів цифрових зображень з навчальної вибірки, етап навчання класифікатора і етап класифікування цифрового зображення.

Введення нових етапів дозволяє ідентифікувати цифрове зображення, що містить ЦВЗ в умовах відсутності апріорних відомостей про закон і місце вбудовування ЦВЗ, при цьому за рахунок введення етапів формування трьох

масивів значень інтенсивності точок трьох колірних складових зображення виникає можливість аналізувати ЦЗ різних форматів (BMP, JPEG, GIF, PNG).

На рис. 2.1 представлена загальна схема реалізації підходу до ідентифікації цифрового зображення, що містить цифровий водяний знак.

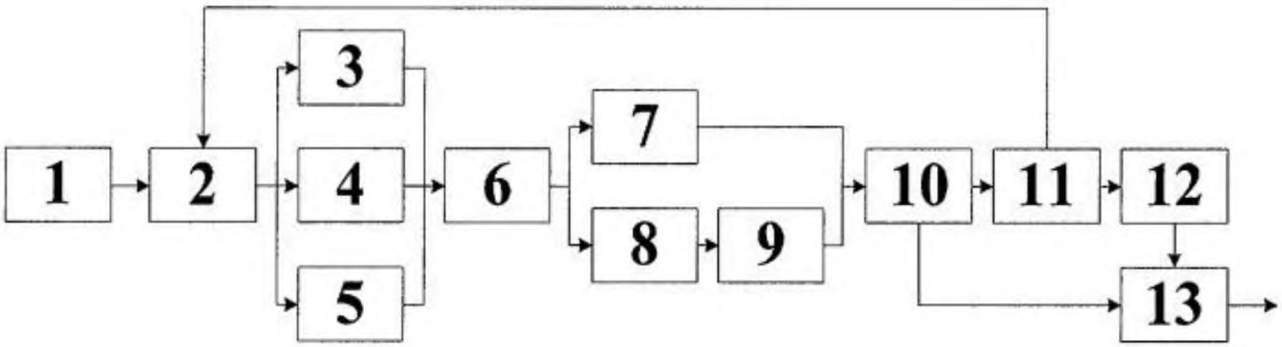


Рисунок 2.1 – Загальна схема реалізації підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу

На рис. 2.1 введено такі позначення:

1 – блок вбудовування в зображення додаткової інформації;

2 – блок формування тривимірного масиву значень інтенсивності точок зображення;

3 – блок формування масиву значень інтенсивності точок червоної кольорової складової зображення;

4 – блок формування масиву значень інтенсивності точок зеленої кольорової складової зображення;

5 – блок формування масиву значень інтенсивності точок синьої кольорової складової зображення;

6 – блок багаторівневого дискретного двовимірного вейвлет-перетворення;

7 – блок обчислення статистичних характеристик високих порядків з розподілу вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення;

8 – блок обчислення похибки передбачення значень коефіцієнтів на різних піддіапазонах вейвлет-перетворення;

9 – блок обчислення статистичних характеристик високих порядків з розподілу похибки передбачення значень вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення;

10 – блок формування власного характеристичного вектора зображення;

11 – блок формування масиву власних характеристичних векторів зображень з навчальної вибірки;

12 – блок навчання класифікатора;

13 – блок класифікування зображення.

Запропонований підхід, схема якого представлена на рис. 2.1, складається з блоку вбудовування в зображення додаткової інформації 1, блоку формування тривимірного масиву значень інтенсивності точок зображення 2, який з'єднаний з блоком формування масиву значень інтенсивності точок червоної кольорової складової зображення 3, з блоком формування масиву значень інтенсивності точок зеленої кольорової складової зображення 4 і з блоком формування масиву значень інтенсивності точок синьої кольорової складової зображення 5, які в свою чергу з'єднані з блоком багаторівневого дискретного двовимірного вейвлет-перетворення 6, вихід якого з'єднаний з входом блоку обчислення статистичних характеристик високих порядків з розподілу вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення 7 і входом блоку обчислення похибки передбачення значень коефіцієнтів на різних піддіапазонах вейвлет-перетворення 8, з'єднаного у свою чергу з блоком обчислення статистичних характеристик високих порядків з розподілу похибки передбачення значень вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення 9, виходи блоків 7 і 9 з'єднуються з входом блоку формування власного характеристичного вектора зображення 10, з'єднаного у свою чергу з блоком класифікування зображення 13 і з блоком формування масиву власних характеристичних векторів зображень з навчальної вибірки 11, який зворотним зв'язком з'єднаний з блоком формування тривимірного масиву значень

інтенсивності точок зображення 2 і прямим зв'язком з блоком навчання класифікатора 12, вихід якого з'єднаний з входом блоку класифікування зображення 13.

Запропонований підхід здійснюють в два етапи, які називаються «навчання» і «аналіз». Етап «навчання» реалізується за рахунок того, що спочатку за допомогою блоку 1 формують навчальну вибірку, яка включає зображення, що містять вбудовані випадковим чином ЦВЗ, потім за допомогою блоків 2, 3, 4, 5 формують три двовимірних масиву значень інтенсивності точок цифрового зображення для кожної з трьох кольорових складових у вигляді карти пікселів кольорової схеми RGB (червоного, зеленого, синього) [30].

