

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення стійкості зображень до спотворень від активних стеганографічних атак на основі методів умовної деконволюції у базисі перетворення Адамара

Виконала: ст. 2-го курсу, групи КІТС-22мз
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напрямку підготовки, спеціальності)

Лащевська Н.О.

(прізвище та ініціали)

Керівник: к.ф-м.н., доц., професор каф. МБІС

Шиян А.А.

(прізвище та ініціали)

«___» _____ 2024 р.

Опонент: д.т.н., проф., директор ННІЗІ ДУІКТ

Савченко В.А.

(прізвище та ініціали)

«___» _____ 2024 р.

Допущено до захисту

Голова секції УБ/кафедри МБІС

Ю.Я.

Юрій ЯРЕМЧУК

«___» _____ 2024 р.

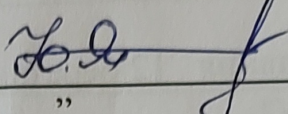
Вінниця ВНТУ - 2024 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти II-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС

 **Юрій ЯРЕМЧУК**
“ ” 2024 р.

ЗАВДАННЯ

на магістерську кваліфікаційну роботу студентці

Лащевській Наталії Олександрівні

(прізвище, ім'я, по-батькові)

1. Тема роботи Підвищення стійкості зображень до спотворень від активних стеганографічних атак на основі методів умовної деконволюції у базисі перетворення Адамара
2. Керівник роботи Шиян Анатолій Антонович, к.ф-м.н., доц.

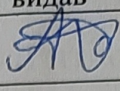
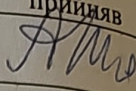
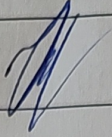
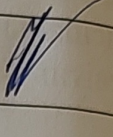
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “ 11” березня 2024 року № 81

2. Строк подання студентом роботи _____

1. 3. Вихідні дані до роботи: Набір тестових зображень у форматах PNG або JPEG різних розмірів; ображення з різними рівнями шуму та спотворень для тестування стійкості методу; Інструменти для генерації стеганографічних зображень; Мова програмування Python та бібліотеки для обробки зображень
4. Зміст текстової частини: 1. Огляд стеганографічних методів; 2. Математична модель методу умовної деконволюції в базисі перетворення Адамара; 3. Практична реалізація методу умовної деконволюції в базисі перетворення Адамара для боротьби з активними стеганографічними атаками; 4. Економічна частина; Висновки; Перелік посилань; Додатки
5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень)
презентація

6. Консультанти розділів роботи

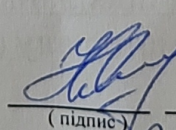
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	Шиян А.А., професор каф. МБІС		
Економічна частина	Причепя І.В., доцент кафедри ЕПВМ		

7. Дата видачі завдання 12 березня 2024 р.

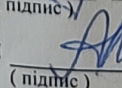
КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
		12.03.2024	25.03.2024	
1	Збір даних	12.03.2024	25.03.2024	
2	Обробка матеріалу	26.03.2024	08.04.2024	
3	Розробка теоретичної частини	09.04.2024	15.04.2024	
4	Виконання розділів 1 та 2	16.04.2024	13.05.2024	
5	Виконання розділу 3	14.05.2024	27.05.2024	
6	Виконання розділу 4 (економічна частина)	28.05.2024	04.06.2024	
7	Висновки за результатами аналізу	28.05.2024	04.06.2024	
8	Розробка презентації	05.06.2024	06.06.2024	
9	Здача в деканат		06.06.2024	

Студент

 Катерина Мисиревська
(підпис)

Керівник роботи

 А.А. Шиян
(підпис)

АНОТАЦІЯ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 86стор., 9 рис., 16 літературних джерел.

У роботі вирішена задача реалізації методу підвищення стійкості зображень до спотворень від активних стенографічних атак шляхом застосування методу умовної деконволюції у базисі перетворення Адамара, розглянуто методи покращення стійкості цифрових зображень до навмисних спотворень, спричинених стеганографічними атаками.

Основна мета роботи полягає у розробці та впровадженні ефективного методу захисту зображень від таких атак, який базується на використанні умовної деконволюції у базисі перетворення Адамара.

Для досягнення цієї мети було проведено наступні дослідження та розробки:

1. Розглянуто різні типи стеганографічних атак, їх характеристики та методи виявлення.
2. Вивчено властивості перетворення Адамара і його ефективність у виявленні аномалій та спотворень в цифрових зображеннях.
3. Запропоновано алгоритм умовної деконволюції, який дозволяє відновлювати оригінальне зображення шляхом зменшення впливу спотворень, спричинених атаками.
4. Запропонована програмна реалізація для оцінки ефективності даного методу в порівнянні з іншими відомими методами обробки зображень. Отримані результати продемонстрували високу ефективність та стабільність розробленого підходу.

Результати роботи показали, що використання умовної деконволюції у базисі перетворення Адамара значно підвищує стійкість зображень до активних стеганографічних атак, забезпечуючи більш точне та надійне відновлення оригінальних даних. Запропонований метод може бути

інтегрований у системи захисту інформації для забезпечення високого рівня безпеки цифрових зображень.

Ключові слова: Стеганографічні атаки, цифрові зображення, умовна деконволюція, перетворення Адамара, захист інформації, обробка зображень.

ABSTRACT

The text part of the qualifying work for obtaining a bachelor's degree: 86 pages, 9 figures, 16 literary sources.

The work solves the problem of implementing a method of increasing the resistance of images to distortions from active shorthand attacks by applying the conditional deconvolution method based on the Hadamard transformation, and methods of improving the resistance of digital images to intentional distortions caused by steganographic attacks are considered.

The main goal of the work is to develop and implement an effective method of image protection against such attacks, which is based on the use of conditional deconvolution in the basis of the Hadamard transformation.

To achieve this goal, the following research and development was carried out:

1. Different types of steganographic attacks, their characteristics and detection methods are considered.
2. The properties of the Hadamard transformation and its effectiveness in detecting anomalies and distortions in digital images were studied.
3. A conditional deconvolution algorithm is proposed, which allows restoring the original image by reducing the influence of distortions caused by attacks.
4. Proposed software implementation for evaluating the effectiveness of this method in comparison with other known methods of image processing. The obtained results demonstrated the high efficiency and stability of the developed approach.

The results of the work showed that the use of conditional deconvolution based on the Hadamard transform significantly increases the resistance of images to active steganographic attacks, providing more accurate and reliable restoration of the original data. The proposed method can be integrated into information protection systems to ensure a high level of digital image security.

Keywords: Steganographic attacks, digital images, conditional deconvolution, Hadamard transformation, information protection, image processing.

ЗМІСТ

1 ОГЛЯД СТЕГАНОГРАФІЧНИХ МЕТОДІВ	10
1.1	Поняття стеганографії 10
1.2	Види стеганографічних методів 14
1.3	Ризики та загрози використання стеганографії 16
1.4. Класифікація систем цифрової стеганографії	18
1.5 Стеганографічний аналіз	25
1.6 Типи атак на стеганографічну систему	26
2 МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА	32
2.1 Модель деградації образу	32
2.2 Ідентифікація імпульсної характеристики	34
2.3 Ідентифікація шуму	36
2.5 Реставрація образів за методом умовної деконволюції	40
2.6 Дискретна фільтрація за методом найменших квадратів	53
2.7. Деконволюція за критерієм форми результуючої імпульсної характеристики	58
2.8 Умовна деконволюція в області трансформант Адамара. Побудова матриці деградації образу	65
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА ДЛЯ БОРОТЬБИ З АКТИВНИМИ СТЕГАНОГРАФІЧНИМИ АТАКАМИ	93
4.ЕКОНОМІЧНА ЧАСТИНА МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ	98
ВИСНОВКИ	111
СПИСОК	113
ВИКОРИСТАНИХ ДЖЕРЕЛ	113
ДОДАТОК 1	118
ДОДАТОК 2	122
ДОДАТОК 3	132

	5
ДОДАТОК 4	143
ДОДАТОК 5	150
ПОКАЗНИКИ ЗВІТУ ПОДІБНОСТІ UNICHECK	150

ВСТУП

Актуальність проблеми, що розглядається у магістерській дисертації, полягає в наступному:

Зростаюча кількість стеганографічних атак: У зв'язку з поширенням цифрових зображень та широкого застосування методів стеганографії, кількість активних стенографічних атак зростає. Це створює необхідність в розробці ефективних методів захисту зображень від таких атак.

Потреба в надійних захисних методах: Збереження конфіденційності та цілісності зображень має велике значення в багатьох сферах, включаючи медицину, правоохоронну діяльність, а також в особистих комунікаціях. Отже, існує потреба в ефективних методах захисту від стеганографічних атак.

Обмеженість існуючих методів захисту: Багато з існуючих методів захисту від стеганографічних атак можуть бути обмануті або неефективні при використанні деяких агресивних технік атаки. Умовна деконволюція у базисі перетворення Адамара може стати інноваційним підходом до вирішення цієї проблеми.

Зростання використання цифрових технологій: З використанням цифрових технологій у всіх сферах життя зростає потреба в захисті цифрових даних, включаючи зображення, від різних видів атак. Пошук нових, більш ефективних методів захисту стає актуальною задачею.

Таким чином, дослідження підвищення стійкості зображень до спотворень від активних стенографічних атак методом умовної деконволюції у базисі перетворення Адамара є актуальним, оскільки воно вирішує важливу проблему забезпечення безпеки та цілісності цифрових зображень у сучасному цифровому середовищі.

Метою даної магістерської дисертації є розробка та реалізація методу підвищення стійкості зображень до спотворень від активних стенографічних атак шляхом застосування методу умовної деконволюції у базисі

перетворення Адамара. Головною метою є забезпечення ефективного захисту цифрових зображень від незаконних модифікацій та спотворень, які можуть бути виконані шляхом вбудовування прихованої інформації або інших атак на стеганографічний алгоритм.

Завдання дослідження:

1) Провести огляд наукових робіт та методів, пов'язаних із стеганографією, активними стенографічними атаками, умовною деконволюцією та перетворенням Адамара.

2) Розробити алгоритм, який дозволить ефективно відновити оригінальне зображення після спотворення внаслідок активних стенографічних атак.

3) Провести експериментальні дослідження, що дозволять виявити типові стенографічні атаки та їх вплив на зображення.

4) Реалізувати розроблений метод у вигляді програмного забезпечення та провести його тестування на різних типах зображень та різних умовах атак.

5) Провести аналіз отриманих результатів, визначити ефективність розробленого методу та зробити відповідні висновки щодо його застосування у практиці.

Ці завдання спрямовані на досягнення загальної мети дослідження та вирішення конкретних проблем, пов'язаних із захистом цифрових зображень від стенографічних атак.

Об'єктом дослідження є процес підвищення стійкості зображень до спотворень від активних стенографічних атак в сучасних радіотехнічних системах.

Предметом дослідження є метод умовної деконволюції у базисі перетворення Адамара для підвищення стійкості зображень до спотворень, які виникають внаслідок активних стенографічних атак.

Основними аспектами предмету дослідження є теоретичні основи методу умовної деконволюції, властивості базису перетворення Адамара та розробка алгоритму, який може ефективно застосовуватися для відновлення

оригінального зображення з врахуванням спотворень внаслідок стенографічних атак.

Отже, об'єкт та предмет дослідження в даній роботі об'єднуються навколо аналізу та розробки методу захисту цифрових зображень від активних стенографічних атак з використанням умовної деконволюції у базисі перетворення Адамара.

Наукова новизна дослідження полягає у впровадженні та вдосконаленні методу умовної деконволюції у базисі перетворення Адамара для підвищення стійкості зображень до спотворень, що виникають внаслідок активних стенографічних атак. Основні аспекти наукової новизни включають:

- ✓ Використання умовної деконволюції: у дослідженні використовується метод умовної деконволюції, який дозволяє ефективно відновлювати оригінальне зображення з урахуванням спотворень, що виникають внаслідок стенографічних атак. Цей метод дозволяє враховувати особливості спотворень та забезпечує високу якість відновленого зображення.

- ✓ Використання базису перетворення Адамара: для підвищення ефективності методу умовної деконволюції в даному дослідженні використовується базис перетворення Адамара. Цей базис має особливості, що дозволяють ефективно представляти та аналізувати зображення, що піддаються стеганографічним атакам, що вносять спотворення.

- ✓ Застосування до активних стенографічних атак: дослідження фокусується на активних стенографічних атаках, які вважаються більш складними та агресивними в порівнянні з пасивними атаками. Метод умовної деконволюції у базисі перетворення Адамара розробляється та тестується саме для цього типу атак, що вносить нові рішення у сферу захисту зображень.

Таким чином, наукова новизна дослідження полягає у розробці та застосуванні вдосконаленого методу умовної деконволюції у базисі перетворення Адамара для захисту цифрових зображень від активних стенографічних атак, що вирізняється новаторством і важливістю для сучасної області цифрової безпеки.

Практичне значення дослідження полягає в наступному:

✓ **Забезпечення безпеки зображень:** розроблений метод умовної деконволюції у базисі перетворення Адамара може бути використаний для захисту цифрових зображень від активних стенографічних атак. Це дозволяє забезпечити конфіденційність та цілісність важливих зображень, наприклад, медичних зображень, зображень у сфері правоохоронних органів тощо.

✓ **Покращення ефективності методів захисту:** використання умовної деконволюції у базисі перетворення Адамара може сприяти покращенню ефективності існуючих методів захисту від стенографічних атак. Це важливо для постійного підвищення рівня безпеки цифрових даних у сучасному інформаційному середовищі.

✓ **Застосування у практичних сферах:** розроблений метод може мати широкі застосування у різних сферах, де збереження конфіденційності та цілісності зображень є критично важливим. Це можуть бути медична діагностика, кримінальне розслідування, стеганографія у комунікаціях тощо.

✓ **Внесення вкладу у науковий прогрес:** дослідження додає нові знання у галузі цифрової безпеки та стеганографії. Розроблений метод умовної деконволюції у базисі перетворення Адамара може стати основою для подальших досліджень та розробок в цій області.

Отже, практичне значення дослідження полягає в його потенційній здатності забезпечити безпеку цифрових зображень і покращити ефективність методів захисту від стенографічних атак у різних практичних сферах застосування.

1 ОГЛЯД СТЕГАНОГРАФІЧНИХ МЕТОДІВ

1.1 Поняття стеганографії

Стеганографія – це мистецтво приховування секретної інформації в файлі таким чином, що тільки відправник та отримувач можуть знати про її наявність. Конфіденційна інформація закодована так, що сам факт існування повідомлення приховується.

У порівнянні з досить добре дослідженими криптографічними системами, поняття і оцінки безпеки стеганографічних систем більш складні і мають багатогранні тлумачення. Зокрема, це пояснюється як недостатньою теоретичною та практичною опрацюванням питань безпеки стегосистем, так і великою різноманітністю завдань стеганографічного захисту інформації [10].

Можна сказати, що стеганографія – це один із шляхів підтримки інформаційної безпеки. Вона являє собою метод організації зв'язку, який приховує сам факт наявності таємних повідомлень. Стеганографічні методи активно використовуються для захисту інформації від сторонніх користувачів та для маскування програмного забезпечення [11].

На конференції Information Hiding (First Information Workshop) у 1996 році були обговорені всі базові поняття стеганографії та прийнята єдина термінологія [11]. Згідно з цією термінологією стеганографічна система або стегосистема – це сукупність засобів та методів, які використовуються для формулювання таємного каналу зв'язку. Будь-яка інформація, в якій приховані таємні дані, називається контейнером. За контейнер може слугувати будь-який файл чи потік даних. Контейнер, який не містить таємного повідомлення, називають порожнім, а той, що містить – заповненим або стегоконтейнером. Канал передачі стегоконтейнера має назву стеганографічного каналу або стегоканалу. Таємний ключ, який необхідний

для «вкраплення» інформації в контейнер, називається стегоключем або просто ключем. Залежно від кількості рівнів захисту в стегосистемі може використовуватись як один, так і декілька ключів[12].

Визначення 1.1. Стеганографічна система (стеганосистема) – це сукупність Σ

$= (X, M, K, Y, E, D)$ пустих контейнерів X , повідомлень M , ключів K , заповнених контейнерів Y і перетворень E та D , що їх пов'язують (алгоритмів вкраплення та вилучення).

Визначення 1.2. Контейнер (носій) – це нетаємна інформація, в якій будуть приховані конфіденційні дані (повідомлення). В комп'ютерній стеганографії контейнером може слугувати будь-який файл чи потік даних. В силу своєї надлишковості найчастіше цифровими контейнерами виступають зображення, аудіо чи відеосигнали.

Визначення 1.3. Повідомленням називається таємна інформація, наявність якої необхідно приховати.

Визначення 1.4. Стеганоключ – елемент стеганосистеми, який параметризує алгоритми вкраплення й вилучення, та відомий тільки відправнику і одержувачу стеганоконтейнера. Стеганоключ зокрема може визначати область вкраплення (часова/просторова чи частотна), базис частотного розкладу, правила розбиття контейнера на сегменти, силу вкраплення, індекси задіяних коефіцієнтів, точки квантування, кодову книгу, вектор розширення та інше.

Визначення 1.5. Пустим називають контейнер, який не містить прихованого стеганографічними методами повідомлення.

Визначення 1.6. Контейнер, що містить приховану інформацію, називають заповненим або стеганоконтейнером, або стеганограмою.

Задача стеганографічної системи – розмістити вхідне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити нічого, крім його основною вмісту. Основний вміст контейнера не відіграє ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна

передача повідомлення, вміщеного в ньому (стеганограми). Потрібно обов'язково враховувати те, що сам факт відправлення контейнера від автора до одержувача не повинен виглядати дивним, а також не повинно спостерігатись помітних відхилень контейнера від норми.

Схематично узагальнена модель стеганографічної системи представлена на рисунку 1.1.



Рисунок 1.1 – Узагальнена модель стеганографічної системи

За аналогією з криптографією, якщо при вкрапленні та вилученні повідомлення використовується один і той же ключ – стеганосистема вважається симетричною, якщо різні – асиметричною.

Стеганографія, як наука, інтегрує в собі здобутки криптографії, теорії інформації, теорії ймовірності та математичної статистики, теорії дискретних ортогональних перетворень, цифрової обробки сигналів та зображень, розпізнавання образів та ін. Зауважимо, що існує підхід, згідно якому стеганографічні системи розглядаються як узагальнення криптографічних. Стеганографічні методи володіють унікальними властивостями, що робить їх незамінними при вирішенні певних задач захисту.

Комп'ютерна стеганографія розвивається у декількох напрямках, що мають як багато спільних рис, так і певні характерні відмінності, спричинені особливостями практичного застосування. Так, серед стеганосистем

виділяють системи прихованої передачі даних, цифрових водяних знаків, ідентифікаційних номерів («відбитків пальців») та заголовків [13]. Задача будь-якої стеганографічної системи – розмістити певне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити різниці між модифікованим контейнером та оригінальним. Зазвичай стеганосистема будується так, щоб забезпечити заданий компроміс її основних характеристик, таких як непомітність, стійкість, безпека, пропускну здатність, обчислювальна складність. Розглянемо особливості кожного з виділених видів стеганосистем [12].

Системи прихованої передачі даних застосовуються для організації таємної комунікації. Вони відрізняються від усіх інших тим, що в цьому випадку оригінальний вміст контейнера не грає ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача вкрапленого повідомлення. Разом із тим потрібно обов'язково враховувати, що факт відправлення контейнера від відправника до одержувача не повинен виглядати дивним, а також не повинно спостерігатися помітних відхилень контейнера від норми. Основна мета таких систем – приховати наявність стеганоканалу, унеможливити розрізнення пустих і заповнених контейнерів без знання ключа. Для таких систем звичайно вважається, що контейнер не підлягає спотворенням в процесі його передачі по каналу зв'язку ($Y' = Y$), тому що таємна комунікація відбувається через відкритий канал цифрової мережі, наприклад, інтернет, що забезпечує відсутність спотворень інформації при її передачі.

Комп'ютерна стеганографія знайшла своє застосування в багатьох областях людської діяльності: таємна передача конфіденційної інформації в мультимедійних файлах; захист авторських прав на аудіо- та відеоматеріали в електронному вигляді; створення таємних архівів; подолання систем моніторингу та управління мережевими ресурсами; камуфлювання програмного забезпечення; обслуговування політичної, технічної, військової та інших видів розвідки [13].

Щодо актуальності стеганографії в теперішній час, можна сказати, що комп'ютерна стеганографія розвивається доволі інтенсивно, застосовуються відомі і розробляються нові методи стеганографії, засновані на різноманітних областях науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стегоконтейнеру, що зберігає дані[20].

Таким чином, до теперішнього часу для цілого кола фахівців з'явилася необхідність ознайомлення з основами сучасної комп'ютерної стеганографії, завданням яких є не тільки розробка, аналіз або протидія засобам стеганографії, а й кваліфікований вибір існуючих засобів і їх вміле використання для вирішення конкретних прикладних завдань захисту інформації.

1.2 Види стеганографічних методів

Залежно від виду спеціальних властивостей форматів розрізняють такі стеганографічні методи:

- засновані на використанні зарезервованих для розширення полів комп'ютерних форматів файлів. Поля для розширення є в багатьох мультимедійних форматах і призначені для вдосконалення, оновлення і сумісності нових версій форматів зі старими. Як правило, ці поля заповнюються нульовою інформацією і не враховуються програмами, і тому можуть бути використані для передачі додаткової інформації. Недоліком цих методів є низький ступінь скритності і передача невеликих обсягів інформації, що приховується[10,12].

- Засновані на спеціальному форматуванні текстових файлів, відомі вже давно, використовувалися задовго до появи комп'ютерних технологій і включають в себе методи[14]:

✓ використовують заздалегідь відоме зміщення слів, речень, абзаців в текстовому файлі, засновані на зміні положення рядків і розстановки слів в реченні, що виробляється вставкою додаткових пробілів між словами, збільшень проміжків непомітно візуально, але фактично передає приховану інформацію;

✓ засновані на виборі певних позицій букв (нульовий шифр). Наприклад, вибір п'ятої літери кожного останнього слова в рядку в межах однієї сторінки. Сюди ж відносяться художні прийоми тайнопису - акростих, добре відомий знавцям поезії, це така організація віршованого тексту, при якій, наприклад, початкові літери кожного рядки утворюють приховуване повідомлення [11];

✓ використовують спеціальні властивості полів форматів, які не відображаються на екрані. Наприклад, використання чорного шрифту на чорному тлі спеціальних «невидимих», прихованих полів для організації виноска і посилань [10].

– Засновані на приховуванні в невикористовуваних місцях гнучких дисків. Назва цієї групи говорить сама за себе і має ті ж переваги і недоліки, що і методи, засновані на використанні зарезервованих для розширення полів форматів.

– Засновані на імітуючій функції (мнемосхема-функція) - цей вид стеганографії заснований на генерації текстів і є узагальненням акровірша. Для заданого приховуваного повідомлення генерується осмислений текст, який містить приховуване повідомлення. При цьому текст є граматично і синтаксично правильним і статистично еквівалентним до текстів на подібну тему. Такі тексти можуть не бути підозрілими для систем моніторингу мережі, але все ж людина може швидко визначити відсутність будь-якого сенсу в змісті тексту [13].