Далі в блоці багаторівневого дискретного двовимірного вейвлет-перетворення 6 кожен масив інтенсивностей точок трьох кольорових складових окремо піддається багаторівневому двовимірному дискретному вейвлет-перетворенню (необхідно не менше трьох рівнів вейвлет-перетворення) з використанням біортогональних низькочастотного (НЧ) і високочастотного (ВЧ) фільтрів [31]. Рекомендується використовувати фільтри з коефіцієнтами згідно з таблицею 2.1.

Таблиця 2.1 – Значення коефіцієнтів блоку біортогональних вейвлет-фільтрів 7/9

№ п/п	Значення коефіцієнтів НЧ фільтру	№ п/п	Значення коефіцієнтів ВЧ фільтру
0	0.852699	0	0.788485
1	0.377403	1	-0.418092
2	-0.110624	2	- 0.040690
3	- 0.023849	3	0.064539
4	0.037829		

Далі в блоці обчислення статистичних характеристик високих порядків з розподілу вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення 7

здійснюється обчислення статистичних характеристик високих порядків з розподілів вейвлет-коефіцієнтів кожного піддіапазону всіх рівнів вейвлет-перетворення, виключаючи три піддіапазони останнього рівня, для кожної колірної складової зображення. Даними статистичними характеристиками є вибіркове середнє, вибіркова дисперсія, асиметрія і ексцес [32] відповідно до формул (2.1-2.4) відповідно:

$$\bar{x}_B = \frac{\sum x_i}{n}, \tag{2.1}$$

де $\bar{x}_B$ – вибіркове середнє; n – кількість коефіцієнтів даного піддіапазону вейвлет-перетворення;

$$D_B = \frac{\sum_{i=1}^{N} \left(x_i - \bar{x}_\Gamma\right)^2}{n - 1}, \tag{2.2}$$

де D_B – вибіркова дисперсія; n – кількість коефіцієнтів даного піддіапазону вейвлет-перетворення;

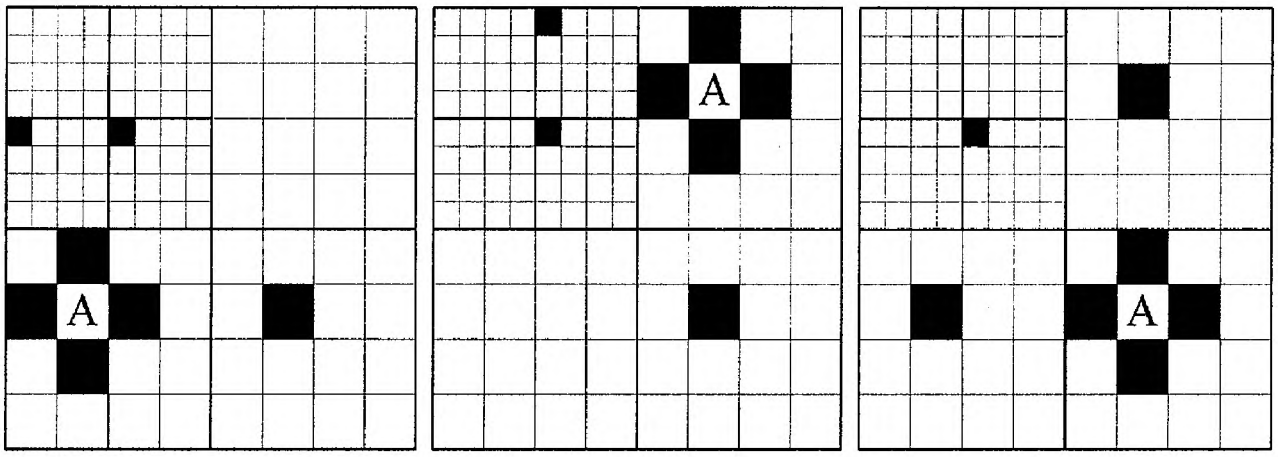
$$A_S = \frac{\mu_3}{\sigma^3}, \tag{2.3}$$

де A_S – асиметрія теоретичного розподілу; μ_3 – центральний момент третього порядку; σ^3 – куб вибіркового середнього квадратичного відхилення;

$$E_k = \frac{\mu_4}{\sigma^4} - 3, \tag{2.4}$$

де E_k – ексцес теоретичного розподілу; μ_4 – центральний момент четвертого порядку; σ^4 – вибіркове середнє квадратичне відхилення в четвертому ступені.

На рис. 2.2 представлено вибір положення коефіцієнтів «сусідів» щодо аналізованого коефіцієнта «А» (закреслені квадрати) вейвлет-перетворення для формули лінійного передбачувача значень вейвлет-коефіцієнтів для: *а* – вертикальних піддіапазонів, *б* – горизонтальних піддіапазонів, *в* – діагональних під діапазонів.



а *б* *в*

Рисунок 2.2 – Вибір положення коефіцієнтів «сусідів» щодо аналізованого коефіцієнта «А» вейвлет-перетворення для формули лінійного передбачувача значень вейвлет-коефіцієнтів для: *а* – вертикальних піддіапазонів, *б* – горизонтальних піддіапазонів, *в* – діагональних під діапазонів

Одночасно з процедурою обчислення статистичних характеристик високих порядків з розподілу вейвлет-коефіцієнтів на різних піддіапазонах вейвлет-перетворення в блоці обчислення похибки передбачення значень коефіцієнтів на різних піддіапазонах вейвлет-перетворення 8 обчислюється похибка передбачення значень вейвлет-коефіцієнтів на різних піддіапазонах n-го рівня вейвлет-перетворення, а також на піддіапазонах подальшого (n+1)-го рівня вейвлет-перетворення згідно з рис. 2.2 і формулами лінійного передбачувача значень вейвлет-коефіцієнтів (2.5-2.7) для вертикального, горизонтального і діагонального піддіапазонів відповідно [33]:

$$|V_i(x, y)| = \omega_1|V_i(x-1, y)| + \omega_2|V_i(x+1, y)| + \omega_3|V_i(x, y-1)| + \omega_4|V_i(x, y+1)| + \omega_5|V_{i+1}(x/2, y/2)| + \omega_6|D_i(x, y)| + \omega_7|D_{i+1}(x/2, y/2)|, \quad (2.5)$$

$$|H_i(x, y)| = \omega_1|H_i(x-1, y)| + \omega_2|H_i(x+1, y)| + \omega_3|H_i(x, y-1)| + \omega_4|H_i(x, y+1)| + \omega_5|H_{i+1}(x/2, y/2)| + \omega_6|D_i(x, y)| + \omega_7|D_{i+1}(x/2, y/2)|, \quad (2.6)$$

$$|D_i(x, y)| = \omega_1|D_i(x-1, y)| + \omega_2|D_i(x+1, y)| + \omega_3|D_i(x, y-1)| + \omega_4|D_i(x, y+1)| + \omega_5|D_{i+1}(x/2, y/2)| + \omega_6|H_i(x, y)| + \omega_7|V_i(x, y)| \quad (2.7)$$

де $|\cdot|$ – означає, що значення коефіцієнтів взяті за модулем; V_i, H_i, D_i – вказують, на якому піддіапазоні і якому рівні вейвлет-перетворення обчислюється

формула лінійного передбачувача (відповідно вертикальний, горизонтальний, діагональний піддіапазон); і – рівень вейвлет-перетворення; х – координата вейвлет-коефіцієнта по горизонталі; у – координата вейвлет-коефіцієнта по вертикалі; ω_k – скалярні вагові коефіцієнти лінійного передбачувача.

Формули (2.5-2.7) можуть бути представлені у векторному вигляді:

$$\vec{V} = \vec{\omega}Q \tag{2.8}$$

де $\vec{\omega} = (\omega_1 \cdots \omega_7)$ – вектор-рядок, що містить вагові коефіцієнти; $\vec{V}$ – вектор-рядок, що включає значення аналізованих коефіцієнтів A_i; Q – матриця, стовпці якої містять значення так званих коефіцієнтів «сусідів» для аналізованих коефіцієнтів A_i (закреслені квадрати на рис. 2.2).

Коефіцієнти лінійного передбачувача ω_i визначаються шляхом мінімізації функції квадрата похибки

$$E(\vec{\omega}) = \left\|\vec{V} - Q\vec{\omega}\right\|^2. \tag{2.9}$$

Потім проводиться диференціювання по $\vec{\omega}$:

$$\frac{dE(\vec{\omega})}{d\vec{\omega}} = 2Q^T\left(\vec{V} - Q\vec{\omega}\right), \tag{2.10}$$

одержуваний результат прирівнюється до нуля, а знаходження $\vec{\omega}$ проводиться за наступною формулою:

$$\vec{\omega} = \left(QQ^T\right)^{-1}\vec{V}Q^T. \tag{2.11}$$

Після визначення значень коефіцієнтів лінійного передбачувача логарифмічна похибка між фактичними коефіцієнтами і передбаченими обчислюється за формулою:

$$\vec{E} = \log_2\left(\vec{V}\right) - \log_2\left(\left|Q\vec{\omega}\right|\right). \tag{2.12}$$

З отриманих на кожному піддіапазоні розподілів векторів похибки $\vec{E}$ в блоці обчислення статистичних характеристик високих порядків з розподілу похибки передбачення значень вейвлет-коефіцієнтів на різних піддіапазонах

вейвлет-перетворення 9 обчислюються вибіркове середнє, вибіркова дисперсія, асиметрія і ексцес відповідно до формул (2.1-2.4).

У блоці формування власного характеристичного вектора (ВХВ) зображення 10 все обчислені значення статистичних характеристик включаються в вектор, званий власним характеристичним вектором зображення, який обчислюється за формулою:

$$\vec{S} = \left(\bar{x}_{B1}, \bar{x}_{B2}, .., \bar{x}_{BN}; D_{B1}, D_{B2}, ..., D_{BN}; A_{S1}, A_{S2}, ..., A_{SN}; E_{k1}, E_{k2}, ..., E_{kN}\right), \quad (2.13)$$

де N=24(n-1), n – число рівнів вейвлет-перетворення.

Таким чином, розмірність такого вектора залежить від кількості рівнів вейвлет-перетворення n і дорівнює 72(n-1).