– Засновані на використанні кодів, що виправляють помилки; приховування даних в додатковій інформації, використовуваної перешкодозахищеними кодами при виправленні випадкових помилок і

забезпеченні точності передачі цифрової інформації. Якщо інформація захищена, а на стороні приймача код знятий, то спостерігач не буде навіть знати, що було відправлено повідомлення.

– Засновані на видаленні заголовка файлу. У цьому методі приховуване повідомлення шифрується і у результаті видаляється ідентифікація заголовку, залишаючи тільки шифровані дані, які видаються за випадкові, можливо, як спотворена інформація. Одержувач заздалегідь знає про передачу секретних даних і має недостатньо інформації. При цьому проблема приховування вирішується тільки частково. Цей метод не є повністю стеганографічним методом, а служить скоріше доповненням до них, хоча багато програмні засоби (White Noise Storm) забезпечують цю додаткову ступінь захисту з використанням алгоритму шифрування PGP [12].

Це лише деякі методи, що ілюструють евристичний підхід в стеганографії. Недоліками відомих методів, заснованих на використанні спеціальних властивостей форматів файлів, є:

- низький ступінь скритності (скритність ґрунтується на незнанні противником самого алгоритму приховування);
- передача невеликих обсягів інформації, що приховується.

До переваг можна віднести простоту реалізації. Слід зауважити, що вже опубліковано ряд програм, що реалізують деякі алгоритми [10,14].

1.3 Ризики та загрози використання стеганографії

Великі корпорації все більше усвідомлюють ризики, пов'язані із використанням стеганографії. З брандмауерами, системи виявлення вторгнень та іншими відповідними засобами захисту, які ще не в змозі виявити повідомлення, сховані в файлі, хакери здатні виконувати такі завдання, як створення креслень для проникнення в комп'ютерні системи компанії, а саме

в аудіофайли, що зберігаються на власній веб-сторінці фірми [13].

В усьому світі уряди прагнуть забезпечити, отримання ключів шифрування для читання повідомлень, коли вони викликають підозру, що такі злочинці, як контрабандисти наркотиків, відмивачі коштів чи терористи, використовують зашифровані повідомлення. Як наслідок, ті, хто зловмисним наміром не використовують метод спілкування, можуть бути легко перехоплені і прочитані.

Пошук в Інтернеті відкриє сотні тисяч посилань на сторінки зі стеганографією. Посилання включають посилання на безкоштовне завантажуване програмне забезпечення та математичні формули описуючи, як працює ця техніка. Злочинці будь-якого типу намагаються приховувати дані щодня, а в Інтернеті дає можливості це робити. Коли приховування секретних даних використовується для зловмисних цілей, ця техніка спілкування стає загрозою для безпеки всесвітньої інформаційної інфраструктури [12].

Стеганографія створює ризики, для національної безпеки. Хоча стеганографія, як видається, є гарним способом безпечного обміну конфіденційною інформацією, її можна також неправильно використовувати. Існують спекуляції про те, що терористи використовують ці методи для спілкування через Інтернет, здавалося б, невинні веб-сайти. Основна теорія полягає в тому, що терористичні групи, як стверджується, приховують карти та фотографії терористичних цілей та розміщують інструкції щодо терористичної діяльності в спортивних чатах, порнографічних плакатах та інших веб-сайтах. Фактично незабаром після 11 вересня 2001 року було проведено розслідування про сканування більше двох мільйонів зображень з веб-сайту eBaу для прихованих повідомлень, що містяться в них. Нібито нічого не знайдено, але уряд США на той момент, безсумнівно, побачив ризик [14].

Загроза, викликана стеганографією, дуже реальна. Її використання нелегко виявити або перехопити, оскільки інформація не повинна транслюватися через Інтернет. Приховане повідомлення може зберігатись без

нагляду на веб-сайті, і його можна переглядати з усього світу. Незважаючи на те, що головна загроза на даний момент полягає у забезпеченні національної безпеки, ця технологія безсумнівно використовується і для інших аморальних цілей. Тому, хоч стеганографія ще не є такою загрозою, але ІТ-аудитори борються проти неї. Це той випадок, який необхідно розглянути та зрозуміти для можливих майбутніх подій [45].

Не всі випадки використання стеганографії є поганими. Водяні знаки можуть бути вставлені для посвідчення особи, що ускладнює підробку для того, хто намагається зробити копію. Іншим позитивним чинником є те, що абсолютно-правова чи конфіденційна інформація може бути передана більш надійно. Крім того, компанії використовують техніку, щоб робити повсякденний бізнес більш безпечним. Наприклад, корпорація Digimarc, провідний постачальник захищених медіа-рішень, надає безпечні рішення щодо ідентифікації водяних знаків урядам у всьому світі.

1.4. Класифікація систем цифрової стеганографії

Задача будь-якої стеганографічної системи – вкрасити повідомлення в контейнер таким чином, щоб будь-який сторонній спостерігач не зміг помітити різниці між оригінальним контейнером та модифікованим. Зазвичай система будується так щоб забезпечити певний компроміс її базових характеристик, до яких відносяться невідчутність, стійкість, безпека, пропускна здатність створюваного стеганоканалу та обчислювальна складність реалізації.

Цифрова стеганографія як наука народилася буквально в останні роки. Вона містить у собі такі напрями:

- вбудовування інформації з метою її прихованої передачі;
- вбудовування цифрових водяних знаків (ЦВДЗн) (watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting);
- вбудовування заголовків (captioning).

ЦВДЗн можуть застосовуватися, в основному, для захисту від

копіювання та несанкціонованого використання. У зв'язку з бурхливим розвитком технологій мультимедіа гостро встало питання захисту авторських прав і інтелектуальної власності, представлені в цифровому вигляді. Прикладами можуть бути фотографії, аудіо- та відеозаписи та ін. Переваги, які дають подання та передача повідомлень у цифровому вигляді, можуть виявитися перекресленими з легкістю, з якою можливі їх викрадення або модифікація. Тому розробляються різні засоби захисту інформації, організаційного та технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в захисті об'єкта невидимих міток – ЦВДЗн. Розробки в цій сфері ведуть найбільші фірми в усьому світі. Оскільки методи ЦВДЗн почали розроблятися зовсім недавно, то тут є багато неясних проблем, що вимагають свого вирішення [11].

Назву цей метод одержав від усім відомого способу захисту цінних паперів, у тому числі грошей, від підробки. Термін "digital watermarking" був уперше застосований у роботі [12]. На відміну від звичайних водяних знаків ЦВДЗн можуть бути не тільки видимими, але й, як правило, невидимими. Невидимі ЦВДЗн аналізуються спеціальним декодером, що виносить рішення про їх коректність. ЦВДЗн можуть містити деякий автентичний код, інформацію про власника або яку-небудь керуючу інформацію. Найбільш придатними об'єктами захисту за допомогою ЦВДЗн є нерухливі зображення, файли аудіо- й відеоданих [13].

Технологія вбудовування ідентифікаційних номерів виробників має багато загального з технологією ЦВДЗн. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний вбудований номер (звідси й назва – дослівно "відбитки пальців"). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то "відбитки пальців" швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад,

для підпису медичних знімків, нанесення легенди на карту й т.д. Метою є зберігання різноманітної представленої інформації в єдиному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній потенційний злоумисник.

Оскільки цифрова стеганографія є молодого наукою, то її термінологія не до кінця сформувалася. Основні поняття стеганографії були погоджені на Першій міжнародній конференції з приховання даних [12]. Проте навіть саме поняття "стеганографія" трактується по-різному. Так, деякі дослідники розуміють під стеганографією тільки приховану передачу інформації. Інші відносять до стеганографії такі додатки, як наприклад, метеорний радіозв'язок, радіозв'язок із псевдовипадковою перебудовою радіочастоти, широкосмуговий радіозв'язок. Неформальне визначення того, що таке цифрова стеганографія, могло б виглядати в такий спосіб: "наука про непомітне і надійне приховання одних бітових послідовностей в інших, що мають аналогову природу". Під це визначення саме підпадають всі чотири вищенаведені напрями приховання даних, а додатка радіозв'язку – немає. Крім того, у визначенні міститься дві головні вимоги до стеганографічному перетворення: непомітність і надійність, або стійкість до різного роду перекручування. Згадування про аналогову природу цифрових даних підкреслює той факт, що вбудовування інформації виконується в оцифровані безперервні сигнали. Таким чином, у рамках цифрової стеганографії не розглядаються питання впровадження даних у заголовки ІР-пакетів і файлів різних форматів, у текстові повідомлення [14].

Яким б різними не були напрями стеганографії, пропоновані ними вимоги багато в чому збігаються, як це буде показано далі. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВДЗн полягає в тому, що в першому випадку злоумисник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більше того, у злоумисника на законних підставах може бути пристрій виявлення ЦВДЗн (наприклад, у

складі DVD-програвача).

Під словом "непомітний" у нашому визначенні цифрової стеганографії мається на увазі обов'язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що висуває до системи передачі досить важко формалізовані вимоги.

На рисунку 1.2 наведена класифікація систем цифрової стеганографії. Стеганосистема утворює стеганоканал, по якому передається заповнений контейнер. Цей канал вважається підданим впливам з боку порушників. Згідно з Г. Сіммонсом [13], у стеганографії звичайно розглядається така постановка завдання ("проблема ув'язнених").

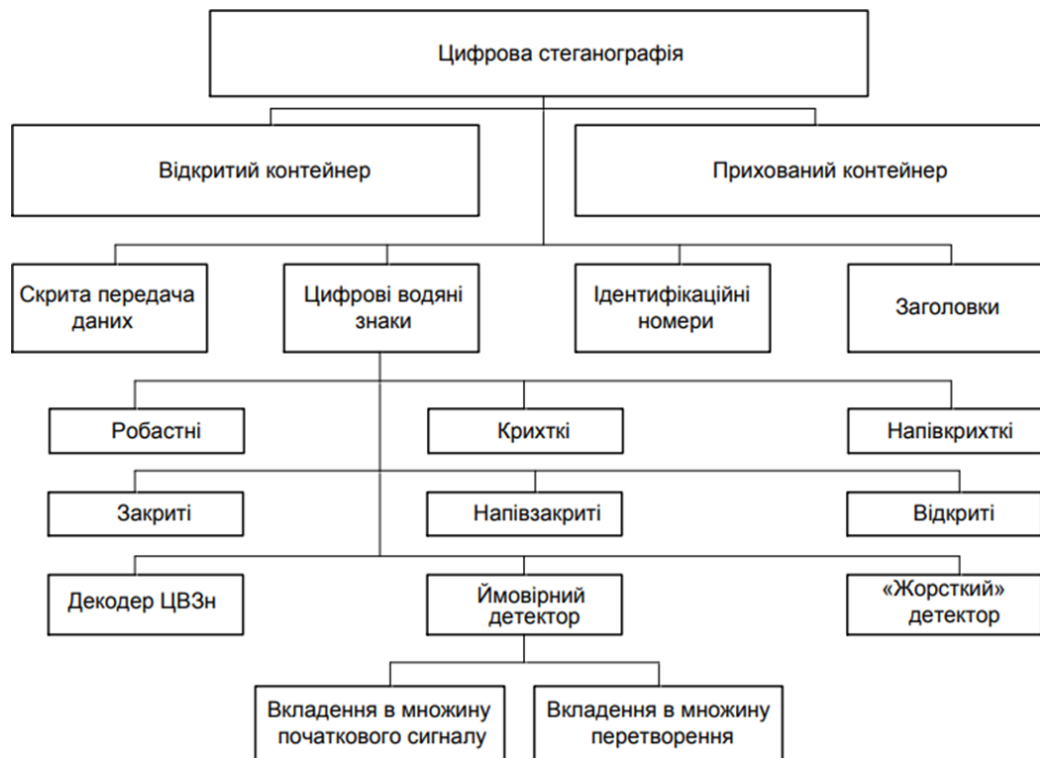


Рисунок 1.2 – Класифікація систем цифрової стеганографії

Для того щоб стеганосистема була надійною, необхідне виконання при її проектуванні ряду вимог.

Безпека системи повинна повністю визначатися таємністю ключа. Це означає, що зломисник може повністю знати всі алгоритми роботи стеганосистеми та статистичні характеристики множин повідомлень і

контейнерів, і це не дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері.

Знання зловмисником факту наявності повідомлення в якому-небудь контейнері не повинне допомогти йому при виявленні повідомлень в інших контейнерах.

Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення у візуально незначущі множини сигналу. Однак ці ж множини використовують і алгоритми стиснення. Тому, якщо зображення буде надалі піддаватися стисненню, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися у візуально значущі множини, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра [12].

Стеганосистема ЦВДЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не утримує. У деяких додатках таке виявлення може привести до серйозних наслідків. Наприклад, помилкове виявлення ЦВДЗ на DVD-диску може викликати відмову від його відтворення плеєром.

Повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна, в основному, для стеганосистем прихованої передачі інформації). У третьому розділі введемо поняття прихованої пропускної здатності й розглянемо шляхи її досягнення.

Стеганосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВДЗ, тобто складний стеганокодер і простий стегано-декодер.

До ЦВДЗ висуваються такі вимоги [11]:

ЦВДЗ повинен легко (обчислювально) витягатися законним користувачем;

ЦВДЗ повинен бути стійким або нестійким до навмисних і випадкових

впливів.

Якщо ЦВДЗ використовується для підтвердження дійсності, то неприпустима зміна контейнера повинна призводити до руйнування ЦВДЗ (тендітний ЦВДЗ). Якщо ж ЦВДЗ містить ідентифікаційний код, логотип фірми тощо, то він повинен зберегатися при максимальних перекручуваннях контейнера, що звичайно, не приводять до істотних перекручень вихідного сигналу. Наприклад, у зображенні можуть бути відредаговані колірна гама або яскравість, в аудіозаписі – посилене звучання низьких тонів і т.п. Крім того, ЦВДЗ повинен бути роботоздатним стосовно афінних перетворень зображення, тобто його поворотів, масштабування.

При цьому треба розрізняти стійкість самого ЦВДЗ і здатність декодера правильно його виявити. Скажемо, при повороті зображення ЦВДЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатки, коли ЦВДЗ повинен бути стійким стосовно одних перетворень і нестійким стосовно інших. Наприклад, може бути дозволене копіювання зображення (ксерокс, сканер), але накладена заборона на внесення в нього яких-небудь змін.

Повинна бути можливість додавання до стега додаткового ЦВДЗ. Наприклад, на DVD-диску є мітка про допустимість однократного копіювання. Після здійснення такого копіювання необхідно додати мітку про заборону подальшого копіювання. Можна було б, звичайно, видалити перший ЦВДЗ і записати на його місце другий, однак це суперечить припущенню про важковіддаленність ЦВДЗ. Кращим виходом є додавання ще одного ЦВДЗ, після якого перший не буде братися до уваги. Однак наявність декількох ЦВДЗ на одному повідомленні може полегшити атаку з боку злоумисника, якщо не почати спеціальних заходів.

У цей час технологія ЦВДЗ перебуває в початковій стадії свого розвитку. Як показує практика, повинно пройти років 10 – 20 для того, щоб новий криптографічний метод почав широко використовуватися в суспільстві. Напевно, аналогічна ситуація буде спостерігатися й зі стеганографією. Однією

із проблем, пов'язаних зі ЦВДЗ, є різноманіття вимог до них, залежно від додатка. Розглянемо докладніше основні множини застосування ЦВДЗ.

Спочатку розглянемо проблему піратства, або необмеженого неавторизованого копіювання. Хоча інформація може бути зашифрована під час передачі, ніщо не перешкодить отримувачу піратської версії зайнятися її копіюванням після розшифровки. Отже, у цьому випадку потрібен додатковий рівень захисту від копіювання, що не може бути забезпечений традиційними методами. Існує можливість впровадження ЦВДЗ, що дозволяє відтворення та забороняє копіювання інформації [13].

Важливою проблемою є визначення дійсності отриманої інформації, тобто її автентифікація. Звичайно для автентифікації даних використовуються засоби цифрового підпису. Однак ці засоби не зовсім підходять для забезпечення автентифікації мультимедійної інформації. Справа в тому, що повідомлення, постачене електронним цифровим підписом, повинне зберігатися й передаватися абсолютно точно, "бітів у бітів". Мультимедійна ж інформація може незначно спотворюватися як при зберіганні (за рахунок стиску), так і при передачі (вплив одиночних або пакетних помилок у каналі зв'язку). При цьому її якість залишається припустимою для користувача, але цифрової підпис працювати не буде. Одержувач не зможе відрізнити справжнє, хоча і трохи перекручене повідомлення, від помилкового. Крім того, мультимедійні дані можуть бути перетворені з одного формату в інший. При цьому традиційні засоби захисту цілісності працювати також не будуть [10].

Можна сказати, що ЦВДЗ здатно захистити саме зміст аудіо-, відеоповідомлення, а не його цифрове подання у вигляді послідовності бітів. Крім того, важливим недоліком цифрового підпису є те, що його легко видалити із завіреного ним повідомлення, після чого прилаштувати до нього новий підпис. Видалення підпису дозволить зловмиснику відмовитися від авторства, або ввести в оману законного одержувача щодо авторства повідомлення. Система ЦВДЗ проектується таким чином, щоб виключити

можливість подібних порушень.

Основні множини використання технології ЦВДЗ можуть бути об'єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації та прихований зв'язок (рис. 1.3).



Рисунок 1.3 – Потенційні множини застосування стеганографії

Популярність мультимедіа-технологій викликало множину досліджень, пов'язаних з розробкою алгоритмів ЦВДЗ для використання в стандартах MP3, MPEG-4, JPEG2000, захисту DVD-дисків від копіювання.

1.5 Стеганографічний аналіз

Основною метою стеганоаналізу є моделювання стеганографічних систем та їхнє дослідження для отримання якісних і кількісних оцінок надійності використовуваного стеганографічного перетворення, а також побудова методів виявлення приховуваної в контейнері інформації, її зміни

або руйнування.

За рівнем забезпечення таємності стегосистеми поділяються на теоретично стійкі системи, практично стійкі і нестійкі.

Теоретично стійка (абсолютно надійна) стегосистема здійснює приховування інформації тільки в тих фрагментах контейнера, значення елементів яких не перевищують рівень шумів або помилок квантування, і при цьому теоретично доведено, що неможливо створити стеганалітичний метод виявлення прихованої інформації.

Практично стійка стегосистема проводить таку модифікацію фрагментів контейнера, зміни яких можуть бути виявлені, але відомо, що на даний момент необхідні стеганалітичні методи в противника відсутні або поки що не розроблені.

Нестійка стегосистема приховує інформацію таким чином, що існуючі стеганалітичні засоби дозволяють її виявити. У цьому випадку стеганографічний аналіз допомагає знайти уразливі місця стеганографічного перетворення і провести його покращення таким чином, щоб усі зміни, внесені в контейнер, знову виявилися б в області теоретичної або практичної нерозрізненості.

1.6 Типи атак на стеганографічну систему

Стегосистема вважається зламаною, якщо противникові, принаймні, вдалося довести існування прихованого повідомлення в перехопленому контейнері. Передбачається, що він здатний проводити будь-які види атак і має необмежені обчислювальні можливості. Якщо йому не вдається підтвердити гіпотезу про те, що в контейнері приховано секретне повідомлення, то стегосистема вважається стійкою. Зазвичай виділяють декілька етапів зламу стеганографічної системи:

- виявлення факту присутності прихованої інформації;
- витягування приховуваного повідомлення;
- перекручування (підміна) приховуваної інформації;
- видалення (руйнування) приховуваного повідомлення;
- заборона на здійснення будь-якого пересилання інформації, у тому числі і приховуваної.

Перші два етапи відносяться до пасивних атак на стегосистему, а останні – до активних (або зловмисних) атак. Виділяють такі види атак на стегосистеми:

- атака з відомою стеганограмою, коли для аналізу доступна тільки стеганограма;
- атака з відомим контейнером, коли є можливість проводити аналіз зі стеганограмою і відповідним йому вихідним контейнером;
- атака з відомим прихованим повідомленням, якщо для аналізу надані зразки приховуваного повідомлення і відповідної стеганограми. Результати їхнього спільного аналізу можуть бути використані для проведення наступних атак на стегосистему (хоча це може виявитися дуже важкою задачею, яка еквівалентна першій);
- атака з вибором контейнера, якщо під час аналізу відомий використовуваний стеганографічний алгоритм і вихідний зразок контейнера;
- атака з вибором стеганограми, коли за допомогою досліджуваної стегосистеми (або алгоритму) є можливість створювати відповідні стеганограми для обраного повідомлення. Мета такої атаки полягає в тому, щоб визначити, які зразки стеганограм можуть ідентифікувати використання певних стегозасобів або алгоритмів;
- атака з повною інформацією, якщо надана вся необхідна інформація для аналізу: стеганографічний алгоритм, контейнери і відповідні їм стеганограми.

Основна мета атаки на стеганографічну систему аналогічна атакам на криптосистему з тією лише різницею, що різко зростає значимість активних

атак. Будь-який контейнер може бути змінений з метою видалення або руйнування прихованого повідомлення, незалежно від того існує воно в контейнері чи ні. Виявлення існування прихованих даних зберігає час на етапі їхнього видалення, тому що буде потрібно обробляти тільки ті контейнери, які містять приховану інформацію. Навіть за найкращих умов для атаки, задача витягування прихованого повідомлення з контейнера може виявитися дуже складною. Однозначно стверджувати про факт наявності прихованої інформації можна лише після її виділення в явному вигляді. Іноді метою стеганографічного аналізу є не алгоритм взагалі, а пошук, наприклад, конкретного стегоключа, що використовується для вибору бітів контейнера в стеганоперетворенні.

Будь-яке стеганографічне перетворення, як правило, базується на двох принципах:

- як носій прихованої інформації (контейнер) вибирається об'єкт, що допускає перекручування власної інформації, зберігаючи при цьому функціональність;
- рівень внесених перекручувань повинний бути нижче рівня чутливості засобів розпізнавання.

Як контейнери можуть використовуватися практично всі носії інформації, застосовувані в мережах передавання даних. При цьому методи приховування інформації орієнтуються в основному на внутрішню структуру контейнера, яка може являти собою символні або бітові дані, коефіцієнти перетворення Фур'є, широкосмугове кодування, коефіцієнти ущільнення та ін. Приховування інформації в медіа середовищі вимагає дотримання певних умов при внесенні змін, щоб не проявлялися сліди використання стеганографічного перетворення.

Наприклад, стосовно до зображень, такі зміни можуть час від часу ставати видимими для людського ока і вказувати на використання стеганографічних засобів. Аналіз навмання вибраних зображень в Інтернеті показує, що деякі з них не мають тієї інформаційної надлишковості, що її

повинні мати типові файли, тобто в них міститься інформація, в якій немає необхідності під час звичайного візуального перегляду зображення. Подібну картину можна отримати, наприклад, у результаті наявності бруду на склі сканера або обробки файлу зображення спеціальними ефектами, передбаченими графічними редакторами, або ж використовуючи стеганографічне перетворення. Сліди, залишені стегозасобами, можуть фактично допомогти виявити існування вбудованого повідомлення, таким чином, компрометуючи стегосистему в цілому.

Однією з головних задач стеганоаналізу є дослідження можливих слідів застосування стеганографічних засобів і розробка методів, які б дозволяли виявляти факти їхнього використання. Застосування конкретного стеганографічного перетворення вимагає від стеганалітика персонального підходу до його дослідження [11].

Дослідження повідомлень, прихованих стеганографічними засобами, або, точніше, підозрілих у цьому відношенні, є досить болісним процесом.

Часто стеганалітик не може навіть сказати, наприклад, чи приховується якесь змістовне повідомлення за незграбно складеним або просто безграмотним текстом. І, навіть, якщо він цілком впевнений, що таке повідомлення там приховано, знайти його найчастіше просто неможливо.

Для успішного проведення стеганоаналізу необхідно, але не достатньо:

- мати для аналізу стегозасіб, за допомогою якого здійснюється приховування повідомлення;
- мати можливість відновлювати застосовувані в стегосистемі криптографічний і стеганографічний алгоритми, проводити їхній експертний аналіз і розробляти алгоритм визначення ключів;
- мати в наявності необхідний обчислювальний ресурс для проведення стеганоаналізу;
- підтримувати на відповідному рівні теоретичні і практичні знання в галузі цифрової стеганографії.

На практиці стеганографічний аналіз розвивається декількома

напрямами.

По-перше, це розробка ймовірісно-статистичних методів розпізнавання, застосування елементів штучного інтелекту для отримання оцінок надійності стеганографічних перетворень і при створенні фільтрів (детекторів) для аналізу інформаційних потоків з метою виявлення стеганограм. У цьому випадку перевірка наявності прихованої інформації зводиться до певної оцінки з використанням статистичних критеріїв (послідовної кореляції, ентропії зображення, дисперсії молодшого біта й ін). Розроблювані з цією метою засоби повинні бути універсальними і забезпечувати необхідний рівень похибки під час розпізнавання прихованих повідомлень, особливо в тих випадках, коли використовується попереднє шифрування.

По-друге, це аналіз конкретних програмних стегозасобів із метою відновлення алгоритмів і оптимальної розробки методу їхнього аналізу.

Основна складність тут полягає у великій трудомісткості, яка обумовлена необхідністю індивідуального підходу до кожного конкретного алгоритму, що реалізує метод приховування інформації, а також об'ємом обчислень, необхідних для відновлення стегоключів.

По-третє, це розробка технології активних і зловмисних атак для внесення невідновлюваних перекручувань у передбачувану стеганограму з метою спровокувати її повторне передавання в іншому контейнері, що підтвердило б факт використання стегозасобів.

Висновки до розділу

Узагальнюючи, можемо зробити висновок, що реалізація будь-якого методу захисту від стеганографічних атак пов'язана з фізичною природою сигналу-повідомлення та сигналу-контейнера. Найчастіше, в якості

контейнера вибираються аудіо-сигнали і зображення. Для високоякісного відтворення аудіо-сигналів і зображень сучасна техніка використовує цифровий запис таких сигналів. В силу своєї аналогової природи, аудіо-сигнали та зображення містять надлишкову інформацію, яку легко замінити на певне повідомлення. При цьому бітовий склад стего відрізняється від бітового складу контейнера, і це не повинно виявлятися за допомогою людських органів чуття і надавати істотного впливу на роботу будь-якої інформаційної системи.

Основні недоліки використання більшості методів кодування полягають в тому, що вони вносять шум як в аудіо файл, так і в зображення, який може бути досить помітним.

Тому постає задача створення надійного алгоритму захисту системи, який би підвищив стійкість сигналу (зображення) на виході системи від спотворень, що спричинені стеганографічними атаками.

2 МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА

2.1 Модель деградації образу

Моделлю деградації (спотворення) образу (одновимірного чи двовимірного) є в загальному випадку нелінійні та анізотропні оператори [1,2,3]. Але в такому вигляді задача оброблення сигналу з метою придушення шумів та корекції спотворень аналітично може бути розв'язана не завжди, а у випадку її розв'язання математичний апарат і апаратурні витрати стають не сумірно великими у порівнянні з досягнутим результатом. Тому, як правило, систему прийому-передачі сигналу вважають **лінійною**, а **шум адитивним** (що на сучасному рівні апаратурного забезпечення і вимог для систем обробки є достатнім) [1,4].

В такому разі спотворений образ $L(x, y)$ можна описати рівнянням

$$L(x, y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} g(x, y, x', y') \cdot f(x', y') dx' dy' + V(x, y), \quad (2.1)$$

де $g(x, y, x', y')$ – результуюча імпульсна характеристика каналу прийому-передачі; $f(x', y')$ – сигнал, що його передають; $V(x, y)$ – адитивний шум, x, y — відповідні просторові координати.

Інтеграл (2.1) має загальний вигляд лінійної суперпозиції, але в ньому імпульсна характеристика залежить від координат x, y (тобто для різних координат буде різною). Це свідчить про те, що інтеграл (2.1) описує лінійну **анізопланарну** систему. Гіпотеза про лінійність на практиці часто теж не відповідає дійсності. Тому для використання моделі (2.1) систему слід попередньо лінеаризувати (наприклад експоненціальним або іншим перетворенням). Також і представлення шуму лише своєю адитивною складовою в багатьох випадках не відповідає дійсності, що викликає необхідність додаткових зусиль по створенню відповідних апаратурних

засобів.

У багатьох практично важливих випадках можна вважати (хоча б у наближенні), що імпульсна характеристика інваріантна відносно координат x, y (для процесів вона завжди інваріантна у часі), тобто $g = g(x - x', y - y')$, а модель деградації образу (одновимірною чи двовимірною) є **ізопланарною**. Тоді модель (2.1) перетворюється у двовимірний інтеграл згортки (інтеграл Дюамеля)

$$L(x, y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} g(x - x', y - y') \cdot f(x', y') dx' dy' + V(x, y), \quad (2.2)$$

У подальшому будемо використовувати, в основному, цю модель, або (у випадку одновимірних сигналів) одновимірний інтеграл [4,5]

$$L(t) = \int_{-\infty}^{\infty} g(t - \tau) \cdot f(\tau) d\tau + V(t). \quad (2.3)$$

Моделі деградації (спотворення) образу (2.2), (2.3) описують процес спотворення ідеального образу $f(x, y)$. Якщо імпульсна характеристика $g(x, y)$ або $g(t)$ не є δ -імпульсом Дірака, то навіть при відсутності адитивного шуму одержаний образ $L(x, y)$ суттєво відрізняється від вихідного сигналу $f(x, y)$. Тому основною задачею обробки є отримання оцінки $\hat{f}(x, y)$ сигналу $f(x, y)$, яка певним чином співпадає з цим сигналом. Міру співпадіння або неспівпадіння обирають за певним **об'єктивним математичним критерієм**, який **суб'єктивно вибирають** внаслідок наявності великої кількості таких критеріїв.

Задачу оброблення сигналів $L(x, y)$ з метою отримання оцінки $\hat{f}(x, y)$ звичайно називають задачею **реставрації** [6—9].

Така задача полягає у пошуку оцінки $\hat{f}(x, y)$ за наявності деякої апріорної (наперед відомої) інформації. У випадку моделі (2.2) задачу реставрації можна сформулювати наступним чином [1 — 9]:

за відомими (апріорі) $g(x, y)$, $L(x, y)$ та характеристиками шуму $V(x, y)$ знайти наближення $\hat{f}(x, y)$ до $f(x, y)$.

Що стосується імпульсної характеристики, то її часто можна виміряти або розрахувати детерміновано. Конкретна реалізація шуму зазвичай

невідома, тому для шуму часто обмежуються середньостатистичними характеристиками. Звичайний образ $L(x,y)$ можна розглядати і як детермінований, і як певну реалізацію випадкового поля.

Різні методи реставрації значно відрізняються [1,9,15] щодо рівня точності опису поодиноких членів моделі (2.2).

Слід особливо наголосити, що успіх процедури реставрації значною мірою залежить від наявності та точності апіорної інформації про причини спотворення (деградації) образу (імпульсна характеристика $g(x,y)$, інформація про шум $V(x,y)$, певні відомості про реставрований образ). Тому велике значення має ідентифікація відповідних характеристик системи деградації образу (системи відображення, яка не є ідеальною).

2.2 Ідентифікація імпульсної характеристики

Для моделі деградації (2.2) найважливішою характеристикою є імпульсна характеристика $g(x,y)$, яка і визначає втрату чіткості відображеного образу. Причини втрати чіткості можуть бути різноманітними і тому імпульсну характеристику не завжди можна виміряти. Тому ідеальним способом визначення імпульсної характеристики слід було б вважати її аналітичне виведення з моделі системи відображення.

Так, наприклад, втрату чіткості за рахунок дифракції оптичного образу впливом вхідного отвору діаметром D , що можна описати формулою

$$P(x,y) = \begin{cases} 1 & \text{— усередині кругового отвору} \\ 0 & \text{— поза отвором} \end{cases},$$

враховуємо імпульсною характеристикою

$$g(u,v) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} P(x,y) \cdot P(x-\lambda \cdot d \cdot u, y-\lambda \cdot d \cdot v) dx dy.$$

Тут λ — довжина хвилі світла (сигналу носія інформації); d — відстань між площиною образу і отвором.

В ряді випадків ізотропну втрату чіткості з розумною точністю можна апроксимувати Гауссовим законом

$$g(x,y) = k_1 \cdot \exp \{ -k_r \cdot r^2 \},$$

де r – відстань від центру кривої; k_1 і k_r – константи, які можна знайти при апроксимації вимірювань. Так само можна апроксимувати втрату чіткості за рахунок розфокусування або за рахунок турбулентності атмосфери, для чого слід використовувати вираз

$$g(x,y) = k_1 \cdot \exp \{ -(k_2 \cdot x^2 + k_3 \cdot y^2)^{5/6} \}.$$

Якщо поле образу ізотропне, то $k_2 = k_3$.

При реставрації образів, спотворених за рахунок паразитних рухів об'єкту відображення або системи зчитування образу (наприклад, в медичних застосуваннях – скіаграфія, класична РТГ томографія [1, 2]) можливим є отримання аналітичного виразу $g(x,y)$. Нехай рух описується посувом осі об'єкта відображення, в площині образу, причому кожна точка осі описує довільну траєкторію. Наприклад, координати початку осі (x_0, y_0) при русі змінювалися у відповідності до виразів

$$x_0 = a(t); \quad y_0 = b(t).$$

Тоді нечіткий («розмазаний») образ описується виразом

$$L(x,y) = \int_{-T/2}^{T/2} f(x-a(t), y-b(t)) dt,$$

де T — час експозиції.

При переході до частотної області можна показати, що в цьому випадку має місце спотворення, яке має характер конволюції (2.2), (2.3), тобто

$$L(u,v) = \int_{-\infty}^{\infty} \left[\int_{-\infty}^{\infty} (e^{-j(ux+vy)} \int_{-T/2}^{T/2} f(x-a(t), y-b(t)) dt) dy \right] dx.$$

Заміною послідовності інтегрування та введенням підстановки

$$x-a(t) = \xi; \quad y-b(t) = \eta$$

Отримаємо

$$L(u,v) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(\xi, \eta) \cdot e^{-j(u\xi+v\eta)} d\xi d\eta \cdot \int_{-T/2}^{T/2} e^{-j(ua(t)+vb(t))} dt == F(u,v) \cdot$$

$G(u,v),$

або

$$L(x,y) = f(x,y) * g(x,y).$$

В багатьох важливих випадках, на жаль, механізми втрати чіткості (еквівалентного розфокусування) настільки складні, що неможна отримати задовільні моделі, які б дали змогу аналітично описати імпульсну характеристику деградації $g(x,y)$. Тому немає іншого виходу, як спиратися на вимірювання, які у подальшому слід обробити та узагальнити.

В деяких випадках імпульсну характеристику можна отримати експериментально відображенням фантома (моделі), створеного «точковими» джерелами (такими «малими», що їх розмірами у порівнянні до графоелементів зображення можна знехтувати). Аналогічно зі спотвореного образу можна знайти (апостеріорі) імпульсну характеристику $g(x,y)$, якщо у неспотвореному образі були точкові джерела (наприклад, зірки в астрономічних фотографіях, «точкові цілі» в ультразвуковій томографії тощо). Але така ситуація є скоріш виняткова.

2.3 Ідентифікація шуму

Різноманітні методи реставрації суттєво відрізняються вимогами до інформації про шум. Таким чином, вибір того чи іншого методу реставрації суттєво залежить від доступної інформації про шум.

Шумову функцію $V(x,y)$ в конкретному образі $L(x,y)$ вважаємо реалізацією випадкового поля. Тому опис шуму є описом цього поля, оскільки для окремих реалізацій будь-яка статистична інформація відсутня.

Повним описом двовимірного випадкового поля є багатовимірна щільність імовірностей (розмірність відповідає кількості елементів в матриці образу). Цей опис є дуже громіздким, потребує значних зусиль для його отримання і внаслідок цього є непридатним для використання у практиці.

Тому обмежуються лише деякими параметрами цього розподілення, які можна на практиці визначити.

З точки зору ідентифікації шуму було б зручно отримати якнайбільшу кількість його реалізацій, незалежних від образу. Тоді виникає можливість обчислювати характеристики [3, 4] шуму **за ансамблем реалізацій**, зокрема такі середні значення, як математичне очікування

$$\mu(x,y) = M \{V(x,y)\}, \quad (2.4a)$$

дисперсія

$$\sigma_v^2(x,y) = M \{(V(x,y) - \mu(x,y))^2\} \quad (2.4б)$$

як функції координат (х,у) та автокореляційна функція

$$R_{vv}(x_1, y_1, x_2, y_2) = M \{V(x_1, y_1), V(x_2, y_2)\}, \quad (2.4в)$$

де $M\{\cdot\}$ — оператор математичного очікування.

На базі такого аналізу вже можна робити висновки про можливу однорідність (гомогенність) та ергодичність шумового поля. Оцінка середніх по ансамблю реалізацій, як відомо, є процедурою досить громіздкою. До того ж в багатьох випадках достатньо велика (репрезентативна) вибірка реалізацій не може бути отримана або відсутня. Особливо трудомісткою є обчислення автокореляційної функції шуму та взаємно кореляційної функції між шумом та образом за ансамблем.

Тому часто буває потрібно зробити деякі **апріорні припущення** (гіпотези) про характер шуму. Тестування вірності таких гіпотез є часто дуже громіздким і таке тестування звичайно служить підставою для висновків про довіру результатам реставрації. Базовим припущенням звичайно є припущення про **гомогенність** (однорідність) шуму, який в такому випадку можна характеризувати середнім значенням (математичним очікуванням) μ та розсіянням (дисперсією) σ^2 , значення яких не залежить від координат (х,у), та автокореляційною функцією $R_{vv}(\Delta x, \Delta y)$. Альтернативою до автокореляційної функції є **спектральна густина потужності шуму**

$$S_{vv} = F \{R_{vv}(\Delta x, \Delta y)\}. \quad (2.5)$$

З припущення про гомогенність шуму автоматично витікає припущення

про незалежність шуму та образу (що, насправді, не завжди виконується).

У випадку, коли в наявності є тільки одна реалізація шуму (один спотворений образ), не залишається нічого іншого, ніж припустити ще й **ергодичність** шумового поля [3, 4, 5]. Тобто можна припустити, що середнє за ансамблем, яке апроксимує μ, σ^2 та R_{vv} середніми значеннями по **просторовим координатам** в площині образу.

Часто взагалі не існує жодної реалізації саме шуму, що примушує аналізувати ділянки вже отриманого спотвореного образу, де (на думку дослідника) графоелементи образу відсутні, тобто шуму на фоні постійних за інтенсивністю ділянок образу. Ясно, що в таких випадках ідентифікувати шум можна тільки на базі гіпотези про його ергодичність.

З точки зору математичних обґрунтувань методів реставрації зручно (якщо це можливе) апроксимувати шум «білим шумом» (з постійним спектром) та іноді нормальним розподіленням його миттєвих випадкових значень. Багато з існуючих методів реставрації базуються саме на таких припущеннях. Але в кожному конкретному випадку слід оцінити, чи такі спрощуючі припущення не обмежують клас образів, які можна реставрувати.

2.4 Розв'язання задачі реставрації в натуральних координатах за відсутності шуму

Покажемо тепер, як за допомогою дискретизації сигналів можна знайти сигнал $\hat{f}(t)$ в моделі деградації (2.3). Для цього перепишемо інтеграл, підставивши замість t відлік $k\Delta t$ замість τ — $n\Delta t$. При цьому інтеграл замінено сумою, а диференціал dt — кроком Δt

$$L(k\Delta t) = \sum_{n=-\infty}^{\infty} g(k\Delta t - n\Delta t) \cdot f(n\Delta t) \cdot \Delta t. \quad (2.6)$$

Якщо «довжина» імпульсної характеристики становить $M\Delta t$, а шуканого сигналу $N\Delta t$, то після нормування кроку ($\Delta t = 1$) одержимо

$$L(k) = \sum_{i=0}^{M+N-1} g(k-n) \cdot f(n), \quad (2.7)$$

що й є загальною формою дискретної згортки.

В матричному записі (2.7) можна подати у вигляді

$$\bar{L} = \bar{\bar{G}} \cdot \bar{f}, \quad (2.8)$$

де $\bar{\bar{G}}$ – дискретний оператор згортки. Дві риски над $\bar{G}$ означають, що матриця $\bar{\bar{G}}$ квадратна, одна рисочка над $\bar{L}$ і $\bar{f}$, що це — стовпці,

$$\begin{aligned} \bar{L}^T = & \\ & \begin{bmatrix} L(0) & L(1) & L(2) & \dots & L(M+N-1) \end{bmatrix} \\ \bar{f}^T = & \\ & \begin{bmatrix} f(0) & f(1) & f(2) & \dots & 0 \end{bmatrix} \\ \bar{\bar{G}} = & \end{aligned} \quad (2.9)$$

$g(0)$	0	0	0	0	...	0	$g(2)$	$g(1)$
$g(1)$	$g(0)$	0	0	0	...	0	0	$g(2)$
$g(2)$	$g(1)$	$g(0)$	0	0	...	0	0	0
0	$g(2)$	$g(1)$	$g(0)$	0	...	0	0	0
0	0	$g(2)$	$g(1)$	$g(0)$	...	0	0	0
.....					...			
0	0	0	0	0	...	$g(2)$	$g(1)$	$g(0)$

де для визначеності обрано $M=3$.

Тоді, для дискретної апроксимації (2.8) моделі (2.3) сигнал $\bar{f}$ можна знайти за простою формулою

$$\bar{f} = \bar{\bar{G}}^{-1} \cdot \bar{L}, \quad (2.10)$$

для чого обернути матрицю дискретного оператора згортки $\bar{\bar{G}}$.

Розглянутий приклад демонструє великі можливості, які надає математичний апарат, пов'язаний з дискретизацією моделей.

Звичайно, розглянуту задачу реставрації сигналу можна було б розв'язати в аналітичному вигляді (при наявності аналітичної формули для $L(t)$, $g(t)$), використовуючи перетворення Фур'є.

За теоремою про згортку оригіналів

$$L(t) = g(t) * f(t) \leftrightarrow G(j\omega) \cdot F(j\omega) = L(j\omega), \quad (2.11)$$

де $L(j\omega)$, $G(j\omega)$ та $F(j\omega)$ перетворенні Фур'є для функцій $L(t)$, $g(t)$, $f(t)$ відповідно.

Тоді, для області спектрів Фур'є

$$F(j\omega) = L(j\omega) G(j\omega), \quad (2.12)$$

$$f(t) = F^{-1}\{F(j\omega)\}, \quad (2.13)$$

де $F^{-1}\{F(j\omega)\}$ — оператор зворотного перетворення Фур'є.

На жаль, обчислення зворотного перетворення Фур'є (навіть для простих аналітичних виразів) викликає значні складності. Тому інтеграл зворотного перетворення Фур'є слід було б розраховувати за наближеними формулами, що знову приводить до дискретизації.

Але, як видно з виразу (2.12), використання формул для обчислення спектру сигналу $f(t)$ значно простіші, ніж розв'язання тієї самої задачі в натуральних координатах. Тому часто доцільніше витратити певні зусилля для пошуку спектрів, розв'язувати задачу в області перетворення Фур'є і робити зворотне перетворення, аніж шукати розв'язок задачі в натуральних координатах.

Отже, великого значення набувають методи обчислення прямого та зворотного перетворення Фур'є.

2.5 Реставрація образів за методом умовної деконволюції

Умовна деконволюція образу – це метод реставрації, що базується на моделі (2.2), (2.8) в натуральних координатах, або на моделі (2.12) — (2.13) в області трансформант Фур'є. При цьому відомими вважають спотворений дискретний образ $\bar{L}$ або його дискретне перетворення Фур'є $\bar{L}_\omega$, дискретний оператор згортки в натуральних координатах (або відповідний до нього оператор у вигляді діагональної матриці, елементами діагоналі якої є

двовимірне перетворення Фур'є від двовимірної імпульсної характеристики системи, причому трансформанти розташовані в діагоналі рядок за рядком). Що стосується шуму $\bar{V}$, то (крім того, що він утворює поле ергодичне, стаціонарне, ізопланарне, гомогенне і адитивне) відома лише його енергія

$$\varepsilon^2 = [\bar{V}]^T \cdot [V]. \quad (2.14)$$

Оскільки логічний і фізичний сенс методу зрозумілий при розгляді моделі деградації в області натуральних координат, то метод з'явився історично саме для моделі деградації (2.2). Оскільки, як вже ясно з наведених вище особливостей моделі деградації в натуральних координатах, процедура реставрації досить громіздка і незручна, то слід перевести алгоритм умовної деконволюції в область трансформант Фур'є.

Тому у подальшому розглянемо обидва варіанти алгоритму умовної деконволюції — в натуральних координатах і в координатах трансформант Фур'є.

2.5.1 Умовна деконволюція в області натуральних координат

Згортка (конволюція) сигналу з імпульсною характеристикою системи з додаванням шуму призводить до спотворення первинного образу в системі відображення

$$\bar{L} = \bar{\bar{G}} \cdot \bar{f} + \bar{V}, \quad (2.15)$$

де $\bar{L}$ — стовпець відліків спотвореного (деградованого) образу; $\bar{\bar{G}}$ — матричний дискретний оператор згортки порядку M ; $\bar{f}$ — стовпець дискретних відліків вихідного образу; $\bar{V}$ — стовпець відліків випадкової реалізації адитивного шуму.

Реставрація (пошук первинного образу) є зворотною операцією відносно до конволюції. Тому таку операцію звичайно називають деконволюцією (за умови урахування впливу адитивного шуму — тому таку деконволюцію називають умовною).

Спочатку для простоти розглянемо особливості умовної деконволюції на прикладі реставрації одновимірного сигналу, модель деградації якого має

вигляд (2.3). Далі одержані результати узагальнимо на двовимірний випадок.

У випадку дискретного поля образу енергію шуму можна обчислити за формулою (2.14).