Далі в блоці формування масиву власних характеристичних векторів зображень з навчальної вибірки 11 здійснюється формування масиву ВХВ всіх зображень з навчальної вибірки, для цього блок 11 з'єднаний з блоком 2 зворотним зв'язком, що вказує на те, що всі наведені вище дії виконуються з кожним зображенням з навчальної вибірки окремо (навчальна вибірка повинна містити не менше 200 ЦЗ, що не містять ЦВЗ, і не менше 200 ЦЗ, що містять ЦВЗ, причому всі ЦЗ даної навчальної вибірки повинні бути одного формату і ЦВЗ повинні вбудовуватися за різними законами).

Після формування масиву ВХВ всіх зображень з навчальної вибірки в блоці 11 отриманий масив подається на вхід блоку навчання класифікатора 12, побудованого на основі дискримінантного аналізу для лінійної дискримінації зображень з навчальної вибірки на два класи: ЦЗ, що містять ЦВЗ, і ЦЗ, що не містять ЦВЗ. Після цього етап «навчання» закінчується і починається другий етап – «аналіз».

На етапі «аналіз» з обраним для аналізу ЦЗ (воно повинно бути одного формату з цифровими зображеннями з навчальної вибірки) здійснюються всі процедури, що проводяться в блоках 2-10 і описані вище, тільки тепер після блоку формування власного характеристичного вектора аналізованого зображення 10 сформований ВХВ подається на вхід блоку класифікування зображення 13, на який одночасно з цим з блоку навчання класифікатора 12

подаються результати дискримінації всіх ВХВ, отриманих від ЦЗ з навчальної вибірки на етапі «навчання».

У блоці класифікування зображення 13 на підставі обчисленої відстані Махаланобіса (згідно з формулою 2.14) приймається рішення про належність аналізованого зображення до одного з класів, або до класу ЦЗ, що містять ЦВЗ, або до класу ЦЗ, що не містять ЦВЗ:

$$d_M(x_i, x_j) = (x_i - x_j)K^{-1}(x_i - x_j) = \sum_{p,q=1}^{m} c_{pq}(x_i^p - x_j^p)(x_i^q - x_j^q), \quad (2.14)$$

де $d_M(x_i, x_j)$ – відстань Махаланобіса; $K^{-1}=C$ – матриця, зворотна коваріаційній матриці К, обчисленій за вибіркою х; c_{pq} – елементи матриці С [34].

2.2 Оцінка ефективності запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу

Оцінка ефективності запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу була проведена шляхом моделювання в середовищі Matlab / Simulink.

Обґрунтування позитивного ефекту запропонованого підходу здійснено наступним чином.

Показником ефективності способів ідентифікації ЦЗ, що містять ЦВЗ, є ймовірність правильної ідентифікації $P_{ідент}$.

Завдання полягає в тому, щоб досягти максимальної ймовірності правильної ідентифікації за умови, що закон вбудовування ЦВЗ і його присутність в аналізованому зображенні апріорно невідомі. Це дозволить відрізнити зображення-оригінал від його копій, отриманих за допомогою роздруківки і сканування.

Для перевірки запропонованого підходу класифікатор, заснований на дискримінантному аналізі, був навчений на вибірці з 1000 зображень різних

форматів, 500 з яких містили ЦВЗ. За допомогою набору з 1650 зображень, які не належать навчальній вибірці, 150 з яких містили вбудований по невідомому закону ЦВЗ (по 50 зображень форматів JPEG, BMP, GIF), були протестовані відомий підхід-прототип і запропонований підхід.

На рис. 2.3 представлений графік ймовірності правильної ідентифікації зображень різних форматів, що містять ЦВЗ, в результаті роботи підходу-прототипу та запропонованого підходу. В табл. 2.1 представлені додаткові результати – значення ймовірностей правильної ідентифікації $P_{ідент}$ зображень різних форматів, що містять ЦВЗ, в результаті роботи підходу-прототипу і запропонованого підходу.