Оскільки шум ергодичний, а формат образу (порядок матриці $\bar{\bar{G}}$) $M \cong 10^3$, то маємо репрезентативну вибірку дискретів шуму (виміряних на тій частині поля образу, де досліджуваний образ $\bar{f}$ відсутній), а тому й сума квадратів цих дискретів є досить точною оцінкою енергії шуму (шумове поле однорідне — тому дисперсія в усіх його точках однакова).

Якщо, наприклад, середнє значення шуму $\mu\{v\} \equiv 0$, тоді

$$\varepsilon^2 = M \cdot \sigma^2, \quad (2.16)$$

тобто енергія шуму пропорційна дисперсії, що зручно, коли дисперсія σ^2 є апіорі відомою.

Ту саму енергію можна виразити з (2.15), якщо записати

$$\begin{aligned} \bar{V} &= \bar{L} - \bar{\bar{G}} \cdot \bar{f}; \\ \bar{V}^T &= (\bar{L} - \bar{\bar{G}} \cdot \bar{f})^T \end{aligned}$$

і згідно з (2.15)

$$\varepsilon^2 = (\bar{L} - \bar{\bar{G}} \cdot \bar{f})^T \cdot (\bar{L} - \bar{\bar{G}} \cdot \bar{f}) \quad (2.16a)$$

З іншого боку ясно, що внаслідок завжди обмеженої інформації про шум обчислення точного значення первинного образу $\bar{f}$ неможливе. Можливе обчислення лише оцінки $\hat{f}$ цього образу, яка (за наданими критеріями) буде наближатися до $\bar{f}$. Одним з таких критеріїв є те, що енергія шуму для оцінки $\hat{f}$ для первинного образу буде однаковою, тобто

$$\varepsilon^2 = (\bar{L} - \bar{\bar{G}} \cdot \hat{f})^T \cdot (\bar{L} - \bar{\bar{G}} \cdot \hat{f}) \quad (2.16б)$$

В формулі (2.16б) відомі ε^2 , $\bar{L}$, $\bar{\bar{G}}$. Але це рівняння відносно шуканої оцінки $\hat{f}$ є нелінійним. Для пояснення цього розглянемо приклад, коли порядок матриці $\bar{\bar{G}}$ дорівнює 3, вектори-стовпці $\bar{L}$ і $\hat{f}$ мають розміри 3×1

$$\begin{aligned}
\varepsilon^2 &= \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \times \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \times \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) = \\
&= \begin{bmatrix} (L_0 - g_{00} \times f_0 - g_{01} \times f_1 - g_{02} \times f_2) \\ (L_1 - g_{10} \times f_0 - g_{11} \times f_1 - g_{12} \times f_2) \\ (L_2 - g_{20} \times f_0 - g_{21} \times f_1 - g_{22} \times f_2) \end{bmatrix}^T \cdot \begin{bmatrix} (L_0 - g_{00} \times f_0 - g_{01} \times f_1 - g_{02} \times f_2) \\ (L_1 - g_{10} \times f_0 - g_{11} \times f_1 - g_{12} \times f_2) \\ (L_2 - g_{20} \times f_0 - g_{21} \times f_1 - g_{22} \times f_2) \end{bmatrix} = \\
&= (L_0 - g_{00} \cdot f_0 - g_{01} \cdot f_1 - g_{02} \cdot f_2)^2 + (L_1 - g_{10} \cdot f_0 - g_{11} \cdot f_1 - g_{12} \cdot f_2)^2 + \\
&\quad + (L_2 - g_{20} \cdot f_0 - g_{21} \cdot f_1 - g_{22} \cdot f_2)^2,
\end{aligned} \tag{2.168}$$

звідки одержимо

$$\begin{aligned}
&(L_0^2 + L_1^2 + L_2^2) - 2(g_{00} \cdot L_0 + g_{10} \cdot L_1 + g_{20} \cdot L_2) \cdot f_0 - \\
&\quad - 2(g_{01} \cdot L_0 + g_{11} \cdot L_1 + g_{21} \cdot L_2) \cdot f_1 - \\
&\quad - 2(g_{02} \cdot L_0 + g_{12} \cdot L_1 + g_{22} \cdot L_2) \cdot f_2 + (g_{00}^2 + g_{10}^2 + g_{20}^2) \cdot f_0^2 + \\
&\quad + 2(g_{00} \cdot g_{01} + g_{10} \cdot g_{11} + g_{20} \cdot g_{21}) \cdot f_0 \cdot f_1 + \\
&\quad + 2(g_{00} \cdot g_{02} + g_{10} \cdot g_{12} + g_{20} \cdot g_{22}) \cdot f_0 \cdot f_2 + \\
&\quad + (g_{01}^2 + g_{11}^2 + g_{21}^2) \cdot f_1^2 + 2(g_{01} \cdot g_{02} + g_{11} \cdot g_{12} + g_{21} \cdot g_{22}) \cdot f_1 \cdot f_2 + \\
&\quad + (g_{02}^2 + g_{12}^2 + g_{22}^2) \cdot f_2^2 - \varepsilon^2 = 0.
\end{aligned} \tag{2.17}$$

Саме для цього виразу, **нелінійного** відносно шуканих векторів $\hat{f} = [f_0 \ f_1 \ f_2]^T$, кількість розв'язків може бути нескінченно великою. Таким чином, слід ввести ще одну (оскільки порядок нелінійності дорівнює двом) додаткову умову, яка б виділила з множини розв'язків $\hat{f}$ лише його єдине значення. Ця друга умова повинна бути простою, щоб не підвищити ступеня нелінійності і обирати з множини образів такий, який відповідає деяким фізичним властивостям, притаманним образам досліджуваних об'єктів. Таким критерієм є критерій "гладкості" одержаного (як і первинного) образу.

Функцію "гладкості" ψ від шуканої оцінки $\hat{f}$ первинного образу надають у вигляді

$$\psi(\hat{f}) = \sum_{i=1}^{M-2} (f_{i-1} - 2f_i + f_{i+1})^2 = \min. \tag{2.18}$$

Так, наприклад, якщо значення знайденої оцінки лежать на одній прямій лінії (рис.1.1,а), то $f_{i-1} - 2f_i + f_{i+1} \equiv 0$. Якщо ж між двома значеннями f_{i-1}, f_{i+1} є велике відхилення значення f_i (рис.2.1,б,в), тоді величина $f_{i-1} - 2f_i + f_{i+1}$ зростає дуже різко і така ситуація не відповідає критерію (2.14), тобто не може з'явитися в реставрованому образі $\hat{f}$.

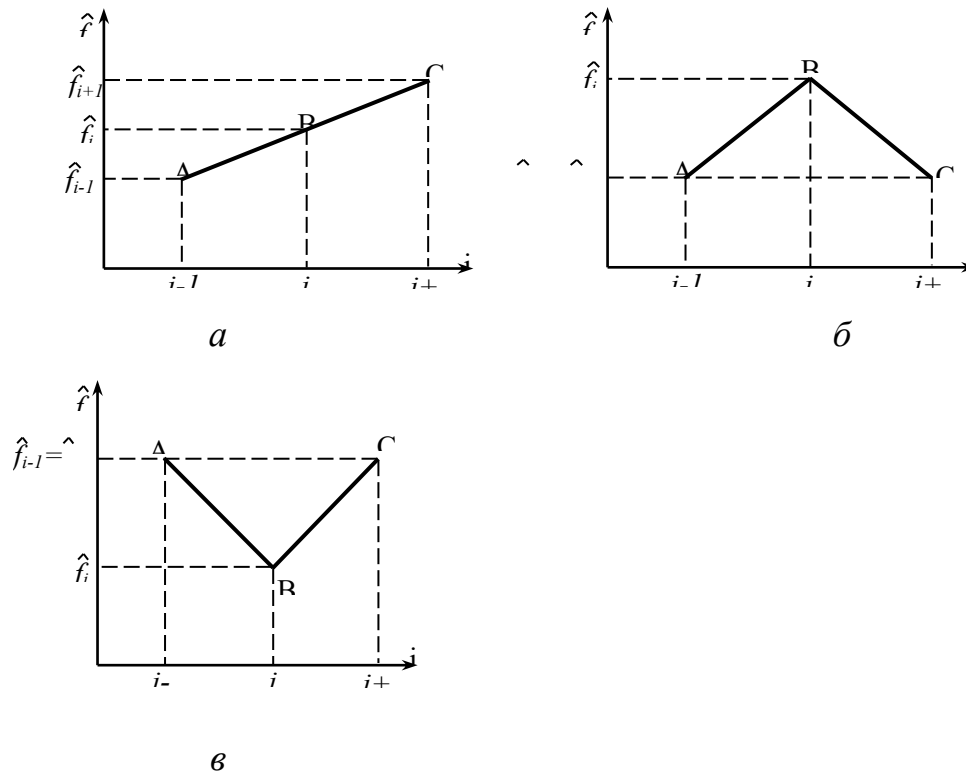


Рис.2.1 Визначення оцінки первинного образу

Критерій (2.18) є найпростішим з можливих, оскільки він враховує мінімальну можливу кількість послідовних точок дискретної оцінки. Кількість точок можна збільшити (тобто у виразі типу (2.18) враховувати чотири, п'ять і т. ін. точок), але в наш час такі більш складні критерії "гладкості" не використовують у практиці. Якщо кожен з виразів в дужках формули (2.18) вважати елементом стовпця $\bar{\varphi}$, то вираз можна записати у матричному вигляді

$$\Psi(\hat{f}) = \bar{\varphi}^T \cdot \bar{\varphi}.$$

Стовпець $\bar{\varphi}$ може бути одержаний із стовпця $\hat{f}$ множенням його на дискретний оператор $\bar{c}$, аналогічний $\bar{G}$ в (2.9). Тобто

$$\bar{\varphi} = \bar{c} \cdot \hat{f}, \quad (2.19)$$

де дискретний оператор $\bar{c}$ одержано з імпульсної характеристики "гладкості" $g = [1 \ -2 \ 1]$, тобто

$$\bar{\bar{c}} = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots \\ -2 & 1 & 0 & 0 & \dots & \dots & \dots & \dots \\ 1 & -2 & 1 & 0 & \dots & \dots & \dots & \dots \\ 0 & 1 & -2 & 1 & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & 1 & -2 & 1 \\ \dots & \dots & \dots & \dots & \dots & 0 & 1 & -2 \\ \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 \end{bmatrix}. \quad (2.20)$$

Тоді вираз (2.17) можна записати у вигляді

$$\Psi(\hat{f}) = (\bar{\bar{c}} \cdot \hat{f})^T \cdot (\bar{\bar{c}} \cdot \hat{f}). \quad (2.21)$$

Загальна система рівнянь, розв'язок якої становитиме шукану (лише єдину, чітко визначену двома умовами) оцінку первинного образу, має, таким чином, вигляд (2.21), (2.16a)

$$(\bar{L} - \bar{G} \cdot \hat{f})^T \times (\bar{L} - \bar{G} \cdot \hat{f}) - \varepsilon^2 = \min = 0; \quad (2.22)$$

$$(\bar{c} \times \hat{f})^T \cdot (\bar{c} \times \hat{f}) = \min.$$

Зауважимо, що обидві системи рівнянь мають розмірність і сенс оцінки шуму. Так, перша система рівнянь має сенс енергії адитивного шуму реставрованого образу, яка після реставрації повинна залишитись хоча б не більшою, ніж у спотвореному образі. Друга система рівнянь має сенс шуму "не гладкості" реставрованого образу. Таким чином, розв'язання системи нелінійних рівнянь — це пошук мінімуму позитивної функції (енергії). Оскільки таких мінімумів може бути багато, то задача зводиться до знаходження або глобального мінімуму, або мінімуму задовільного (такого, що задовольняє вимогам для якісної "гладкої" оцінки $\hat{f}$, в якій енергія шуму не перевищує первинну енергію шуму образу $\bar{V}$).

Для розв'язання задачі треба обидві системи рівнянь в (2.22) об'єднати в єдину (оскільки сума мінімумів двох позитивних функцій не є мінімумом сумарної функції). Для об'єднання скористаємося методом Лагранжа невизначених коефіцієнтів λ (позитивних), тобто будемо шукати мінімум

єдиної системи рівнянь, взявши кожне з них в (2.22) з деякою вагою. Для цього зважимо коефіцієнтом λ першу систему в (2.22) і знайдемо суму першої та другої системи. Одержимо

$$\beta = \lambda \cdot \left[(\bar{L} - \bar{G} \times \hat{f})^T \cdot (\bar{L} - \bar{G} \times \hat{f}) - \varepsilon^2 \right] + (\bar{c} \cdot \hat{f})^T \cdot (\bar{c} \cdot \hat{f}) = \min. \quad (2.23)$$

В мінімумі (екстремумі) функції в (1.23) похідна від неї за координатами f_i (дискретами шуканої оцінки $\hat{f}$) повинна дорівнювати нулю (для усіх часткових похідних $\partial\beta/\partial f_i$).

Таким чином треба обчислити всі похідні від виразу (2.23) для кожного дискрета f_i ($i = 0, 1, \dots, M-1$). Для пояснення правила обчислення похідних від складного матричного виразу (2.23) розглянемо вираз (2.16в). Тоді

$$\beta = \quad (2.24a)$$

$$\lambda \left\{ \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) - \varepsilon^2 \right\} +$$

$$+ \left(\begin{bmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \times \left(\begin{bmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right).$$

Похідна має вигляд

$$\partial\beta/\partial f_0 = \quad (2.24б)$$

$$\lambda \times \left\{ \left(- \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) + \right.$$

$$+ \left. \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(- \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right) \right\} +$$

$$+ \left(\begin{bmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) +$$

$$+ \left(\begin{bmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \times \left(\begin{bmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right).$$

Розглянемо перший вираз в дужках в (2.24б). Оскільки вважаємо всі значення пікселів f_i незалежними від f_0 , то всі похідні $\partial f_i / \partial f_0$, $i \neq$

0 дорівнюють нулю, а $\partial f_0/\partial f_0 = 1$. Якщо диференціювати $\partial\beta/\partial f_1$, то, аналогічно, в перших дужках усі елементи стовпця $\partial\hat{f}/\partial f_1=0$ крім, $\partial f_1/\partial f_1$ що знаходиться у другому рядку. Тоді

$$\begin{aligned} \partial\beta/\partial f_0 &= \lambda \times \left(- \begin{bmatrix} g_{00} \\ g_{10} \\ g_{20} \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) + \\ &+ \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(- \begin{bmatrix} g_{00} \\ g_{10} \\ g_{20} \end{bmatrix} \right) + \left(\begin{bmatrix} c_{00} \\ c_{10} \\ c_{20} \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} c_{00} & c_{01} & c_{02} \\ c_{10} & c_{11} & c_{12} \\ c_{20} & c_{21} & c_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) + \\ &\left(\begin{bmatrix} c_{00} & c_{01} & c_{02} \\ c_{10} & c_{11} & c_{12} \\ c_{20} & c_{21} & c_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} c_{00} \\ c_{10} \\ c_{20} \end{bmatrix} \right); \\ \partial\beta/\partial f_1 &= \lambda \cdot \left(- \begin{bmatrix} g_{01} \\ g_{11} \\ g_{21} \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) + \\ &+ \left(\begin{bmatrix} L_0 \\ L_1 \\ L_2 \end{bmatrix} - \begin{bmatrix} g_{00} & g_{01} & g_{02} \\ g_{10} & g_{11} & g_{12} \\ g_{20} & g_{21} & g_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(- \begin{bmatrix} g_{01} \\ g_{11} \\ g_{21} \end{bmatrix} \right) + \left(\begin{bmatrix} c_{01} \\ c_{11} \\ c_{21} \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} c_{00} & c_{01} & c_{02} \\ c_{10} & c_{11} & c_{12} \\ c_{20} & c_{21} & c_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right) + \\ &+ \left(\begin{bmatrix} c_{00} & c_{01} & c_{02} \\ c_{10} & c_{11} & c_{12} \\ c_{20} & c_{21} & c_{22} \end{bmatrix} \cdot \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} \right)^T \cdot \left(\begin{bmatrix} c_{01} \\ c_{11} \\ c_{21} \end{bmatrix} \right). \end{aligned}$$

Аналогічно для $\partial\beta/\partial f_2$.

Проводячи елементарні матричні операції групування складових при однакових множниках, одержимо

$$\begin{bmatrix} \partial\beta/f_0 \\ \partial\beta/f_1 \\ \partial\beta/f_2 \end{bmatrix} = \lambda \cdot \left\{ (-\bar{G}^T) \cdot (\bar{L} - \bar{G} \cdot \hat{f}) + (\bar{L} - \bar{G} \cdot \hat{f})^T \cdot (-\bar{G}) \right\} + 2\bar{c}^T \cdot \bar{c} \cdot \hat{f},$$

звідки, враховуючи, що $(-\bar{G}^T) \cdot (\bar{L} - \bar{G} \cdot \hat{f}) = (\bar{L} - \bar{G} \cdot \hat{f})^T \cdot (-\bar{G})$, одержимо

$$\begin{bmatrix} \partial\beta/f_0 \\ \dots \dots \dots \\ \partial\beta/f_{M-1} \end{bmatrix} = 2\{\bar{G}^T \cdot \bar{G} \cdot \hat{f} - \bar{G}^T \cdot \bar{L}\} \cdot \lambda + 2\bar{c}^T \cdot \bar{c} \cdot \hat{f}$$

або, враховуючи, що в точці екстремуму похідні дорівнюють нулю,

$$\{\bar{G}^T \cdot \bar{G} \cdot \hat{f} - \bar{G}^T \cdot \bar{L}\} \cdot \lambda + \bar{c}^T \cdot \bar{c} \cdot \hat{f} = 0. \quad (2.25)$$

Таким чином, нелінійна задача (2.23) з нелінійностями другого порядку (квадратична форма) за рахунок диференціювання зведена до лінійної (до

системи лінійних рівнянь M -го порядку (2.25) відносно шуканого стовпця λ , але з невизначеним (невідомим) коефіцієнтом λ .

Розв'язок цієї системи рівнянь має вигляд

$$\hat{f} = \left[\bar{\bar{G}}^T \cdot \bar{\bar{G}} + \frac{1}{\lambda} \cdot \bar{\bar{c}}^T \cdot \bar{\bar{c}} \right]^{-1} \cdot \bar{\bar{G}}^T \cdot \bar{L}. \quad (2.26)$$

Для розв'язання рівняння (2.26) слід задати заздалегідь деяке значення λ (оптимальна величина якого не відома). Тому задачу умовної деконволюції слід розв'язувати за ітеративною процедурою:

- 1) обчислити (сформувані) матриці $\bar{\bar{G}}$, $\bar{\bar{c}}$, $\bar{L}$, виразу (2.26) (нагадаємо, що для одновимірного деградованого сигналу $\bar{L}$ з $M = 1024$ дискретами розміри матриць $\bar{\bar{G}}$, $\bar{\bar{c}}$ становлять $M \times M = 1024 \times 1024$);
- 2) призначити початкове значення константи λ ;
- 3) обчислити $\hat{f}$ за (2.26) (для цього слід обернути матрицю в квадратних дужках розміру 1024×1024);
- 4) обчислити енергію шуму $\hat{\varepsilon}^2$ за формулою (2.16);
- 5) перевірити, чи обчислене значення $\hat{\varepsilon}^2$ є задовільним (тобто $\hat{\varepsilon}^2 \leq \varepsilon^2$, де ε^2 — енергія адитивного шуму спотвореного образу), чи ні. Якщо $\hat{\varepsilon}^2$ задовільне, то обчислення закінчити; якщо ні — то перейти до пункту (6) алгоритму;
- 6) змінити значення λ (якщо $\hat{\varepsilon}^2 \geq \varepsilon^2$, то збільшити λ , якщо $\hat{\varepsilon}^2 < \varepsilon^2$, то λ слід зменшити) і перейти до пункту (3) алгоритму.

З формули (2.26) і опису ітераційної процедури ясно, що метод умовної деконволюції навіть у випадку реставрації одновимірних образів великого формату ($M = 512, 1024, 2048$) є надзвичайно складним і потребує великих об'ємів пам'яті та громіздких обчислень, які до того ж призводять до накопичення великих операційних похибок. Тому в сучасній медичній та технічній практиці метод у такому вигляді не реалізують.

У випадку реставрації двовимірних образів ситуація катастрофічно погіршується.

Всі формули та ітераційний алгоритм залишаються тими самими, що й

для одновимірного випадку. Винятком лише є умова "гладкості", яка у двовимірному варіанті описується імпульсною характеристикою

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

(на відміну від $[1, -2, 1]$ у випадку одновимірному). Але розміри матриць катастрофічно зростають. Так, для образу розміром 1024×1024 скануванням за рядками утворюють стовпець $\bar{L}$ деградованого образу, але вже розміру $(1024)^2 \times 1$. Матриця $\bar{G}$ має розміри $(1024)^2 \times (1024)^2$. Такий самий розмір $(10^6 \times 10^6)$ має матриця у квадратних дужках в формулі (2.26). Для її обернення потрібно близько $N = (10^6)^3 = 10^{18}$ операцій.

Але сформульований в натуральних координатах метод умовної деконволюції знайшов широке поширення при переході до області трансформант Фур'є. У цьому випадку реставрація образу розміру 1024×1024 становить хоча й досить складну, але успішно (і досить швидко) розв'язувану задачу.

2.5.2. Умовна деконволюція в області трансформант Фур'є

На базі теореми про згортку дискретного оригіналу можна для дискретного перетворення Фур'є—образу (того ж формату $M \times M$, що й оригінал) записати формули деградації і одержати формулювання методу умовної деконволюції [15].

Так, модель (2.8) деградації (для двовимірного випадку) в області трансформант перетворення Фур'є можна записати у наступному вигляді

$$L(m, n) = M^2 \cdot G(m, n) \cdot F(m, n) + V(m, n), \quad (2.27)$$

де всі операнди одержані з оригіналів в натуральних координатах за допомогою ДПФ. Тоді умова (2.18б) в спектральній області має вигляд

$$M^2 \cdot \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} |L(m, n) - M^2 \cdot \hat{F}(m, n) \cdot G(m, n)|^2 = \varepsilon^2. \quad (2.28)$$

Умова "гладкості" (у двовимірному випадку) має вигляд

$$M^2 \cdot \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} |\hat{F}(m, n) \cdot C(m, n)|^2 = \min, \quad (2.29)$$

де $C(m, n)$ — перетворення Фур'є від двовимірної функції "гладкості"

$$[c] = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad (2.29a)$$

в форматі $M \times M$ (тобто, оскільки $M \gg 3$, матрицю $[c]$ доповнюють нулями для одержання формату $M \times M$).

Вираз типу (2.25) має простий і компактний вигляд

$$M^2 \cdot \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \{ \lambda \cdot (|L(m, n) - M^2 \cdot \hat{F}(m, n) \cdot G(m, n)|^2 - \varepsilon^2) + |C(m, n) \cdot \hat{F}(m, n)|^2 \} = \min. \quad (2.30)$$

Такий простий вигляд основної формули, за якою знаходять $\hat{F}(m, n)$ є наслідком діагоналізації матриці дискретної згортки при переході до області трансформант Фур'є (згідно теореми про конволюцію оригіналів).

Диференціювання кожного з доданків суми (2.30) за $\hat{F}(m, n)$

також виконати значно легше, ніж у матричному випадку в натуральних координатах. Оскільки

$$|L(m, n) - M^2 \cdot \hat{F}(m, n) \cdot G(m, n)|^2 = [L(m, n) - M^2 \cdot \hat{F}(m, n) \cdot G(m, n)]^* \cdot [L(m, n) - M^2 \cdot \hat{F}(m, n) \cdot G(m, n)],$$

де $*$ — означає комплексне спряження, то внаслідок диференціювання (2.30) одержимо розв'язок для кожного елемента (аналогічно до (2.26) у вигляді

$$\begin{aligned} \hat{F}(m, n) &= \frac{1}{M^2} \cdot (G^*(m, n) \cdot L(m, n)) / \left(\frac{1}{\lambda} \cdot |C(m, n)|^2 + |G(m, n)|^2 \right) = \\ &= \frac{1}{G(m, n)} \cdot \frac{|G(m, n)|^2}{M^2 \cdot (|C(m, n)|^2 + \frac{1}{\lambda} |G(m, n)|^2)} \times L(m, n). \end{aligned} \quad (2.31)$$

Формула (2.31) описує коефіцієнт передачі фільтра, який реалізує умовну деконволюцію з підстроюваним параметром λ

$$K_{DF}(m,n) = \frac{1}{G(m,n)} \cdot \frac{|G(m,n)|^2}{M^2 \cdot (|C(m,n)|^2 + \frac{1}{\lambda} |G(m,n)|^2)} \quad (2.32)$$

і дуже (за формою) нагадує Вінерівський фільтр

$$K_W(m, n) = \frac{1}{G(m,n)} \cdot \frac{|G(m,n)|^2}{|G(m,n)|^2 + \frac{W_{vv}(m,n)}{W_{ff}(m,n)}},$$

де W_{vv} — спектр потужності шуму (перетворення Фур'є від кореляційної функції); W_{ff} — спектр потужності сигналів певного класу, на які фільтр налаштовано (перетворення Фур'є від кореляційної функції сигналів цього класу). Але замість корегуючого доданка у знаменнику

$$W_{vv}(m,n)/W_{ff}(m,n)$$

він має інший корегуючий доданок $1/\lambda \cdot |C(m,n)|^2$, який відображає умову "гладкості" з вагою $1/\lambda$.

Підставленням (2.32) до (2.31) можна одержати результуючу формулу (для урахування значення λ в розв'язку)

$$M^2 \cdot \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \frac{\frac{1}{\lambda^2} |L(m,n)|^2 \cdot |C(m,n)|^4}{\left[\frac{1}{\lambda} |C(m,n)|^2 + |G(m,n)|^2 \right]^2} = \varepsilon^2. \quad (2.33)$$

Таким чином, на відміну від реставрації в натуральних координатах, ітераційно знаходять лише λ для рівняння (2.33). Тобто ітераційне обчислення за (2.33) (підстройку деконволюційного фільтра) можна виконати за наступним алгоритмом:

1) обчислити спектри (за допомогою ДПФ) деградованого образу $L(m,n)$, коефіцієнта передачі деградуючої системи $G(m,n)$ і згладжуючого фільтра $C(m,n)$;

2) сформулювати фільтр (2.33) з невідомим коефіцієнтом λ ;

3) надати λ значення і обчислити за (2.33) значення ε^2 ;

4) якщо ε^2 задовільне, зупинити підстройку; якщо ж ні — змінити λ ;

5) перейти до пункту (3) алгоритму.

Оскільки рівність нулю похідних означає екстремум, то треба

визначити, чи знайдене значення є мінімумом чи максимумом. Тому треба враховувати другі похідні від виразу (2.30) (за $\hat{F}(m, n)$). З аналізу виразу для других похідних виходить вимога

$$\lambda > \min \frac{|C(m, n)|^2}{|G(m, n)|^2} = \lambda_{min} \quad (2.34)$$

Виконання умови (2.34) перед закінченням циклу обчислень слід перевірити. Якщо вона не виконується, треба змінити початкове значення λ .

На завершення розгляду деконволюційного фільтра слід зазначити, що, хоча він (2.32) нагадує Вінерівський фільтр, між цими фільтрами існує принципова різниця. Вінерівський фільтр підстроєний під клас сигналів з наданим спектром потужності і шумом з теж відомим спектром потужності. При фільтрації сигналу і шуму даного класу такий фільтр підстроювати не потрібно. Навпаки, деконволюційний фільтр має додатковий підстроюваний параметр λ , обчислення якого за формулою (2.33) потребує урахування даного конкретного деградованого образу $L(m, n)$. Тобто для кожного нового образу підстроювання параметра λ з урахуванням $L(m, n)$ слід проводити знову. Але початкова (апріорна) інформація для використання методу умовної деконволюції є значно меншою (відома тільки енергія шуму). До того ж відсутня вимога, щоб усі образи і реалізації шуму відносились до гомогенних і некорельованих полів. Нема потреби обчислювати усереднені спектри потужності образу і шуму.

Обраний в розглянутому алгоритмі критерій оптимальності — "гладкість" функції — у вигляді Лапласіана є одним з багатьох можливих, що відкриває можливості варіації алгоритмів умовної деконволюції при їх подальшому поширенні у практиці. Ще й досі існує некоректна думка про відносну трудомісткість перетворення Фур'є, що є базою до переходу в область трансформант. Але це додаткове ускладнення настільки мале у порівнянні до трудомісткості деконволюції в натуральних координатах, а реалізація ДПФ настільки прискорює і полегшує обчислення, що саме перетворення Фур'є навпаки радикально (на декілька порядків) спрощує

процедуру реставрації.

Як приклад, на рис. 2.2 при наданій імпульсній характеристиці деградуючої системи $g(x,y)$, дисперсії адитивного білого шуму σ^2 наведено вихідний (рис.2.2,*а*), деградований (рис.2.2,*б*) і реставрований (рис.2.2,*в*) образи (на рис. 2.2,*г* наведено результати фільтрації за методом зворотної корекції).

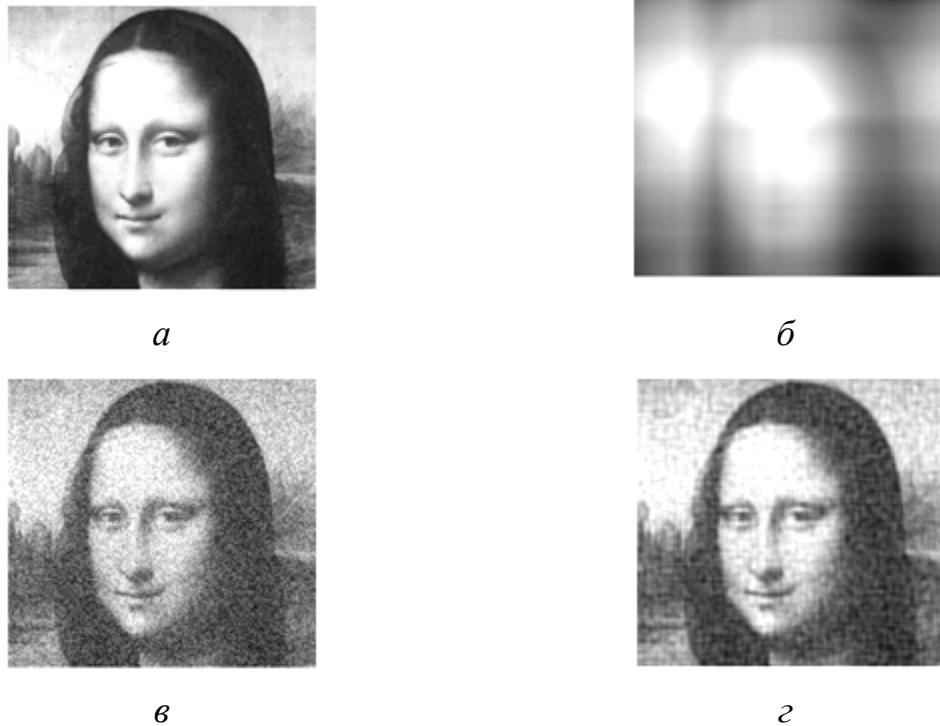


Рис.2.2 Приклад реставрації образу

2.6 Дискретна фільтрація за методом найменших квадратів

Методи реставрації, що були розглянуті вище, базуються на моделі деградації (2.2), (2.15) для **гомогенного** (однорідного) поля образу. В багатьох випадках обробки зображень негомогенністю поля образу знехтувати не можна. Тоді слід використовувати модель (1.1), для якої **теорема про конволюцію оригіналу відсутня**. Тому перехід у частотну область Фур'є (конволюція оригіналів не дорівнює добутку їх спектрів) при такій постановці

задачі недоцільний.

У даному розділі розглянемо саме узагальнення Вінерівської фільтрації на випадок обробки образу і шуму в негомогенному полі. Аналогічно можна побудувати алгоритм умовної деконволюції і алгоритм деконволюції по критерію оптимальної імпульсної характеристики за умови негомогенності полів образу і шуму.

Ця умова значно ускладнює задачу, але й робить її значно загальнішою. Друга умова (відсутність теореми про конволюцію оригіналів) значно розширює інструментарій дослідника, оскільки, якщо за нею перехід у частотну область Фур'є не є єдиним можливим способом спрощення алгоритму, то можна використовувати перетворення з дійсним ядром (Адамара, Хаара і т.ін. [6]).

Для простоти ілюстрації особливостей методу у подальшому будемо розглядати випадок фільтрації одновимірного образу. Для двовимірного образу (скануванням) можна перейти до одновимірного вектора і (враховуючи нюанси такого сканування) одержати той самий алгоритм.

Тобто модель деградації знову має вигляд (2.15)

$$\bar{L} = \bar{\bar{G}} \cdot \bar{f} + \bar{V}. \quad (2.35)$$

Оскільки у подальшому будемо розглядати дискретні ортогональні перетворення — вектор $\bar{f}$ періодичний, періодичною є кожна реалізація імпульсної характеристики (різної для різних координат дії у вигляді δ -імпульсу). Як і у випадку перетворення Фур'є (використання якого у даному разі можливе, але недоцільне) алгоритм будь-якого ортогонального перетворення має наступний вигляд.

1. Пряме (дискретне) перетворення деградованого образу

$$\bar{L}_A = \bar{\bar{A}} \cdot \bar{f}, \quad (2.36)$$

де $\bar{\bar{A}}$ — матриця перетворень (Адамара, Хаара, Фур'є, косинусного, похилого, тощо). Матриця перетворень $\bar{\bar{A}}$ звичайно є унітарною.

2. Корекція у "частотній" області (яку й треба знайти)

$$\bar{L}'_A = \bar{\bar{M}} \cdot \bar{L}_A, \quad (2.37)$$

тобто матриця $\bar{\bar{M}}$ є матрицею корегуючого фільтра в області трансформант глобального ортогонального перетворення. Якщо, наприклад, поле образу гомогенне (і має сенс використовувати теорему про згортку оригіналів в перетворенні Фур'є), тоді матриця $\bar{\bar{M}}$ є діагональною матрицею дискретів частотної характеристики корегуючого фільтра і у подальшому (за критерієм найменших квадратів), вводячи додаткові обмеження, можна одержати фільтр Вінера.

Для негомогенного поля (для усіх перетворень, для яких відсутня теорема про згортку оригіналів) матриця $\bar{\bar{M}}$ не є діагональною. Фізична інтерпретація такої узагальненої матриці $\bar{\bar{M}}$ незвична: результуюча складова $\bar{L}'_A$ ("частотна" складова) після фільтрації є функцією не лише відповідної (за номером) нефільтрованої складової $\bar{L}'_A$, але багатьох або усіх складових. Вибором матриці $\bar{\bar{M}}$ обирають конкретний реставруючий фільтр.

3. Зворотне перетворення

$$\hat{f} = \bar{A}^{-1} \cdot \bar{L}'_A = \bar{A}^{-1} \cdot [\bar{\bar{M}} \cdot (\bar{A} \cdot \bar{L})]. \quad (2.38)$$

Для визначення матриці $\bar{\bar{M}}$ слід ввести (як і в попередніх методах) додаткову умову. Нехай критерієм оптимальності фільтрації є вимога мінімуму суми квадратів відхилень лінійної оцінки шуканого вектора $\hat{f}$ на базі вимірюного вектора $\bar{L}$. **За принципом ортогональності** цей критерій можна ввести у вигляді математичного очікування

$$\mu\{(\bar{f} - \hat{f}) \cdot \bar{L}^T\} = \bar{0}, \quad (2.39)$$

де $\bar{0}$ — квадратна матриця нулів.

Тоді підставленням (1.38) до (1.39), одержимо

$$\mu\{(\bar{f} - \bar{A}^{-1} \cdot \bar{\bar{M}} \cdot \bar{A} \cdot \bar{L}) \cdot \bar{L}^T\} = \bar{0} \quad (2.40)$$

Після підстановки (1.40) до (1.35) одержимо

$$\mu\left\{\left(\bar{f} - \bar{A}^{-1} \cdot \bar{\bar{M}} \cdot \bar{A} \cdot (\bar{G} \cdot \bar{f} + \bar{V})\right) \cdot (\bar{G} \cdot \bar{f} + \bar{V})^T\right\} = \bar{0} \quad (2.41)$$

Оскільки $\bar{A}$, $\bar{G}$, $\bar{\bar{M}}$ є матрицями констант, їх можна виносити за знак

математичного очікування. Шум $\bar{V}$ та сигнал $\bar{f}$ вважаємо **не корельованими**.

Позначимо математичні очікування

$$\mu\{\bar{f} \cdot \bar{f}^T\} = \bar{R}_{ff}; \quad (2.42a)$$

$$\mu\{\bar{V} \cdot \bar{V}^T\} = \bar{R}_{vv}, \quad (2.42b)$$

де $\bar{R}_{ff}, \bar{R}_{vv}$ — кореляційні матриці сигналу $\bar{f}$ і шуму $\bar{V}$ відповідно.

Тоді з (2.38) можна одержати

$$\bar{M} = \bar{A} \cdot \bar{R}_{ff} \cdot \bar{G}^T \cdot (\bar{G} \cdot \bar{R}_{ff} \cdot \bar{G}^T + \bar{R}_{vv})^{-1} \cdot \bar{A}^{-1}. \quad (2.43a)$$

Після множень на одиничні матриці

$$\bar{E} = \bar{A} \cdot \bar{A}^{-1} \text{ або } \bar{E} = \bar{A}^{-1} \cdot \bar{A}$$

одержимо

$$\begin{aligned} \bar{M} = & \bar{A} \cdot \bar{R}_{ff} \cdot \bar{A}^{-1} \cdot \bar{A} \cdot \bar{G}^T \cdot \bar{A}^{-1} \cdot \bar{A} \cdot (\bar{G} \cdot \bar{A}^{-1} \cdot \bar{A} \cdot \bar{R}_{ff} \cdot \bar{A}^{-1} \cdot \bar{A} \cdot \bar{G}^T + \bar{R}_{vv})^{-1} \cdot \\ & \cdot \bar{A}^{-1} \cdot (\bar{A} \bar{R}_{ff} \bar{A}^{-1}) \cdot (\bar{A} \bar{G}^T \bar{A}^{-1}) \cdot \left[(\bar{A} \bar{G} \bar{A}^{-1}) \cdot (\bar{A} \bar{R}_{ff} \bar{A}^{-1}) \cdot (\bar{A} \bar{G}^T \bar{A}^{-1}) + \right. \\ & \left. + (\bar{A}) \bar{R}_{vv} \bar{A}^{-1} \right]^{-1} \end{aligned} \quad (2.43b)$$

Введемо визначення (аналогічні спектру потужності Вінера–Хінчина) для матриці перетворення у "частотну" область $\bar{A}$

$$\bar{S}_{ff} = \bar{A} \cdot \bar{R}_{ff} \cdot \bar{A}^{-1}; \quad (2.44a)$$

$$\bar{K} = \bar{A} \cdot \bar{G} \cdot \bar{A}^{-1}; \quad (2.44b)$$

$$\bar{K}^* = \bar{A} \cdot \bar{G}^T \cdot \bar{A}^{-1} \quad (2.44c)$$

Тут $\bar{K}^*$ — аналог "спряженню" (за Фур'є) спектра.

Тоді (з урахуванням (2.38), (2.44)) одержимо для корегуючої матриці $\bar{M}$

$$\bar{M} = \bar{S}_{ff} \cdot \bar{K}^* (\bar{K} \cdot \bar{S}_{ff} \cdot \bar{K}^* + \bar{S}_{vv})^{-1} \quad (2.45)$$

Одержаний вираз у матричному вигляді дуже нагадує Вінерівський фільтр, але він вірний для довільного "частотного" базису (Адамара, Хаара, похилого перетворення, тощо). Цей вираз вірний і для базису Фур'є у гомогенному полі, але в Фур'є-області матриці $\bar{S}, \bar{K}, \bar{K}^*$ мають діагональну структуру (тобто всі елементи цих матриць крім елементів головної діагоналі нульові і тому перемноження матриць відповідає перемноженню однакових за номером – частотою елементів діагоналі). Тому вираз (2.45) для базису Фур'є

(тобто для перетворення Фур'є-образу в гомогенному полі) дуже сильно спрощується і набуває вигляду

$$M(n) = \frac{G^*(n)}{|G(n)|^2 + \frac{S_{vv}(n)}{S_{ff}(n)}} \quad (2.46a)$$

або для двовимірного образу

$$M(m, n) = \frac{G^*(m, n)}{|G(m, n)|^2 + \frac{S_{vv}(m, n)}{S_{ff}(m, n)}}. \quad (2.46b)$$

Для випадку негомогенного поля образу у виразі (2.43а,б) **усі матриці недіагональні**. Це значно ускладнює операції над одержаним узагальненим виразом, особливо у двовимірному випадку, оскільки, якщо діагональ матриці $\bar{M}$ Вінерівського фільтра має той самий формат N , що й шуканий сигнал $\bar{f}$, то в матрицях (2.45) матриця $\bar{M}$ має N^2 ненульових елементів.

На завершення наведемо деякі властивості методу:

1) узагальнена дискретна фільтрація є значно **універсальнішою**, ніж Вінерівська фільтрація, оскільки **виключає вимогу гомогенності** поля (особливо це важливо для двовимірних образів). Тобто Вінерівська фільтрація є частковим випадком узагальненої щодо базису (Фур'є) і умови гомогенності поля образу фільтрації. Додамо, що гомогенність поля образу практично ніколи не виконується. З іншого боку, така фільтрація має операнди-матриці з квадратично зростаючими порядками, що значно ускладнює її реалізацію;

2) обчислення кореляційних матриць для побудови фільтра є окремою проблемою, оскільки, якщо **поля негомогенні**, то вони й **не ергодичні**. Тому треба знаходити **середнє за ансамблем**. Це виключає можливість використання узагальненої фільтрації, якщо в наявності є мала кількість реалізацій образу і шуму;

3) позитивною властивістю методу є те, що $\bar{A}$ — **це матриця довільного глобального ортогонального перетворення**. При цьому трудомісткість обчислень, наприклад, при використанні перетворення Адамара може бути суттєво зменшена;

4) у деяких випадках алгоритм можна спростити. Так, якщо $\bar{G} = \bar{E}$, тобто деградація має місце лише за рахунок адитивного шуму, можливе значне зменшення кількості операцій. У цьому випадку

$$\bar{M} = \bar{A} \cdot \bar{R}_{ff} \cdot (\bar{R}_{ff} + \bar{R}_{vv})^{-1} \cdot \bar{A}^{-1} = \bar{A} \cdot \bar{R}_{ff} \cdot \bar{A}^{-1} \cdot \bar{A} \cdot (\bar{R}_{ff} + \bar{R}_{vv})^{-1}. \quad (2.47)$$

$$\bar{A}^{-1} = S_{ff} \cdot (\bar{S}_{ff} + \bar{S}_{vv})^{-1}.$$

2.7. Деконволюція за критерієм форми результуючої імпульсної характеристики

Цей метод також відноситься до сукупності методів лінійних оцінок. На відміну від умовної деконволюції і Вінерівської фільтрації за критерій реставрації тут беруть не різницю між первинним та деградованим образом, а **відхилення імпульсної характеристики від $\delta(x,y)$ –функції Дірака.**

Тому ідея реставрації в побудові корегуючого фільтра $\xi(x,y)$, який перетворить імпульсну характеристику деградуєної системи $g(x,y)$ в обрану $c(x,y)$, яку за обраними критеріями вважають наближенням δ –функції Дірака

$$c(x,y) = g(x,y) * \xi(x,y) \rightarrow \delta(x,y). \quad (2.48)$$

Одержання результуючої імпульсної характеристики у вигляді δ –імпульсу (в дискретній версії вона б мала розміри єдиного пікселя) відповідало б інверсній деконволюції або (в області трансформант Фур'є) простій частотній інверсній фільтрації образу.

Але необхідність урахування адитивного шуму в моделі деградації (2.1) при реалізації формули (1.48), в якій $c(x,y) \equiv \delta(x,y)$ призведе до наступного результату

$$v(x,y) * \xi(x,y) = \xi(x,y) * [g(x,y) * f(x,y) + u(x,y)] = f(x,y) + \xi(x,y) * u(x,y). \quad (2.49)$$

Останній нульовий доданок в (1.49) може призвести до більшого маскування шумом одержаного образу, ніж це було для (2.1). Тому

результуюча імпульсна характеристика $c(x,y)$ не є δ -імпульсом, а повинна мати таку форму, щоб (як і раніше) рівень шуму (дисперсія) не перевищував (або був меншим) рівня шуму в моделі деградації образу (2.1).

Тому на імпульсну характеристику корегуючого фільтра слід ввести додаткові обмеження (сенси яких витікає з досвіду реставрації і діагностичних вимог до ступеня реставрації образу в медичній практиці).

Мірою спотворень імпульсної характеристики є гострота $1/r^2$ результуючої функції $c(x,y)$, де

$$r^2(x,y) = \iint_{-\infty}^{\infty} w(x,y) \cdot c^2(x,y) dx dy / \iint_{-\infty}^{\infty} c^2(x,y) dx dy \quad (2.50)$$

Ця функція є максимальною при мінімальному значенні $r^2(x,y)$. В формулі (2.50) $w(x,y)$ – вагова функція (або функція штрафів), яка й визначає необхідну форму імпульсної характеристики $c(x,y)$. Вона "штрафує" значення гостроти $(1/r^2)$, які знаходяться за точкою $(x,y) = (0,0)$ з визначеною вагою.