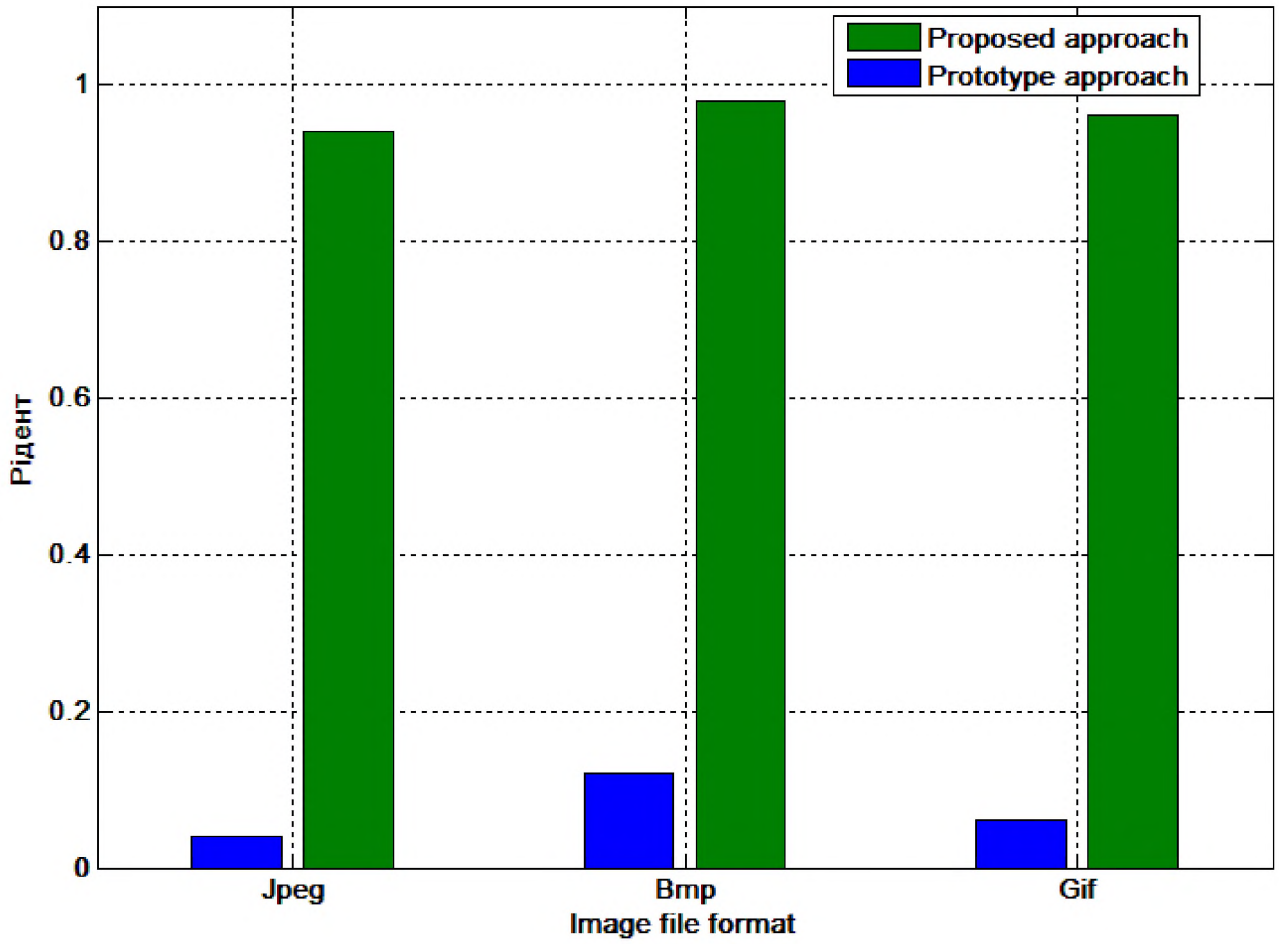


Рисунок 2.3 – Графік ймовірності правильної ідентифікації зображень різних форматів, що містять ЦВЗ, в результаті роботи підходу-прототипу і запропонованого підходу

Таблиця 2.1 – Значення ймовірностей правильної ідентифікації $P_{ідент}$ зображень різних форматів, що містять ЦВЗ, в результаті роботи підходу-прототипу і запропонованого підходу

Формат зображень, що містять ЦВЗ	Значення ймовірностей правильної ідентифікації $P_{ідент}$	
	в результаті роботи підходу-прототипу	в результаті роботи запропонованого підходу
Jpeg	0,04	0,94
Bmp	0,12	0,98
Gif	0,06	0,96

Результати, представлені на рис. 2.3 та в табл. 2.1, показали, що в умовах відсутності апріорних відомостей про закон вбудовування ЦВЗ відомий підхід-прототип правильно ідентифікував 11 зображень-оригіналів з 150, а за допомогою запропонованого підходу вдалося правильно відрізнити 144 зображення-оригінали з 150 від їх високоякісних копій. Це підтверджує істотний позитивний ефект від впровадження запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу.

Отже, запропонований підхід з використанням дискримінантного аналізу може забезпечити ідентифікацію ЦЗ, що містять ЦВЗ в умовах відсутності апріорних відомостей про закон його вбудовування в аналізоване зображення, при цьому підхід може бути застосований для ідентифікації зображень різного формату.

2.3 Висновки

Запропонований підхід відноситься до області стеганографії, а саме до способів ідентифікації ЦЗ, що містять ЦВЗ, і може бути використаний для розрізнення оригінального ЦЗ, захищеного авторськими правами за допомогою

впровадженого в нього ЦВЗ, від його копій, а також для пошуку ЦЗ різних форматів, що містять додаткову цифрову інформацію в умовах відсутності апріорних відомостей про закон її вбудовування та присутності в зображенні.

Технічний результат запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу полягає в можливості ідентифікації ЦЗ, що містять ЦВЗ в умовах відсутності апріорних відомостей про наявність ЦВЗ в даному зображенні і про закон вбудовування ЦВЗ. Технічний результат досягається за рахунок побудови власних характеристичних векторів зображень з навчальної вибірки, що включають в себе статистичні характеристики, обчислені з розподілів вейвлет-коефіцієнтів і з розподілів похибки передбачення величин вейвлет-коефіцієнтів на різних піддіапазонах. У навчальну вибірку включаються два класи зображень: ЦЗ, що містять ЦВЗ і ЦЗ, що не містять ЦВЗ. Після навчання класифікатора, заснованого на дискримінантному аналізі, проводиться класифікація аналізованого зображення, тобто віднесення його до одного з класів. Завдяки цьому існує можливість ідентифікації ЦЗ, що містить ЦВЗ, тобто розрізнення зображення-оригіналу, захищеного авторськими правами від його копій, отриманих шляхом роздруківки і сканування.

Оцінка ефективності запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу була проведена шляхом моделювання в середовищі Matlab / Simulink.

Встановлено, що в умовах відсутності апріорних відомостей про закон вбудовування ЦВЗ відомий підхід-прототип правильно ідентифікував 11 зображень-оригіналів з 150, а за допомогою запропонованого підходу вдалося правильно відрізнити 144 зображення-оригінали з 150 від їх високоякісних копій. Це підтверджує істотний позитивний ефект від впровадження запропонованого підходу.

Отже, запропонований підхід з використанням дискримінантного аналізу може забезпечити ідентифікацію ЦЗ, що містять ЦВЗ в умовах відсутності

апріорних відомостей про закон його вбудовування в аналізоване зображення, при цьому підхід може бути застосований для ідентифікації зображень різного формату.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є обґрунтування економічної доцільності перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака. Для досягнення цієї мети необхідно здійснити наступні розрахунки: капітальні витрат на придбання і налагодження складових системи інформаційної безпеки або витрати, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення; річні експлуатаційні витрат 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 (фіксованих) капітальних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

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

Визначення трудомісткості розробки підходу щодо перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака, $t_{тз}$=19;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=*38*;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=*42*;

$t_р$ – тривалість розробки підходу щодо перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака, $t_м=80$;

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

Отже,

$$t = t_{тз}+ t_в+ t_а+ t_р+ t_д = 19+38+42+80+16 = 195 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака

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 $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 28080 +1433,25= 29513,25 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 195*144 = 28080 \text{ грн.}$$

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:

$$З_{мч}= t*С_{мч}=195*7,35=1433,25 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 1,1 \cdot 3 \cdot 1,55 + \frac{6900 \cdot 0,4}{1920} + \frac{5124 \cdot 0,3}{1920} = 7,35 \text{ грн.}$$

Оцінка ефективності запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак, з використанням дискримінантного аналізу була проведена шляхом моделювання в середовищі

Matlab / Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 2000 грн.

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

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

$$=29513,25+2000= 31513,25 \text{ грн.}$$

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 (ПЗ), 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.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.}$$

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 ($С_{ак} = 0$ грн.).

Оскільки середовище Matlab/Simulink, яке використовується для оцінки ефективності запропонованого підходу до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака, вже є наявним, 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 6000 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 14620 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,3 ставки. Отже,

$$С_з = (14620*12 + 14620*12*0,08)*0,3= 56842,56 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 56842,56*0,22 = 12505,36 \text{ грн.}$$

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=1,1 кВт);

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

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

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

$$С_{ел} = 1,1*3*1920*1,55 = 9820,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 31513,25*0,01=315,13 грн).

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

$$С_к = 6000+56842,56+12505,36+9820,8 +315,13 = 85483,85 \text{ грн.}$$

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

$$С = 85483,85 \text{ грн.}$$

3.2 Оцінка можливого збитку

Запропонований підхід щодо перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака відноситься до області стеганографії, а саме до способів ідентифікації ЦЗ, що містять ЦВЗ, і може бути використаний для розрізнення оригінального ЦЗ, захищеного авторськими правами за допомогою впровадженого в нього ЦВЗ, від його копій, а також для пошуку ЦЗ різних форматів, що містять додаткову цифрову інформацію в умовах відсутності апріорних відомостей про закон її вбудовування та присутності в зображенні.

При порушенні прав інтелектуальної власності на цифрові зображення величина можливого збитку може бути визначена відповідно до розміру відшкодування завданих збитків, що визначається правом інтелектуальної власності, зокрема Цивільним кодексом України, Кримінальним кодексом України, ВСУ від 31.03.95 р. №4 «Про судову практику у справах про відшкодування морального (немайнового) збитку» тощо. У разі встановлення величини компенсації за завдану шкоду підприємству, яка виникла внаслідок

недостатнього рівня захищеності його об'єктів інтелектуальної власності, а саме, зображень за допомогою ЦВЗ, величину можливого збитку можна встановити наступним чином:

$$B = n * R * F$$

де n – кількість зображень, що потребує захисту;

R – середнє значення можливості реалізації ризику порушень прав інтелектуальної власності;

F – середнє значення можливого штрафу за законодавством України (ВСУ від 31.03.95 р. № 4 «Про судову практику у справах про відшкодування морального (немайнового) збитку»).

При кількості цифрових зображень у 80 одиниць, вірогідності реалізації ризику, яка дорівнює 40% (R=0,4) та величині штрафу за порушення прав інтелектуальної власності, який дорівнюватиме 22000 грн., величина можливого збитку складе:

B=50*0,2*22000=220000 грн.

3.2.1 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 (40%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 220000 – 85483,85 = 134516,2 грн.