Такі штрафні функції можуть бути задані різним чином, наприклад:

$$\begin{aligned} 1) \quad w(x,y) &= x^2 + y^2; \\ 2) \quad w(x,y) &= \begin{cases} 0 & \text{для } x, y \in D \\ 1 & \text{для інших } x, y \end{cases} \end{aligned} \quad (2.51)$$

де D є заданою околицею точки $(0,0)$;

Найчастіше використовують функцію, встановлюючи:

$$D \in \{x,y; |x| < r_0; |y| < r_0\}.$$

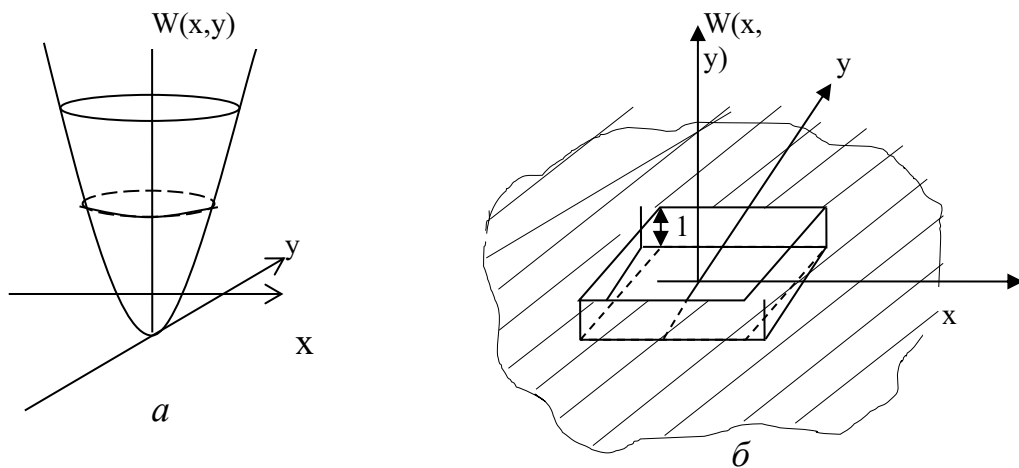


Рис.2.3 Графіки штрафних функцій

Для уявлення суті "штрафування" на рис.2.3 наведені графіки функцій:

(1) — рис.2.3,а; (2) — рис.2.3,б.

Алгоритм деградації–реставрації для даної задачі має наступний вигляд:

1) неперервна (континуальна) деградація

$$g(x, y) * f(x, y);$$

2) додавання шуму

$$L(x, y) = g(x, y) * f(x, y) + \nu(x, y);$$

3) дискретизація, що надає дані $L(x, y)$ у вигляді матриці образу розміру $N \times N$;

4) дискретна реставрація за допомогою лінійного фільтра з імпульсною характеристикою $\xi(x_i, y_i)$ з розміром $(2M+1) \times (2M+1)$, який і дає дискретну оцінку $\hat{f}(x, y)$.

Розглянемо тепер більш детально процес обчислення імпульсної характеристики реставруючого фільтра. Нехай для області D при обраному форматі імпульсної характеристики $M \times M$ реставруючого фільтра мінімізована характеристика r за умови

$$\varepsilon_0^2 \leq \varepsilon^2,$$

де ε^2 – енергія шуму перед реставрацією;

ε_0^2 – енергія шуму після реставрації.

Для простоти розглянемо одновимірний випадок реставрації образу, тобто нехай усі операнди у формулах (2.48) – (2.51) будуть одновимірними. Тоді рівняння (2.50), (2.51) можна записати у вигляді

$$r^2 = \int_{-\infty}^{\infty} w(x) \cdot c^2(x) dx / \int_{-\infty}^{\infty} c^2(x) dx; \quad (2.52)$$

$$w(x) = \begin{cases} 0 & \text{для } |x| < D/2 \\ 1 & \text{для інших } x. \end{cases}$$

Енергію шуму ε_0^2 після реставрації можна записати у вигляді

$$\varepsilon_0^2 = \sum_{k=-M}^M \sum_{p=-M}^M \xi(x_k) \cdot \xi(x_p) \cdot R_{vv}(p - k). \quad (2.52a)$$

Цей вираз вірний для однорідного поля образу.

Результуюча імпульсна характеристика має вигляд

$$c(x) = g(x) * \xi(x) = \sum_{i=-M}^M \xi(x_i) \cdot g(x - x_i). \quad (2.53)$$

Той самий результат у матричному вигляді

$$[\bar{G}(x - x_i)]^T \cdot \bar{\xi}(x_i). \quad (2.54)$$

Тоді $c^2(x)$ можна обчислити за формулою

$$c^2(x) = \bar{\xi}^T \cdot \bar{G} \cdot \bar{G}^T \cdot \bar{\xi}, \quad (2.55)$$

де $\bar{\xi} = [\xi(x_{-M}) \ \xi(x_{-M+1}) \ \dots \ \xi(x_1) \ \dots \ \xi(x_M)]^T$;

$$\bar{G} = [g(x - x_{-M}) \ \dots \ g(x - x_i) \ \dots \ g(x - x_M)]^T.$$

Розглянемо ядро виразу (1.55)

$$\bar{\beta} = \bar{G} \times \bar{G}^T = \begin{bmatrix} g(x - x_{-M}) \\ \dots \dots \dots \\ g(x - x_M) \end{bmatrix} \cdot [g(x - x_{-M}) \ \dots \ g(x - x_M)].$$

Тоді в (1.52)

$$\int_{-\infty}^{\infty} c^2(x) dx = \int_{-\infty}^{\infty} \bar{\xi}^T \cdot \bar{\beta}(x) \cdot \bar{\xi} dx$$

Оскільки дискрети корегуючого фільтра $\bar{\xi}$ не залежать від континуальних координат x , одержимо

$$\int_{-\infty}^{\infty} c^2(x) dx = \bar{\xi}^T \cdot \left[\int_{-\infty}^{\infty} \bar{\beta}(x) dx \right] \cdot \bar{\xi}$$

Таким чином, для обчислень велике значення має обчислення матриці

$$\bar{\bar{B}} = \int_{-\infty}^{\infty} \bar{\beta}(x) dx.$$

Для кращої ілюстрації елементів матриці $\bar{\bar{B}}$ розглянемо вигляд підінтегральної матриці $\beta(x)$ для випадку $M \in [0, 1, 2, 3]$. Тобто

$$\bar{\beta} = \begin{bmatrix} g(x - x_0) \\ g(x - x_1) \\ g(x - x_2) \\ g(x - x_3) \end{bmatrix} \cdot [g(x - x_0) \ g(x - x_1) \ g(x - x_2) \ g(x - x_3)] =$$

$$\begin{bmatrix} g(x - x_0) \cdot g(x - x_0) & g(x - x_0) \cdot g(x - x_1) & g(x - x_0) \cdot g(x - x_2) & g(x - x_0) \cdot g(x - x_3) \\ g(x - x_1) \cdot g(x - x_0) & g(x - x_1) \cdot g(x - x_1) & g(x - x_1) \cdot g(x - x_2) & g(x - x_1) \cdot g(x - x_3) \\ g(x - x_2) \cdot g(x - x_0) & g(x - x_2) \cdot g(x - x_1) & g(x - x_2) \cdot g(x - x_2) & g(x - x_2) \cdot g(x - x_3) \\ g(x - x_3) \cdot g(x - x_0) & g(x - x_3) \cdot g(x - x_1) & g(x - x_3) \cdot g(x - x_2) & g(x - x_3) \cdot g(x - x_3) \end{bmatrix}$$

Таким чином, для обчислення елементів матриці $\bar{\bar{B}}$ слід обчислити всі інтеграли

$$B_{ij} = \int_{-\infty}^{\infty} g(x - x_i) \cdot g(x - x_j) dx. \quad (2.56a)$$

Аналогічно, для чисельника функції гостроти (1.51) (тобто матриці $\bar{\bar{A}}$)

$$A_{ij} = \int_{-\infty}^{\infty} w(x) \cdot g(x - x_i) \cdot g(x - x_j) dx. \quad (2.56b)$$

Після наведених обчислень елементів матриць $\bar{\bar{A}}$ і $\bar{\bar{B}}$ одержимо (2.56b) у матричному вигляді

$$r^2 = \bar{\xi}^T \cdot \bar{\bar{A}} \cdot \bar{\xi} / (\bar{\xi}^T \cdot \bar{\bar{B}} \cdot \bar{\xi}), \quad (2.57)$$

яке залежить як від імпульсної характеристики моделі деградації, так і від вигляду штрафної функції $w(x)$, і яке й повинно бути мінімальним в сенсі виконання умови

$$\bar{\xi}^T \cdot \bar{\bar{R}}_{vv} \cdot \bar{\xi} = \varepsilon_0^2, \quad (2.58)$$

яка є матричним записом виразу (2.52a). Тобто формально—математично деконволюцію за критерієм оптимальної (в сенсі $w(x)$ і $\varepsilon_0^2 < \varepsilon^2$) імпульсної характеристики (оптимізуючий фільтр при цьому має імпульсну характеристику $\bar{\xi}$) є конволюція фільтром (2.49), дискрети якого є розв'язком системи рівнянь

$$\begin{cases} \bar{\xi}^T \cdot \bar{\bar{A}} \cdot \bar{\xi} / \bar{\xi}^T \cdot \bar{\bar{B}} \cdot \bar{\xi} = \min \\ \bar{\xi}^T \cdot \bar{\bar{R}}_{vv} \cdot \bar{\xi} = \varepsilon_0^2. \end{cases} \quad (2.59)$$

Нагадаємо, що всі матриці (2.59) крім $\bar{\xi}$ обчислені (відомі) заздалегідь. Матрицю $\bar{\bar{A}}$ обчислюють на базі $g(x)$ за виразом (2.56b), аналогічно — матрицю $\bar{\bar{B}}$ (з урахуванням вибраної функції $w(x)$). Найбільш трудомістким буде обчислення $\bar{\bar{R}}_{vv}$ — автокореляційної матриці первинного шуму.

З першого рівняння (2.59) за методом невизначених коефіцієнтів $\lambda^{(1)}$ матимемо

$$\bar{\xi}^T \cdot \bar{\bar{A}} \cdot \bar{\xi} - \lambda^{(1)} \cdot \bar{\xi}^T \cdot \bar{\bar{B}} \cdot \bar{\xi} = 0, \quad (2.60a)$$

а з другого рівняння в (1.59)

$$\bar{\xi}^T \cdot \bar{\bar{R}}_{vv} \cdot \bar{\xi} - \varepsilon_0^2 = 0 \quad (2.60b)$$

Об'єднуючи обидва рівняння (з коефіцієнтом $\lambda^{(2)}$), одержимо

$$(\bar{\xi}^T \cdot \bar{A} \cdot \bar{\xi} - \lambda^{(1)} \cdot \bar{\xi}^T \cdot \bar{B} \cdot \bar{\xi}) + \lambda^{(2)} \cdot (\bar{\xi}^T \cdot \bar{R}_{vv} \cdot \bar{\xi} - \varepsilon_0^2) = \min. \quad (2.61)$$

Оскільки рівняння (2.61) оперує з квадратичними формами невідомих $\bar{\xi}$, тому (як і в методі умовної деконволюції) лінеаризуємо умову (2.61) диференціюванням за $\bar{\xi}$. Одержимо

$$\bar{A} \cdot \bar{\xi} - \lambda^{(1)} \cdot \bar{B} \cdot \bar{\xi} + \lambda^{(2)} \cdot \bar{R}_{vv} \cdot \bar{\xi} = 0, \quad (2.62)$$

звідки

$$(\bar{A} + \lambda^{(2)} \cdot \bar{R}_{vv}) \cdot \bar{\xi} = \lambda^{(1)} \cdot \bar{B} \cdot \bar{\xi} \quad (2.63)$$

або

$$\bar{B}^{-1} \cdot (\bar{A} + \lambda^{(2)} \cdot \bar{R}_{vv}) \cdot \bar{\xi} = \lambda^{(1)} \cdot \bar{\xi}.$$

Якщо тепер привести рівняння (1.63) до вигляду

$$[\bar{B}^{-1} \cdot (\bar{A} + \lambda^{(2)} \cdot \bar{R}_{vv}) - \lambda^{(1)} \cdot \bar{E}] \cdot \bar{\xi} = 0, \quad (2.64)$$

то побачимо, що $\lambda^{(1)}$ має сенс власного значення матриці

$$\bar{B}^{-1} \cdot$$

$(\bar{A} + \lambda^{(2)} \cdot \bar{R}_{vv})$, а $\bar{\xi}$ – сенс її власного вектора.

Отже, для обчислення стовпця $\bar{\xi}$ дискретів імпульсної характеристики оптимізуючого фільтра слід сформулювати (надаючи деяке значення $\lambda^{(2)}$) матрицю

$$\bar{D} = \bar{B}^{-1} \cdot (\bar{A} + \lambda^{(2)} \cdot \bar{R}_{vv}).$$

Далі обчислити власні значення матриці $\bar{D}$, тобто знайти розв'язок рівняння

$$|\bar{D} - \lambda^{(1)} \cdot \bar{E}| = 0. \quad (2.65)$$

Для одержаних значень $\lambda_i^{(1)}$ знайти власні вектори $\bar{\xi}_v^{(i)}$

$$[\bar{D} - \lambda_i^{(1)} \cdot \bar{E}] \cdot \bar{\xi}_v^{(i)} = 0. \quad (2.66)$$

Тобто задача деконволюції може мати m розв'язків (m векторів $\bar{\xi}_v^{(i)}$, де m – порядок матриці $\bar{D}$).

Аналіз даної методики деконволюції показує, що, якщо в (2.66) шукають глобальний мінімум, то $\lambda_{opt}^{(1)}$ – це найменше з усіх $\lambda_i^{(1)}$ (при наданому $\lambda^{(2)}$ в (2.64)).

Таким чином, для математично коректного розв'язання задачі

реставрації треба:

- 1) надати значення $\lambda^{(2)}$ в (2.64) і сформувати матрицю $\bar{\bar{D}}$;
- 2) знайти усі власні значення $\lambda_i^{(1)}$ матриці $\bar{\bar{D}}$ за (2.65);
- 3) обрати значення $\lambda_i^{(1)}$ – мінімальне;
- 4) знайти за (2.66) власний вектор $\bar{\xi}_v^{(i)}$, що відповідає власному значенню $\lambda_i^{(1)}$;
- 5) знайти реставровані образи (2.53) за набором фантомів;
- 6) якщо образи задовільні, то обчислення закінчити; якщо ні – то надати нове значення $\lambda^{(2)}$ в (2.64) і перейти до пункту (2).

При великих форматах образу задача формування рівняння (2.64) є досить складною, але складові виразу і **імпульсну характеристику** $\xi(x)$ для даної **системи знаходять лише один раз** (оскільки $g(x)$ системи і притаманні їй внутрішні шуми і їх характеристики ε^2 , $R_{vv}(\Delta x, \Delta y)$ не змінюються і є сталими для всіх досліджуваних образів.

До розглянутої методики слід додати деякі зауваження:

- 1) обмеженням методу є гомогенність (однорідність) випадкових полів (образу і шуму) і лінійність методики (конволюційний реставруючий фільтр);
- 2) критерієм вірного розв'язку є мінімізація відхилення результуючої імпульсної характеристики від δ -імпульсу (або іншого імпульсу, наданого критерієм $w(x, y)$). Цей критерій фізично зрозумілий і наочний;
- 3) методику слід (і можна) доопрацювати у двох напрямках:
 - а) знайти простіший шлях (апріорної) оцінки коефіцієнта $\lambda^{(2)}$;
 - б) **перевести методику у частотну область** (за рахунок ДПФ), де слід очікувати значного зменшення трудомісткості.

2.8 Умовна деконволюція в області трансформант Адамара. Побудова матриці деградації образу

В першому розділі розглянуто метод умовної деконволюції реставрації образу, за яким в натуральних координатах оцінка шуканого (реставрованого) образу може бути отримана (у випадку одновимірного образу) за виразом

$$\hat{f} = \left[\bar{\bar{G}}^T \cdot \bar{\bar{G}} + \frac{1}{\lambda} \cdot \bar{\bar{c}}^T \cdot \bar{\bar{c}} \right]^{-1} \cdot \bar{\bar{G}}^T \cdot \bar{L}, \quad (2.67)$$

де $\hat{f}$ — шукана оцінка розміру $N \times 1$; $\bar{\bar{G}}$ — матричний оператор дискретної згортки (2.9) порядку N ; $\bar{\bar{c}}$ — матричний дискретний оператор умови «гладкості» оцінки (2.20) порядку N ; $\bar{L}$ — стовпець відліків деградованого образу; λ — коефіцієнт варіації Лагранжа; T — знак транспонування.

Формальний перехід від виразу (2.67) до виразу для оцінки спектру в області ортогональних перетворень достатньо простий. Для цього слід помножити певним чином матричні оператори виразу (2.67) на нормовані матричні оператори обраного ортогонального перетворення $\bar{\bar{W}}_H$ та $\bar{\bar{W}}_H^{*T}$ (враховуючи при цьому, що $\bar{\bar{W}}_H \cdot \bar{\bar{W}}_H^{*T} = \bar{\bar{E}}$) і отримати

$$\begin{aligned} \bar{\bar{W}}_H \cdot \hat{f} &= \bar{\bar{W}}_H \cdot \left[\bar{\bar{G}}^T \cdot \bar{\bar{G}} + \frac{1}{\lambda} \cdot \bar{\bar{c}}^T \cdot \bar{\bar{c}} \right]^{-1} \cdot \bar{\bar{W}}_H^{*T} \cdot \bar{\bar{W}}_H \cdot \bar{\bar{G}}^T \cdot \bar{\bar{W}}_H^{*T} \cdot \bar{\bar{W}}_H \cdot \bar{L} = \\ \hat{f}_\xi &= \left[\bar{\bar{W}}_H \cdot \bar{\bar{G}}^T \cdot \bar{\bar{G}} \cdot \bar{\bar{W}}_H^{*T} + \frac{1}{\lambda} \cdot \bar{\bar{W}}_H \cdot \bar{\bar{c}}^T \cdot \bar{\bar{c}} \cdot \bar{\bar{W}}_H^{*T} \right]^{-1} \cdot \bar{\bar{W}}_H \cdot \bar{\bar{G}}^T \cdot \bar{\bar{W}}_H^{*T} \cdot \bar{L}_\xi. \end{aligned}$$

Звідки

$$\hat{f}_\xi = \left[\bar{\bar{G}}_{2\xi} + \frac{1}{\lambda} \cdot \bar{\bar{c}}_{2\xi} \right]^{-1} \cdot \bar{\bar{G}}_\xi^T \cdot \bar{L}_\xi, \quad (2.68)$$

де $\hat{f}_\xi, \bar{L}_\xi$ — стовпці спектрів оцінки реставрованого та деградованого образів відповідно розміру $N \times 1$; $\bar{\bar{G}}_{2\xi} = \bar{\bar{W}}_H \cdot \bar{\bar{G}}^T \cdot \bar{\bar{G}} \cdot \bar{\bar{W}}_H^{*T}$ — спектр квадратичної форми дискретного матричного оператора згортки; $\bar{\bar{G}}_\xi^T$ — ортогональне перетворення матричного оператора дискретної згортки; $\bar{\bar{c}}_{2\xi}$ — ортогональне перетворення матричного оператора «гладкості»; λ — коефіцієнт варіації Лагранжа; T — знак транспонування. Усі квадратні матриці мають порядок N .

Вираз (2.68), наприклад у випадку, коли $\bar{\bar{W}}_H$ — матричний дискретний оператор нормованого перетворення Фур'є, перетворюється до вигляду

$$\hat{f}_\omega = \left[\bar{\bar{G}}_{2\omega} + \frac{1}{\lambda} \cdot \bar{\bar{c}}_{2\omega} \right]^{-1} \cdot \bar{\bar{G}}_\omega^* \cdot \bar{L}_\omega, \quad (2.68a)$$

де $\hat{f}_\omega, \bar{L}_\omega$ — стовпці відліків спектрів Фур'є реставрованого та деградованого образів відповідно розміру $N \times 1$; $\bar{\bar{G}}_\omega^*$ — діагональна матриця спряженого спектру імпульсної характеристики деградації образу порядку N ; $\bar{\bar{G}}_{2\omega}, \bar{\bar{c}}_{2\omega}$ — діагональні матриці спектрів потужності деградації образу та умови гладкості (2.29a) відповідно порядку N .

З виразу (2.68a), враховуючи, що матриці $\bar{\bar{G}}_\omega^*, \bar{\bar{G}}_{2\omega}, \bar{\bar{c}}_{2\omega}$ є діагональними, легко отримати вираз (2.31).

У випадку використання спектрів перетворення Адамара вираз (2.68) приймає вигляд [15]

$$\hat{f}_{Had} = \left[\bar{\bar{G}}_{2Had} + \frac{1}{\lambda} \cdot \bar{\bar{c}}_{2Had} \right]^{-1} \cdot \bar{\bar{G}}_{1Had}^T \cdot \bar{L}_{Had}, \quad (2.69)$$

де $\hat{f}_{Had}, \bar{L}_{Had}$ — стовпці відліків спектрів Адамара реставрованого та деградованого образів відповідно розміру $N \times 1$; $\bar{\bar{G}}_{1Had}^T$ — блочно-діагональна матриця $\bar{\bar{Had}}_H \cdot \bar{\bar{G}}^T \cdot \bar{\bar{Had}}_H^T$; $\bar{\bar{G}}_{2Had} = \bar{\bar{Had}}_H \cdot \bar{\bar{G}}_2 \cdot \bar{\bar{Had}}_H^T$ та $\bar{\bar{c}}_{2Had} = \bar{\bar{Had}}_H \cdot \bar{\bar{c}}_2 \cdot \bar{\bar{Had}}_H^T$; $\bar{\bar{G}}_{1Had} = \bar{\bar{Had}}_H \cdot \bar{\bar{G}}_1 \cdot \bar{\bar{Had}}_H^T$ — блочно-діагональні матриці порядку N .

В (2.69) матрицю $\bar{\bar{G}}_{2Had}$ можна представити у вигляді

$$\bar{\bar{G}}_{2Had} = \bar{\bar{Had}}_H \cdot \bar{\bar{G}}^T \cdot \bar{\bar{Had}}_H^T \cdot \bar{\bar{Had}}_H \cdot \bar{\bar{G}} \cdot \bar{\bar{Had}}_H^T$$

Тому слід більш детально розглянути властивості одного з множників

$$\bar{\bar{G}}_{1Had} = \bar{\bar{Had}}_H \cdot \bar{\bar{G}} \cdot \bar{\bar{Had}}_H^T \quad (2.70)$$

добутку $\bar{\bar{G}}_{2Had}$.

Матриця $\bar{\bar{G}}_{1Had}$ є блочно-діагональною матрицею, причому величина блоків зростає із зростанням номерів рядків матриці. Так, перші два елементи цієї матриці є діагональними

$$g_{H1,00} = (g_0 + g_1 + g_2 + \dots + g_{N-1}); \quad (2.70a)$$

$$g_{H1,00} = (g_0 - g_1 + g_2 - g_3 + g_4 \dots + g_{2n} - g_{2n+1} \dots +),$$

де g_i – i -й відлік імпульсної характеристики деградації ($i = 0, 1, 2, \dots, N - 1$); $N = 2^k$ – формат перетворення (оскільки імпульсна характеристика завжди значно коротша, ніж формат образу N , то рядки матриці $\bar{G}$ поповнюють нулями); k – ціле позитивне число.