3.3 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:

$$ROSI = \frac{134516,2}{31513,25} = 4,3, \quad \text{частки одиниці,}$$

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, (6%);

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$4,3 > (6 - 5)/100 = 4,3 > 0,01.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{4,3} = 0,23 \text{ років (біля 3 місяців).}$$

3.4 Висновок

Отже, запропонований підхід щодо перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака можна вважати економічно доцільним. Використання такого підходу щодо ідентифікації цифрових зображень, що містять цифрові водяні знаки, та може бути використаний для розрізнення оригінальних цифрових зображень, захищених авторськими правами за допомогою впроваджених в них цифрових водяних знаків, від їх копій, а також для пошуку цифрових зображень різних форматів, що містять додаткову цифрову інформацію дозволяє отримувати економічний ефект, що може скласти 134516,2 грн. Капітальні витрати складають 31513,25 грн., експлуатаційні – 85483,85 грн. Коефіцієнт повернення інвестицій складає 4,3 грн./грн. і дає 4,3 грн. економічного ефекту на 1 грн. капітальних витрат.

ВИСНОВКИ

1. В результаті аналізу технологій цифрового маркування графічних зображень, а також дискримінантного аналізу встановлено, що стеганографія має багато областей застосування, одним з яких є вбудовування цифрових водяних знаків. Даний напрямок прекрасно підходить для вирішення завдань запобігання незаконному копіюванню і модифікації мультимедійної інформації, захисту авторських прав. Встановлено, що дискримінантний аналіз застосовується для вирішення задач розпізнавання образів, класифікації багатовимірних спостережень за принципом максимальної схожості при наявності навчальних ознак.

2. В результаті аналізу існуючих підходів до перевірки графічних зображень на наявність стеганографічно вбудованого водяного знака встановлено їх недоліки. Недоліками відомого підходу до декодування ЦВЗ, що міститься в зображенні формату JPEG [27] та підходу для ідентифікації даних зображення JPEG [28] є те, що вони можуть бути застосовані тільки в разі апріорного знання про присутність ЦВЗ в уже згадуваному зображенні формату JPEG і про закон його вбудовування, при цьому підходи застосовні тільки для ЦЗ формату JPEG. Недоліком відомого підходу-прототипу до ідентифікації зображення, що містить багаторазовий ЦВЗ [29] є те, що він застосовується тільки в умовах присутності апріорних відомостей про закон вбудовування ЦВЗ, в іншому випадку підхід стає неефективним і розрізнити, чи є ідентифікований документ (оригінал) копією або оригіналом, не представляється можливим.

3. Запропоновано підхід до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу. Метою розробки підходу є в можливість ідентифікації ЦЗ, що містять ЦВЗ в умовах відсутності апріорних відомостей про наявність ЦВЗ в даному зображенні і про закон вбудовування ЦВЗ. Це досягається за рахунок побудови власних характеристичних векторів зображень з навчальної вибірки, що

включають в себе статистичні характеристики, обчислені з розподілів вейвлет-коефіцієнтів і з розподілів похибки передбачення величин вейвлет-коефіцієнтів на різних піддіапазонах. У навчальну вибірку включаються два класи зображень: ЦЗ, що містять ЦВЗ і ЦЗ, що не містять ЦВЗ. Після навчання класифікатора, заснованого на дискримінантному аналізі, проводиться класифікація аналізованого зображення, тобто віднесення його до одного з класів. Завдяки цьому існує можливість ідентифікації ЦЗ, що містить ЦВЗ, тобто розрізнення зображення-оригіналу, захищеного авторськими правами від його копій, отриманих шляхом роздруківки і сканування.

4. В результаті оцінки ефективності запропонованого підходу до ідентифікації цифрових зображень, що містять цифровий водяний знак з використанням дискримінантного аналізу встановлено, що він може забезпечити ідентифікацію ЦЗ, що містять ЦВЗ в умовах відсутності апріорних відомостей про закон його вбудовування в аналізоване зображення, при цьому підхід може бути застосований для ідентифікації зображень різного формату. Встановлено, що в умовах відсутності апріорних відомостей про закон вбудовування ЦВЗ відомий підхід-прототип правильно ідентифікував 11 зображень-оригіналів з 150, а за допомогою запропонованого підходу вдалося правильно відрізнити 144 зображення-оригінали з 150 від їх високоякісних копій. Це підтверджує істотний позитивний ефект від впровадження запропонованого підходу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Арцыбашева А.А. Анализ подлинности изображения: Учебное пособие. / А.А. Арцыбашева, А.А. Козлов, В.Г. Сидоренко– М.: РУТ (МИИТ). 2018. – 106 с.

2. Коробейников А.Г. Цифровые водяные знаки в графических файлах / А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов // Научно-технический вестник информационных технологий, механики и оптики. - 2013. - № 1 (83). - С. 152-157.

3. Хорошко В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. – К. : ЮНИОР, 2003. – 505 с.

4. Грибунин В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

5. Osborne C.F. A Digital Watermark / C.F. Osborne, R.V. Schyndel, A.Z. Tirkel // IEEE Intern. Conf. on Image Processing. – 1994. – 86-90 p.

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

7. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. / А.В. Аграновский, Балакин А.В., Грибунин В.Г., Сапожников С.А. // – М.: Вузовская книга, 2009. – 220 с.

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

9. Phizmann B. Information Hiding Terminology / B. Phizmann // Information Hiding, Springer Lecture Notes in Computer Science. – 1996. – Vol. 1174. – 347-350 p.

10. Генне О.В. Основные положения стеганографии / О.В. Генне // «Защита информации. Конфидент». – 2000. – №3.

11. Westfeld A. Attacks on steganographic systems / A. Westfeld, A. Pfitzmann // Proc. of Information Hiding, Third Int. Workshop, Dresden, Germany, September 28-October 1, 1999. – pp. 61-75.

12. Fridrich J. Steganalysis of LSB encoding in color images / J. Fridrich, R. Du, L. Meng // Proc. IEEE Int. Conf. on Multimedia and Expo, New York, July 31-August 2. – 2000.

13. Fridrich J. Detecting LSB steganography in color and gray-scale images / J. Fridrich, M. Goljan, R. Du // IEEE Multimedia Magaz., Special Issue on Security (October-November 2001). – pp. 22-28.

14. Fridrich J. Practical steganalysis of digital images-state of the art / J. Fridrich, M. Goljan // Proc. SPIE Photonics West, Electronic Imaging (2002), Security and Watermarking of Multimedia Contents, San Jose, CA, – January 2002. – vol. 4675. – pp. 1-13.

15. Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes / J. Fridrich // Proc. Inf. HidingWorkshop, Lecture Notes in Computer Science, Springer, – vol. 3200. – 2004. – pp. 67-81.

16. Avcibas I. Image steganalysis with binary similarity measures / I. Avcibas, N. Memon, B. Sankur // IEEE Int. Conf. on Image Processing, Rochester, New York, – September 2002. – N. 3. – pp. 645-648.

17. Dumitrescu S. A new framework of LSB steganalysis of Digital Media / S. Dumitrescu, X. Wu // IEEE Trans. Signal Process. – October 2005. – vol. 53, no. 10. – pp. 3936-3947.

18. Wang Y. Steganalysis of block DCT image steganography / Y. Wang, P. Moulin // IEEE Workshop on Statistical Signal Processing. – 2003. – pp. 339-342.

19. Yu X. On estimation of secret message length in JSteg-like steganography / X. Yu, Y. Wang, T. Tan // Proc. of 7th ICPR. – 2004. – vol. 4. v pp. 673-676.

20. Jiang M., Wong E.K., Memon N., Wu X. Steganalysis, of halftone images / M. Jiang, E.K. Wong, N. Memon, X. Wu // IEEE ICASSP'05. – 2005. – Vol. 2. – P. 793-796.

21. Tanha, M. An Overview of Attacks against Digital Watermarking and their Respective Countermeasures / M. Tanha, S.D.S. Torshizi, M.T. Abdullah, F. Hashim // IEEE Published Proceeding in International Cyber Security Conference (CyberSec 2012). – 2012. – pp. 265-270.

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

23. Ситюк В.Є. Прогнозування. Моделі. Методи. Алгоритми: Навчальний посібник. – К.: «Маклаут», 2008. – 364 с.

24. Дуброва Т.А., Архипова М.Ю. Статистические методы прогнозирования в экономике. Учебно-методический комплекс. – М.: Изд. Центр ЕАОИ, 2008. – 136 с.

25 Дубров А.М. Многомерные статистические методы и основы эконометрики. [Текст]: Учебное пособие. – М.: МЭСИ, 2008. – 79 с.

26. Калинина В.Н. Введение в многомерный статистический анализ [Текст]: Учебное пособие. – ГУУ. – М., 2010. – 66 с.

27. Patent US 20040001626. Method and system to decode image watermarks / Severine Baudry, Philippe N'guyen. – Application 08.01.2003, publication 01.01.2004.

28. Patent US 20040015697. System and method for authentication of JPEG image data / Ricardo de Queiroz. – Application 22.07.2002, publication 22.01.2004.

29. Patent US 20050058320. Identification document including multiple watermarks / Geoffrey Rhoads, Ammon Gustafson. – Application 01.06.2004, publication 17.03.2005.

30. Миано Д. Форматы и алгоритмы сжатия изображений в действии. – М.: Триумф, 2003.

31. Воробьев В.И. Теория и практика вейвлет-преобразования. / В.И. Воробьев, В.Г. Грибунин. – С.-Петербург: Военный университет связи, 1999.

32. Гурман В.Е. Теория вероятностей и математическая статистика. – М.: Высшая школа, 1972.

33. Portilla J., Simoncelli E. A. Parametric texture model based on joint statistics of complex wavelet coefficients. – International Journal of Computer Vision, 2000.

34. Калугина Т.Ф. Математическая статистика. Учебное пособие / Т.Ф. Калугина, В.Ю. Киселев // Иван. гос. энерг. университет. – Иваново, 2001. – 236 с.

35. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	34	
6	А4	Спеціальна частина	12	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	4	
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 Шило.ppt

2 Диплом Шило.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-1 Шило О.В.

на тему: «Перевірка графічних зображень на наявність стеганографічно вбудованого водяного знака»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 76 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на можливість ідентифікації цифрових зображень, що містять ЦВЗ в умовах відсутності апріорних відомостей про наявність ЦВЗ і про закон вбудовування ЦВЗ.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу технологій цифрового маркування ЦЗ, дискримінантного аналізу і існуючих підходів до перевірки графічних зображень на наявність стеганографічно вбудованого ЦВЗ в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до ідентифікації ЦЗ, що містять ЦВЗ, з використанням дискримінантного аналізу та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід може бути використаний для розрізнення оригінального ЦЗ, захищеного авторськими правами, від його копій, а також для пошуку ЦЗ різних форматів, що містять додаткову цифрову інформацію.

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 Шило О.В. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

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