Елементи другого та третього рядків утворюють матрицю другого порядку, елементи якої

$$g_{H1,22} = g_{H1,33} = (g_0 - g_2 + g_4 - g_6 + g_8 - g_{10} + \dots); \quad (2.70б)$$

$$g_{H1,23} = -g_{H1,32} = (g_1 - g_3 + g_5 - g_7 + g_9 - g_{11} + \dots).$$

Наступним є блок четвертого порядку, який має елементи

$$g_{H1,44} = g_{H1,66} = [g_0 + (1/2) \cdot (g_1 - g_3) - g_4 - (1/2) \cdot \quad (2.70в)$$

$$(g_5 - g_7) + g_8 + (1/2) \cdot (g_9 - g_{11}) - g_{12} - \dots];$$

$$g_{H1,45} = g_{H1,67} = -g_{H1,54} = -g_{H1,76} = (1/2) \cdot [(g_1 + g_3) - (g_5 + g_7) + (g_9 + g_{11}) - \dots];$$

$$g_{H1,55} = g_{H1,77} = [g_0 - (1/2) \cdot (g_1 - g_3) + g_4 - (1/2) \cdot$$

$$(g_5 - g_7) - g_8 + (1/2) \cdot (g_9 - g_{11}) - g_{12} + \dots];$$

$$g_{H1,46} = -g_{H1,64} [(1/2) \cdot g_1 + g_2 + (1/2) \cdot g_3 - (1/2) \cdot g_5 - g_6 - (1/2) \cdot g_7 + (1/2) \cdot g_9 + g_{10} + (1/2) \cdot g_{11} - \dots]$$

$$-g_{H1,57} = g_{H1,75} = [(1/2) \cdot g_1 - g_2 + (1/2) \cdot g_3 - (1/2) \cdot g_5 + g_6 - (1/2) \cdot g_7 + (1/2) \cdot g_9 - g_{10} + (1/2) \cdot g_{11} - \dots];$$

$$-g_{H1,17} = g_{H1,52} - g_{H1,71} = g_{H1,65} [(1/2) \cdot (g_1 - g_3) + (1/2) \cdot (g_5 - g_7) + (1/2) \cdot (g_9 - g_{11}) - g_{12} + (1/2) \cdot (g_{13} - g_{15}) + \dots].$$

Наступний блок — матриця восьмого порядку з номерами рядків та стовпців 8...15, далі матриця з номерами рядків та стовпців 16...31 і т.д. [15].

2.8.1 Алгоритм обчислення коефіцієнтів блочно-діагональної матриці

$\bar{\bar{G}}_{1Had}$

Безпосереднє обчислення добутку матриць (2.70) в чисельній формі призведе до громіздких математичних обчислень (враховуючи порядок N матриць $\bar{\bar{Had}}_n$ та $\bar{\bar{G}}$). Так, для одновимірних сигналів N зазвичай дорівнює 128...512, а для двовимірних відповідно $(512)^2 \dots (2048)^2$ (тобто $\approx 2,5 \cdot 10^4 \dots 4 \cdot 10^6$).

Кількість трудоемних операцій при формуванні $\bar{\bar{G}}_{1Had}$ безпосереднім множенням матриць оцінюється як $2 \cdot N^3$. Крім того велика кількість складових в $g_{n1,ij}$ в процесі обчислень взаємно знищується. Використання того, що матриця $\bar{\bar{G}}_{1Had}$ має блочно-діагональний вигляд, дозволяє зекономити на кількості операцій множення, якщо не обчислювати ті добутки рядків та стовпців матриць $\bar{\bar{Had}}$, $\bar{\bar{Had}}_n^T$ на матрицю $\bar{\bar{G}}$, які апіорі дорівнюють нулю. Тим не менше, обчислення ненульових добутків в (2.70) в чисельному вигляді призведе (враховуючи великі порядки матриць N) до накопичення великої операційної похибки за рахунок обмеженої розрядності операнд. Враховуючи структуру матриці $\bar{\bar{G}}$, можна проводити обчислення без згаданого накопичення операційної похибки. Для пояснення розглянемо структуру матриці $\bar{\bar{G}}$ та процедуру обчислення елементів матриці $\bar{\bar{G}}_{1Had}$, на простому прикладі матриць восьмого порядку для найбільшої можливої для такого порядку кількості (вісім) відліків імпульсної характеристики g_i . Так, матриця $\bar{\bar{G}}$ восьмого порядку має вигляд

g_0	g_7	g_6	g_5	g_4	g_3	g_2	g_1
g_1	g_0	g_7	g_6	g_5	g_4	g_3	g_2
g_2	g_1	g_0	g_7	g_6	g_5	g_4	g_3
g_3	g_2	g_1	g_0	g_7	g_6	g_5	g_4

(2.71a)

g_4	g_3	g_2	g_1	g_0	g_7	g_6	g_5
g_5	g_4	g_3	g_2	g_1	g_0	g_7	g_6
g_6	g_5	g_4	g_3	g_2	g_1	g_0	g_7
g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_0

а, наприклад, елемент $g_{H1,45}$ можна обчислити множенням цієї матриці $\bar{\bar{G}}$ на четвертий рядок had_4 матриці $\bar{\bar{Had}}$ ліворуч та п'ятий стовпець had_5 матриці $\bar{\bar{Had}}^T$ праворуч. Для даного прикладу

$$had_4 = [1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad -1]; \quad (2.716)$$

$$had_5 = [1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad -1 \quad 1]^T.$$

Можна показати, що знаки перед елементами g_i добутку (2.70) для множників (2.70б) можна отримати у вигляді матриці $\bar{\bar{\varphi}}$ множенням had_4 у вигляді стовпця на had_5 у вигляді рядка, тобто

$$\bar{\bar{\varphi}} = \quad (2.72)$$

1	-1	1	-1	-1	1	-1	1
1	-1	1	-1	-1	1	-1	1
1	-1	1	-1	-1	1	-1	1
1	-1	1	-1	-1	1	-1	1
-1	1	-1	1	1	-1	1	-1
-1	1	-1	1	1	-1	1	-1
-1	1	-1	1	1	-1	1	-1
-1	1	-1	1	1	-1	1	-1

Порівнюючи (2.71а) та (2.72), можна визначити, з якими знаками підсумовуються елементи g_i . Так, наприклад, коефіцієнт перед відліком g_0 при представленні елемента матриці $\bar{\bar{G}}_{1Had}$ в символному вигляді в клітині (4,5) дорівнює сумі всіх елементів 1 та -1 головної діагоналі матриці (2.72), а, наприклад, елемент g_3 має коефіцієнт, обчислений як сума елементів третьої нижньої піддіагоналі матриці (2.72) та верхньої п'ятої. При запропонованому способі обчислення коефіцієнтів перед відліками g_i :

а) обчислюються тільки ненульові елементи матриці $\bar{\bar{G}}_{1Had}$, для чого

перемножуються з цією матрицею тільки ті рядки і стовпці дискретних матричних операторів перетворення Адамара, які і утворюють відповідні елементи добутку;

б) обчислення коефіцієнтів перед ненульовими елементами матриці $\bar{\bar{G}}_{1Had}$ проводиться підсумовуванням цілих чисел $+1$ та -1 , що дозволяє запобігти накопиченню операційної похибки за рахунок обмеженої розрядності операндів при підсумовуванні чисельних значень g_i .

Алгоритм обчислення елементів блоків діагоналі матриці $\bar{\bar{G}}_{1Had}$ має наступний вигляд.

1. Для наданого формату N матриці $\bar{\bar{G}}$ ($N=2^n$, n —ціле число) визначити номери рядків та стовпців матричного оператора дискретного перетворення Адамара $\bar{\bar{Had}}$, які відповідають номерам рядків та стовпців окремих блоків діагоналі матриці $\bar{\bar{G}}_{1Had}$.

2. Множенням i -го стовпця матриці $\bar{\bar{Had}}$ на її j -й рядок отримати матрицю $\bar{\bar{\varphi}}_{ij}$ для обчислення коефіцієнтів при відліках імпульсної характеристики g_i , що дозволить обчислити значення елемента h_{ij} матриці $\bar{\bar{G}}_{1Had}$.

3. Послідовно обчислюючи усі елементи $g_{H1,ij}$ блоків діагоналі побудувати блочно-діагональну матрицю $\bar{\bar{G}}_{1Had}$.

При реалізації алгоритму слід враховувати додатково властивості отримуваних матриць $\bar{\bar{G}}_{(a...b),(a...b)}$ блоків діагоналі матриці $\bar{\bar{G}}_{1Had}$ (тут індекси $a \dots b$ означають номери початку та кінця нумерації рядків та стовпців блоку). Так, будь-яка матриця блоку має однакову структуру, а саме

$$\bar{\bar{G}}_{(a...b),(a...b)} = \begin{bmatrix} \bar{\bar{G}}_{(a...a+\frac{M}{2}-1),(a...a+\frac{M}{2}-1)} & \bar{\bar{G}}_{(a...a+\frac{M}{2}-1),(b-\frac{M}{2}...b)} \\ -\bar{\bar{G}}_{(a...a+\frac{M}{2}-1),(b-M/2...b)} & \bar{\bar{G}}_{(a...a+\frac{M}{2}-1),(a...a+M/2-1)} \end{bmatrix}, \quad (2.73)$$

де $M = 2^m$ — порядок матриці-блока діагоналі, m — ціле число. Таким чином, для формування будь-якої з матриць $\bar{\bar{G}}_{(a...b),(a...b)}$ достатньо сформувати лише матриці $\bar{\bar{G}}_{(a...a+M/2-1)}$ та $\bar{\bar{G}}_{(b-M/2...b)}$. Формування цих

матриць за запропонованим алгоритмом дозволяє в символічному вигляді знайти запис кожного елемента матриці $\bar{\bar{G}}_{1Had}$ будь-якого порядку.

2.8.2 Символьний метод формування матриці $\bar{\bar{G}}_{1Had}$

Для символічного аналізу у подальшому будемо зберігати значення усіх коефіцієнтів при відліках g_i кожного ненульового елемента $g_{H1,kl}$ матриці $\bar{\bar{G}}_{H1}$ в масивах чисел $\bar{\mu}_{k,l}$, в яких номери $i = 0, 1, 2, \dots, D - 1$, D — кількість відліків імпульсної характеристики ($D = 2^s$, s — ціле число).

Тоді для матриці $\bar{\bar{G}}_{(0),(0)}$ (нульовий за номером елемент діагоналі матриці $\bar{\bar{G}}_{1Had}$ маємо $\bar{\mu}_{0,0} = [1, 1, 1, \dots, 1]$. Аналогічно, одновимірна матриця $\bar{\mu}_{1,1} = [1, -1, 1, -1, 1, -1, \dots, 1, -1]$. Матриця другого порядку з номерами рядків та стовпців 2 та 3 має коефіцієнти

$$\bar{\mu}_{2,2} = \bar{\mu}_{3,3} = [1, 0, -1, 0, 1, 0, -1, 0, \dots, 1, 0, -1, 0], \quad (2.74a)$$

$$\bar{\mu}_{2,3} = -\bar{\mu}_{3,2} = [0, 1, 0, -1, 0, 1, 0, -1, \dots].$$

Матриця четвертого порядку має коефіцієнти при відліках імпульсної характеристики для підматриці $\bar{\bar{G}}_{(4\dots 5)}$ у вигляді

$$\bar{\mu}_{4,4} = \bar{\mu}_{6,6} = \left[1, \frac{1}{2}, 0, -\frac{1}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, \dots, 1, \frac{1}{2}, 0, \dots\right], \quad (2.74b)$$

$$\bar{\mu}_{5,5} = \bar{\mu}_{7,7} = \left[1, -\frac{1}{2}, 0, \frac{1}{2}, -1, \frac{1}{2}, 0, -\frac{1}{2}, \dots, 1, -\frac{1}{2}, 0, \dots\right],$$

$$\bar{\mu}_{4,5} = -\bar{\mu}_{5,4} = \bar{\mu}_{6,7} = -\bar{\mu}_{7,6} = \left[0, \frac{1}{2}, 0, \frac{1}{2}, 0, -\frac{1}{2}, 0, -\frac{1}{2}, \dots, 0, \frac{1}{2}, 0, \dots\right],$$

$$\bar{\mu}_{4,6} = -\bar{\mu}_{6,4} = \left[0, \frac{1}{2}, 1, \frac{1}{2}, 0, -\frac{1}{2}, -1, -\frac{1}{2}, \dots, 0, \frac{1}{2}, 1, \dots\right],$$

$$\bar{\mu}_{5,7} = -\bar{\mu}_{7,5} = \left[0, -\frac{1}{2}, 1, -\frac{1}{2}, 0, \frac{1}{2}, -1, \frac{1}{2}, \dots, 0, -\frac{1}{2}, 1, \dots\right],$$

$$\bar{\mu}_{6,5} = \bar{\mu}_{5,6} = -\bar{\mu}_{4,7} = -\bar{\mu}_{7,4} = \left[0, -\frac{1}{2}, 0, \frac{1}{2}, 0, \frac{1}{2}, 0, -\frac{1}{2}, \dots, 0, -\frac{1}{2}, 0, \dots\right].$$

Блок $\bar{\bar{G}}_{(a\dots a+M/2-1)}$ (2.73) підматриці $\bar{\bar{\mu}}$ восьмого порядку (рядки та стовпці з номерами 8...15) має коефіцієнти (для рядків та стовпців з номерами 8...11) у вигляді [15]

$$\bar{\bar{\mu}}_{8...11,8...11} =$$

(1,3/4,1/2,1/4, 0,- 1/4,-1/2,-3/4, -1,-3/4,-1/2,-1/4, 0,1/4,1/2,3/4, 1,3/4...)	(0,1/4,0,1/4,0, 1/4,0,1/4, 0,-1/4,0,-1/4,0, -1/4,0,-1/4, 0,1/4...)	(0,1/4,1/2,1/4, 0,1/4,1/2,1/4, 0,-1/4,-1/2,- 1/4,0, -1/4,-1/2,-1/4, 0,1/4,...)	(0,-1/4,0,1/4,0, -1/4,0,1/4, 0,1/4,0,-1/4,0, 1/4,0,-1/4, 0,-1/4,...)
(0,-1/4,0,-1/4,0, -1/4,0,-1/4, 0,1/4,0,1/4,0, 1/4,0,1/4, 0,-1/4...)	(1,-3/4,1/2,-1/4, 0,1/4,-1/2,3/4, -1,3/4,-1/2,1/4, 0,-1/4,1/2,-3/4, 1,-3/4,...)	(0,1/4,0,-1/4,0, 1/4,0,-1/4, 0,-1/4,0,1/4,0, -1/4,0,1/4, 0,1/4...)	(0,-1/4,1/2,-1/4,0, -1/4,1/2,-1/4, 0,1/4,-1/2,1/4,0, 1/4,-1/2,1/4, 0,-1/4,...)
(0,-1/4,-1/2,-1/4, 0,-1/4,-1/2,-1/4, 0,1/4,1/2,1/4,0, 1/4,1/2,1/4, 0,-1/4,...)	(0,1/4,0,-1/4,0, 1/4,0,-1/4, 0,-1/4,0,1/4,0, -1/4,0,1/4, 0,1/4...)	(1,1/4,-1/2,-1/4,0, 1/4,1/2,-1/4, -1,-1/4,1/2,1/4,0, -1/4,-1/2,1/4, 1,1/4,...)	(0,3/4,0,-1/4,0, -1/4,0,3/4, 0,-3/4,0,1/4,0, 1/4,0,-3/4, 0,3/4,...)
(0,-1/4,0,1/4,0, -1/4,0,1/4, 0,1/4,0,-1/4,0, 1/4,0,-1/4, 0,-1/4,...)	(0,1/4,-1/2,1/4,0, 1/4,-1/2,1/4, 0,-1/4,1/2,-1/4,0, -1/4,1/2,-1/4, 0,1/4,...)	(0,-3/4,0,1/4,0, 1/4,0,-3/4, 0,3/4,0,-1/4,0, -1/4,0,3/4, 0,-3/4,...)	(1,-1/4,-1/2,1/4,0, -1/4,1/2,1/4, -1,1/4,1/2,-1/4,0, 1/4,-1/2,-1/4, 1,-1/4,...)

(2.75a)

При цьому видно, що $\mu_{8,9} = -\mu_{9,8}$; $\mu_{10,11} = -\mu_{11,10}$; матриця $\bar{\bar{\mu}}_{8...9,10...11} = -\bar{\bar{\mu}}_{10...11,8...9}$.

Блок $\bar{G}_{(b-M/2...b)}$ в (2.73) підматриці $\bar{\mu}$ восьмого порядку (номери рядків 8...11, номери стовпців 12...15) має коефіцієнти при відліках g_i наступного вигляду $\bar{\bar{\mu}}_{8...11,12...15} = -\bar{\bar{\mu}}_{12...15,8...11}$

(0,1/4,1/2,3/4,	(0,-1/4,0,-1/4,0,	(0,-1/4,-1/2,-1/4,	(0,1/4,0,-1/4,0,
-----------------	-------------------	--------------------	------------------

1,3/4,1/2,1/4, 0,-1/4,-1/2,-3/4, -1,-3/4,-1/2,-1/4, 0,1/4,...)	1/4,0,1/4, 0,1/4,0,1/4,0, -1/4,0,-1/4, 0,-1/4...)	0,1/4,1/2,1/4, 0,1/4,1/2,1/4, 0,-1/4,-1/2,-1/4, 0,-1/4,...)	-1/4,0,1/4, 0,-1/4,0,1/4,0, 1/4,0,-1/4, 0,1/4...)
(0,1/4,0,1/4,0, -1/4,0,-1/4, 0,-1/4,0,-1/4,0, 1/4,0,1/4, 0,1/4...)	(0,-1/4,1/2,-3/4, 1,-3/4,1/2,-1/4, 0,1/4,-1/2,3/4, -1,3/4,-1/2,1/4, 0,-1/4,...)	(0,-1/4,0,1/4,0, 1/4,0,-1/4, 0,1/4,0,-1/4,0, -1/4,0,1/4, 0,-1/4...)	(0,1/4,-1/2,1/4, 0,-1/4,1/2,-1/4, 0,-1/4,1/2,-1/4, 0,1/4,-1/2,1/4, 0,1/4,...)
(0,1/4,1/2,1/4, 0,-1/4,-1/2,-1/4, 0,-1/4,-1/2,-1/4, 0,1/4,1/2,1/4, 0,1/4,...)	(0,-1/4,0,1/4,0, 1/4,0,-1/4, 0,1/4,0,-1/4,0, -1/4,0,1/4, 0,-1/4...)	(0,-1/4,-1/2,1/4,1, 1/4,-1/2,-1/4, 0,1/4,1/2,-1/4,-1, -1/4,1/2,1/4, 0,-1/4,...)	(0,1/4,0,-3/4,0, 3/4,0,-1/4, 0,-1/4,0,3/4,0, -3/4,0,1/4, 0,1/4,...)
(0,1/4,0,-1/4,0, -1/4,0,1/4, 0,-1/4,0,1/4,0, 1/4,0,-1/4, 0,1/4...)	(0,-1/4,1/2,-1/4, 0,1/4,-1/2,1/4, 0,1/4,-1/2,1/4, 0,-1/4,1/2,-1/4, 0,-1/4,...)	(0,-1/4,0,3/4,0, -3/4,0,1/4, 0,1/4,0,-3/4,0, 3/4,0,-1/4, 0,-1/4,...)	(0,1/4,-1/2,-1/4,1, -1/4,-1/2,1/4, 0,-1/4,1/2,1/4,-1, 1/4,1/2,-1/4, 0,1/4,...)

(2.756)

При цьому видно, що $\mu_{8,13} = -\mu_{9,12}$; $\mu_{10,15} = -\mu_{11,14}$, а матриця $\bar{\bar{\mu}}_{8...11,12...15} = -\bar{\bar{\mu}}_{12...15,8...11}$.

Отриманої інформації про коефіцієнти достатньо для пошуку закономірностей прямого. При цьому, по-перше, слід відзначити, що обчислені коефіцієнти при відліках імпульсної характеристики періодично повторюються при зростанні кількості таких відліків. Так, для матриці першого порядку $\bar{\bar{G}}_{1Had1,1}$ період повторень коефіцієнтів μ_{11} дорівнює двом, для матриці другого порядку $\bar{\bar{G}}_{1Had2...3,2...3}$ період становить чотири, для матриці четвертого порядку $\bar{\bar{G}}_{1Had4...7,4...7}$ період дорівнює восьми, для матриці

восьмого порядку — шістнадцять, а для матриці шістнадцятого порядку — тридцять два. Тобто період повторення коефіцієнтів при відліках імпульсної характеристики дорівнює мінімальному порядку матриці $\bar{\bar{G}}_{1nad}$, в якій розміщується матричний блок діагоналі, для якого ці коефіцієнти обчислюються.

По-друге, усі коефіцієнти діагональних елементів з парними індексами $\mu_{2k,2l}$ матриць $\bar{\bar{\mu}}_{a...b,c...d}$ обчислюються «розширенням» індексів елементів попереднього матричного блоку, яке полягає в поповненні ряду індексів, додаючи нові індекси між вже існуючими зі значеннями, що дорівнюють середньому арифметичному чисел праворуч та ліворуч поповнення. Так, наприклад, елемент

$\mu_{8,10} = (0, 1/4, 1/2, 1/4, 0, 1/4, 1/2, 1/4, 0, -1/4, -1/2, -1/4, 0, -1/4, -1/2, -1/4, \dots)$ матриці $\bar{\bar{\mu}}_{8...11,8...11}$ отримаємо по елементу $\mu_{4,5}$ матриці $\bar{\bar{\mu}}_{4...7,4...7} = (0, \frac{1}{2}, 0, \frac{1}{2}, 0, -\frac{1}{2}, 0, -\frac{1}{2}, \dots, 0, \frac{1}{2}, 0, \dots)$. Кожен наступний елемент $\mu_{2k+1,2l+1}$ тієї ж діагоналі отримуємо множенням коефіцієнтів елемента $\mu_{2k,2l}$ на $1, -1, 1, -1, 1, \dots$, тобто, наприклад, елемент $\mu_{9,11} = (0, -1/4, 1/2, -1/4, 0, -1/4, 1/2, -1/4, 0, 1/4, -1/2, 1/4, 0, 1/4, -1/2, 1/4, \dots)$. Таким чином, для усіх діагоналей (для матричних блоків), які починаються елементами $\mu_{2k,2l}$ обчислення елементів діагоналі не становить труднощів. Трошки інакше формуються ті діагоналі матричних блоків, які починаються елементами $\mu_{2k+1,2l}$ або $\mu_{2k,2l+1}$. Для пояснення процедури формування таких елементів розглянемо спочатку структуру матриць коефіцієнтів при відліках більш детально. Матриці $\bar{\bar{G}}_{(a...a+\frac{M}{2}-1),(a...a+\frac{M}{2}-1)}$ та $\bar{\bar{G}}_{(a...a+\frac{M}{2}-1),(b-\frac{M}{2}...b)}$ в (2.73), як і відповідні матриці коефіцієнтів, мають певну структуру. Так, матриця коефіцієнтів $\bar{\bar{\mu}}_{4...7,4...7}$ має вигляд

$$\bar{\bar{\mu}}_{4...7,4...7} = \begin{bmatrix} \bar{\bar{\mu}}_{4...5,4...5} & \bar{\bar{\mu}}_{4...5,6...7} \\ -\bar{\bar{\mu}}_{4...5,6...7} & \bar{\bar{\mu}}_{4...5,4...5} \end{bmatrix}, \text{ матриця } \bar{\bar{\mu}}_{4...7,4...7} = \begin{bmatrix} \mu_{44} & \mu_{45} \\ -\mu_{45} & \mu_{44} \end{bmatrix}, \text{ а} \quad (2.76)$$

матриця $\bar{\bar{\mu}}_{4...5,6...7} = \begin{bmatrix} \mu_{46} & \mu_{47} \\ -\mu_{47} & \mu_{46} \end{bmatrix}$. Аналогічно $\bar{\bar{\mu}}_{8...15,8...15} =$

$$\begin{bmatrix} \bar{\mu}_{8\dots11,8\dots11} & \bar{\mu}_{8\dots11,12\dots15} \\ -\bar{\mu}_{8\dots11,12\dots15} & \bar{\mu}_{8\dots11,8\dots11} \end{bmatrix}, \text{ причому } \bar{\mu}_{8\dots11,8\dots11} = \begin{bmatrix} \bar{\mu}_{8\dots9,8\dots9} & \bar{\mu}_{8\dots9,10\dots11} \\ -\bar{\mu}_{8\dots9,10\dots11} & \bar{\mu}_{10\dots11,10\dots11} \end{bmatrix}.$$

$$\text{Матриці } \bar{\mu}_{8\dots9,8\dots9} = \begin{bmatrix} \mu_{88} & \mu_{89} \\ -\mu_{89} & \mu_{99} \end{bmatrix}, \quad \bar{\mu}_{10\dots11,10\dots11} = \begin{bmatrix} \mu_{10,10} & \mu_{10,11} \\ -\mu_{10,11} & \mu_{11,11} \end{bmatrix}, \quad \bar{\mu}_{8\dots9,10\dots11} =$$

$$\begin{bmatrix} \mu_{8,10} & \mu_{8,11} \\ -\mu_{8,11} & \mu_{9,11} \end{bmatrix}. \text{ Так само } \bar{\mu}_{8\dots11,12\dots15} = \begin{bmatrix} \bar{\mu}_{8\dots9,12\dots13} & \bar{\mu}_{8\dots9,14\dots15} \\ -\bar{\mu}_{8\dots9,14\dots15} & \bar{\mu}_{10\dots11,14\dots15} \end{bmatrix}, \text{ причому}$$

$$\bar{\mu}_{8\dots9,12\dots13} = \begin{bmatrix} \mu_{8,12} & \mu_{8,13} \\ -\mu_{8,13} & \mu_{9,13} \end{bmatrix}, \quad \bar{\mu}_{8\dots9,14\dots15} = \begin{bmatrix} \mu_{8,14} & \mu_{8,15} \\ -\mu_{8,15} & \mu_{9,15} \end{bmatrix}, \quad \bar{\mu}_{10\dots11,14\dots15} =$$

$$\begin{bmatrix} \mu_{10,14} & \mu_{10,15} \\ -\mu_{10,15} & \mu_{11,15} \end{bmatrix}.$$

Аналогічні закономірності структури матриць коефіцієнтів при відліках спотворюючої сигнал (образ) імпульсної характеристики системи відображення. Для описаної структури усі закономірності формування коефіцієнтів елементів матриці $\mu_{2k+1,2l}$ та $\mu_{2k,2l+1}$, які будуть наведені нижче, вірні лише для блоків $\bar{G}_{(a\dots a+\frac{M}{2}-1),(a\dots a+\frac{M}{2}-1)}$ та $\bar{G}_{(a\dots a+\frac{M}{2}-1),(b-\frac{M}{2}\dots b)}$, а не для всієї матриці $\bar{G}_{(a\dots b),(a\dots b)}$ в (2.73). Зауважимо також, що для формування матриці $\bar{G}_{(a\dots b),(a\dots b)}$ достатньо сформувати лише верхньотрикутні (або нижньотрикутні) частини (разом з головною діагоналлю) матриць коефіцієнтів $\bar{\mu}_{(a\dots a+\frac{M}{2}-1),(a\dots a+\frac{M}{2}-1)}$ та $\bar{\mu}_{(a\dots a+\frac{M}{2}-1),(b-\frac{M}{2}\dots b)}$. Коефіцієнти $\mu_{2k+1,2l}$ та $\mu_{2k,2l+1}$ формуються за наступними рекурентними кроками.

Так, за матрицею $\bar{\mu}_{2\dots3,2\dots3}$ елемент $\mu_{2,3} = (0,1,0,-1,0,1,0,-1,\dots)$. Тоді елемент матриці $\bar{\mu}_{4\dots7,4\dots7} \mu_{2 \times 2, 2 \times 2 + 1} = \mu_{4,5} = (0,1/2,0,1/2,0,-1/2,0,-1/2,0,\dots)$ одержуємо «розширенням» послідовності коефіцієнтів елемента $\mu_{2,3}$ обчисленням проміжних значень між 0 та 1 і 0 та -1 та «проріджуванням» отриманого результату заміною чисел послідовності $(0,1,0,-1,0,1,0,-1,\dots)$ нулями, тобто $(0,1/2,1,1/2,0,-1/2,-1,-1/2,0,\dots) \rightarrow (0,1/2,0,1/2,0,-1/2,0,-1/2,0,\dots)$. Елемент $\mu_{5,6}$ отримаємо з $\mu_{4,5}$ множенням на послідовність $1,1,-1,-1,1,1,-1,-1,\dots$. Для матриці $\bar{\mu}_{8\dots15,8\dots15}$ (підматриць $\bar{\mu}_{8\dots11,8\dots11}$ та $\bar{\mu}_{8\dots11,12\dots15}$) отримуємо наступні діагональні елементи з непарними індексами. Елемент $\mu_{8,9} = \mu_{4 \times 2, 4 \times 2 + 1} = (0,1/4,0,1/4,0,1/4,0,1/4,0,-1/4,0,-1/4,0,-1/4,0,-1/4,0,1/4,\dots)$ отримуємо з елемента $\mu_{4,5}$ «розширенням» та

«проріджуванням». Аналогічно для елемента $\mu_{8,13} = \mu_{4 \times 2,6 \times 2+1}$ по елементу $\mu_{4,7}$. Елементи тих самих діагоналей $\mu_{9,10}$ та $\mu_{9,14}$ отримуємо множенням на послідовність $1, 1, -1, -1, 1, 1, -1, -1, \dots$ елементів $\mu_{8,9}$ та $\mu_{8,13}$ відповідно. Треті елементи діагоналей, що починаються елементами $\mu_{8,9}$ та $\mu_{8,13}$ отримуємо «розширенням» та «проріджуванням» елементів $\mu_{4,4}$ та $\mu_{4,6}$ з їх подальшим множенням на послідовність $1, 1, -1, -1, 1, 1, -1, -1, \dots$. При формуванні матриці $\bar{\mu}_{16 \dots 31, 16 \dots 31}$ процедура формування аналогічна попередньо зазначеній з урахуванням збільшення кількості подвоєних індексів.

Для формування матриці $\bar{\mu}$ довільного порядку слід зазначити наступні властивості отримуваних матриць.

Будь-яка матриця $\bar{\mu}$ порядку $N = 2^n$, n — ціле позитивне число, складається з чотирьох підматриць порядку 2^{n-1} , причому дві підматриці головної діагоналі рівні між собою, а підматриці зворотної діагоналі мають елементи на однакових позиціях рівні за модулем, але протилежні за знаком. Кожна з цих підматриць складається з чотирьох підматриць порядку 2^{n-2} , причому підматриці головної діагоналі вже різні, а підматриці зворотної діагоналі так, як і раніше мають елементи рівні за модулем, але протилежні за знаком. Аналогічною є структура підматриць меншого порядку (до четвертого включно).

Таким чином, алгоритм формування матриці коефіцієнтів $\bar{\mu}$ довільного порядку $N = 2^n$, n — ціле позитивне число, має наступний вигляд.

1. Розбити матрицю порядку $N = 2^n$, n — ціле позитивне число, на блоки четвертого порядку для використання описаних вище її структурних властивостей. Усі подальші операції по формуванню матриці $\bar{\mu}$ застосувати для вказаних блоків, що утворюють верхньотрикутну частину цієї матриці.
2. За матрицею $\bar{\mu}$ порядку 2^{n-1} сформувати коефіцієнти діагоналей з парними індексами $\mu_{2k,2l}$ по елементам $\mu_{k,l}$ матриці $\bar{\mu}$ порядку 2^{n-1} , використовуючи процедуру «розширення».
3. За елементами $\mu_{k,l+1}$ матриці $\bar{\mu}$ порядку 2^{n-1} «розширенням» послідовності

коефіцієнтів (обчисленням проміжних значень) та «проріджуванням» отримаємо елемент $\mu_{2k,2l+1}$, а множенням отриманого результату на послідовність $1,1,-1,-1,1,-1,\dots$ отримаємо елемент $\mu_{2k+1,2l+2}$. Елемент $\mu_{2k,2l+3} = -\mu_{2k,2l+1}$. Виконання пунктів 2,1 алгоритму дозволяє сформувати перші два рядки верхньотрикутної підматриці четвертого порядку.

4. Третій елемент піддіагоналі $\mu_{2k+2,2l+3}$ отримаємо «проріджуванням» $\mu_{2k,2l}$ та множенням отриманих коефіцієнтів на послідовність $1,1,-1,-1,1,-1,\dots$

Таким чином, безпосереднє формування матриці $\bar{\bar{G}}_{1Had}$ в (3.3) можливе і до того ж легко програмується, що дозволяє зекономити на кількості операцій множення матриць високих порядків.

Матриця $\bar{\bar{G}}$ є циркулянтною і складається з дискретних відліків. Нумерація відліків являється зворотною відносно нумерації стовпців рядка.

Елементи матриці $\bar{\bar{G}}_{1Had}$ є комбінаціями відліків g_i з коефіцієнтами μ_{ij} . Якщо в лінійних комбінаціях відліків g_s з коефіцієнтами μ_{ij} записувати впорядковано за зростанням номерів s (враховуючи і відліки з нульовими коефіцієнтами) отримаємо наступні формалізовані результати, які у подальшому дозволять сформувати алгоритм побудови матриці $\bar{\bar{G}}_{1Had}$ без множень матриць.

Формування коефіцієнтів μ_{ij} має певну закономірність, яку можна помітити у наведених формулах для коефіцієнтів при відліках імпульсної характеристики. Дана закономірність дозволяє значно зекономити на кількості операцій, які використовуються для обчислення матриці $\bar{\bar{G}}_{1Had}$.

Безпосереднє формування коефіцієнтів μ_{ij} дозволяє уникнути громіздких обчислень та накопичення операційної похибки.

За основу в такому методі приймається матриця коефіцієнтів другого порядку $\bar{\bar{\mu}}_{2,2;3,3}$.

Алгоритм для програмування має наступний вигляд (на прикладі блоку 16-го порядку).

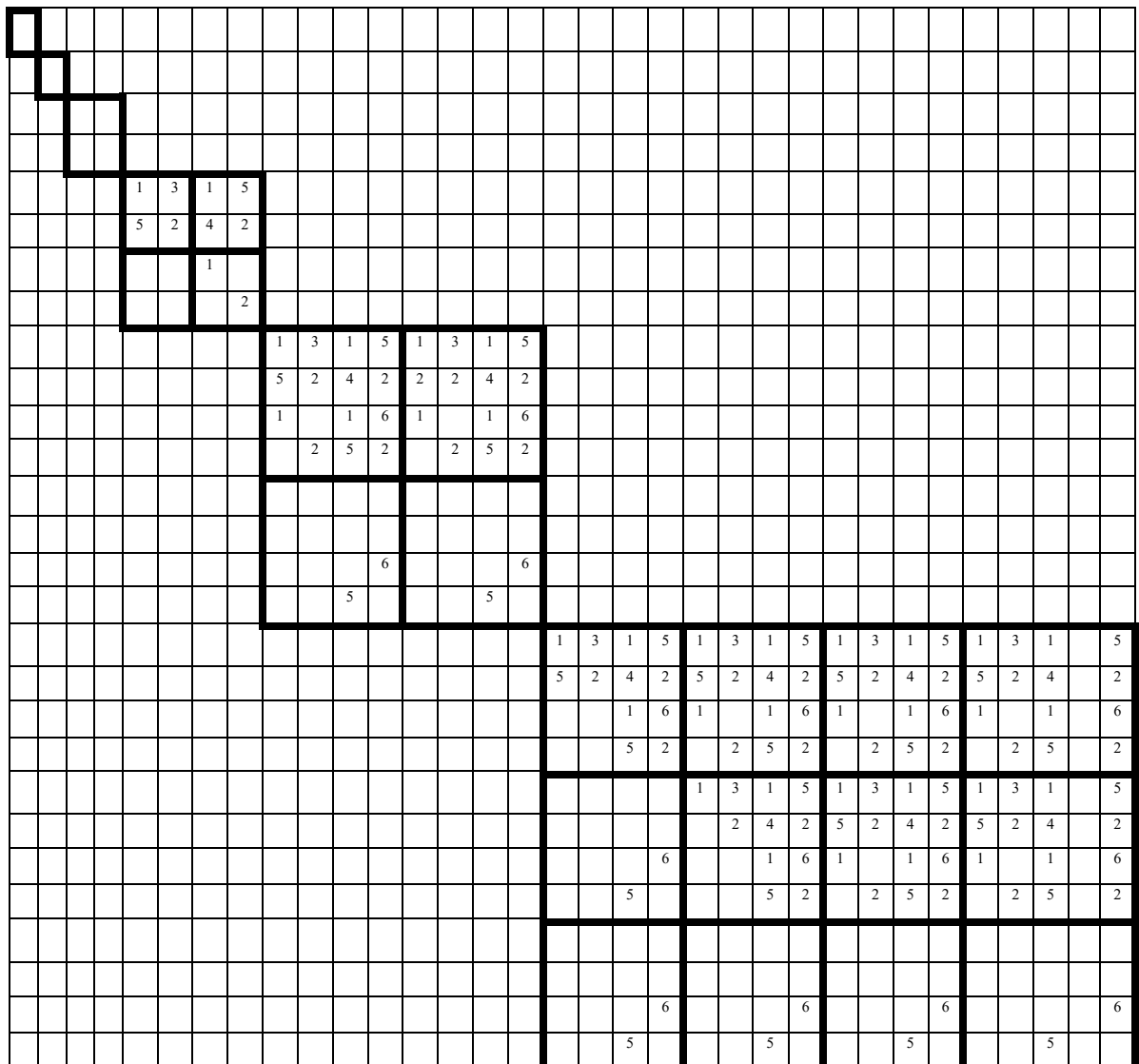
1. Сформувані коефіцієнти при елементах матриці з парними індексами (отримувані з коефіцієнтів попередньої матриці восьмого порядку подвоєнням індексів). Це елементи $\mu_{16,16}, \mu_{16,18}, \mu_{16,20}, \mu_{16,22}, \mu_{16,24}, \mu_{16,26}, \mu_{16,28}, \mu_{16,30}, \mu_{18,18}, \mu_{18,20}, \mu_{18,22}, \mu_{18,24}, \mu_{18,26}, \mu_{18,28}, \mu_{18,30}, \mu_{20,20}, \mu_{20,22}, \mu_{20,24}, \mu_{20,26}, \mu_{20,28}, \mu_{20,30}, \mu_{22,22}, \mu_{22,24}, \mu_{22,26}, \mu_{22,28}, \mu_{22,30}$, які отримуємо «розширенням» з елементів $\mu_{8,8}, \mu_{8,10}, \mu_{8,12}, \mu_{8,14}, \mu_{8,16}, \mu_{8,18}, \mu_{8,20}, \mu_{8,22}, \mu_{8,24}, \mu_{8,26}, \mu_{8,28}, \mu_{8,30}, \mu_{10,10}, \mu_{10,12}, \mu_{10,14}, \mu_{10,16}, \mu_{10,18}, \mu_{10,20}, \mu_{10,22}, \mu_{10,24}, \mu_{10,26}, \mu_{10,28}, \mu_{10,30}, \mu_{12,12}, \mu_{12,14}, \mu_{12,16}, \mu_{12,18}, \mu_{12,20}, \mu_{12,22}, \mu_{12,24}, \mu_{12,26}, \mu_{12,28}, \mu_{12,30}, \mu_{14,14}, \mu_{14,16}, \mu_{14,18}, \mu_{14,20}, \mu_{14,22}, \mu_{14,24}, \mu_{14,26}, \mu_{14,28}, \mu_{14,30}, \mu_{16,16}, \mu_{16,18}, \mu_{16,20}, \mu_{16,22}, \mu_{16,24}, \mu_{16,26}, \mu_{16,28}, \mu_{16,30}$ відповідно.
2. Сформувані елементи діагоналей, до яких належать елементи, сформовані в п. 1. Це $\mu_{17,17}, \mu_{17,19}, \mu_{17,21}, \mu_{17,23}, \mu_{17,25}, \mu_{17,27}, \mu_{17,29}, \mu_{17,31}, \mu_{19,19}, \mu_{19,21}, \mu_{19,23}, \mu_{19,25}, \mu_{19,27}, \mu_{19,29}, \mu_{19,31}, \mu_{21,21}, \mu_{21,23}, \mu_{21,25}, \mu_{21,27}, \mu_{21,29}, \mu_{21,31}, \mu_{23,23}, \mu_{23,25}, \mu_{23,27}, \mu_{23,29}, \mu_{23,31}$, які отримати «приведенням» з елементів $\mu_{16,16}, \mu_{16,18}, \mu_{16,20}, \mu_{16,22}, \mu_{16,24}, \mu_{16,26}, \mu_{16,28}, \mu_{16,30}, \mu_{18,18}, \mu_{18,20}, \mu_{18,22}, \mu_{18,24}, \mu_{18,26}, \mu_{18,28}, \mu_{18,30}, \mu_{20,20}, \mu_{20,22}, \mu_{20,24}, \mu_{20,26}, \mu_{20,28}, \mu_{20,30}, \mu_{22,22}, \mu_{22,24}, \mu_{22,26}, \mu_{22,28}, \mu_{22,30}$ відповідно.
3. Сформувані елементи $\mu_{16,17}, \mu_{16,21}, \mu_{16,25}, \mu_{16,29}, \mu_{20,21}, \mu_{20,25}, \mu_{20,29}$, по елементам попередньої матриці (матриці восьмого порядку), які знаходяться праворуч від елементів з парними індексами, тобто по елементам $\mu_{8,9}, \mu_{8,11}, \mu_{8,13}, \mu_{8,15}, \mu_{10,11}, \mu_{10,13}, \mu_{10,15}$. Ці елементи знайти з відповідних елементів попередньої матриці «розмноженням» та «проріджуванням».
4. Наступні елементи клітин четвертого порядку (які знаходяться в тих самих діагоналях, що й елементи, знайдені в п.3), тобто $\mu_{17,18}, \mu_{17,22}, \mu_{17,26}, \mu_{17,30}, \mu_{21,22}, \mu_{21,26}, \mu_{21,30}$ знайти з елементів $\mu_{16,17}, \mu_{16,21}, \mu_{16,25}, \mu_{16,29}, \mu_{20,21}, \mu_{20,25}, \mu_{20,29}$ «приведенням» у два кроки.
5. Елементи $\mu_{16,17+2}, \mu_{16,21+2}, \mu_{16,25+2}, \mu_{16,29+2}, \mu_{20,21+2}, \mu_{20,25+2}, \mu_{20,29+2}$ мають знаки коефіцієнтів перед відліками протилежні до відповідних $\mu_{17,18}, \mu_{17,22}, \mu_{17,26}, \mu_{17,30}, \mu_{21,22}, \mu_{21,26}, \mu_{21,30}$.

6. Прикінцеві коефіцієнти елементів клітин четвертого порядку (треті елементи других діагоналей) $\mu_{18,19}$, $\mu_{18,23}$, $\mu_{18,27}$, $\mu_{18,31}$, $\mu_{22,23}$, $\mu_{22,31}$, знайти за елементами $\mu_{16,16}$, $\mu_{16,20}$, $\mu_{16,24}$, $\mu_{16,28}$, $\mu_{20,20}$, $\mu_{20,28}$ шляхом «проріджування» та «приведення» за два кроки.
7. Усі інші інші коефіцієнти елементів знайти, враховуючи симетрію (з точністю до знаку) елементів матриці.

На рис.2.4 проілюстровано алгоритм формування коефіцієнтів μ_{ij} матриці $\bar{G}_\xi$ для матриці 32-го порядку.

Всі операції, які були введені в роботі позначені на рисунку наступним чином:

1 – операція «розширення», 2 – операція «приведення», 3 – операція «розширення з проріджуванням», 4 – операція «приведення в два кроки», 5 – операція «інверсія», 6 – операція «проріджування в два кроки».



β_3		β_3	β_2	β_1	β_0	β_1	β_2
β_2	β_3		β_3	β_2	β_1	β_0	β_1
β_1	β_2	β_3		β_3	β_2	β_1	β_0

Порівнюючи тепер (2.77) та (2.71a), можна знайти коефіцієнти при β_k . Так, β_0 займає в (2.77) ті ж самі позиції, що й g_0 в (2.71a), β_1 займає ті ж позиції, що й g_1 та g_7 ; β_2 — ті ж самі позиції, що й g_2 та g_6 , а β_3 — ті ж позиції, що й g_3 та g_5 і т. д. Тому для визначення коефіцієнтів γ_{ij} при β_k слід підсумувати коефіцієнти μ_{ij} при відліках імпульсної характеристики. Так, при форматі імпульсної характеристики 8 з вищенаведених формул для μ_{ij} отримаємо елементи матриці $\bar{\bar{G}}_{2Had}$ (порядку $N \geq 16$):

$$\theta_{0,0} = \beta_0 + 2\beta_1 + 2\beta_2 + 2\beta_3 + 2\beta_4 + 2\beta_5 + 2\beta_6 + 2\beta_7;$$

$$\theta_{1,1} = \beta_0 - 2\beta_1 + 2\beta_2 - 2\beta_3 + 2\beta_4 - 2\beta_5 + 2\beta_6 - 2\beta_7;$$

$$\theta_{2,2} = \theta_{3,3} = \beta_0 + 0 - 2\beta_2 + 0 + 2\beta_4 + 0 - 2\beta_6 + 0; \theta_{2,3} = \theta_{3,2} = 0;$$

$$\theta_{4,4} = \theta_{6,6} = \beta_0 + \beta_1 + 0 - \beta_3 - 2\beta_4 - \beta_5 + 0 + \beta_7;$$

$$\theta_{4,5} = \theta_{5,4} = \theta_{6,7} = \theta_{7,6} = \theta_{4,6} = \theta_{6,4} = \theta_{5,7} = \theta_{7,5} = 0;$$

$$\theta_{5,5} = \theta_{7,7} = 0 - \beta_1 + 0 + \beta_3 - 2\beta_4 + \beta_5 + 0 - \beta_7$$

і т. д. Аналогічно знаходимо елементи матриці $\bar{\bar{C}}_{2Had}$.

Запропонований алгоритм формування матриць $\bar{\bar{G}}_{2Had}$ та $\bar{\bar{G}}_{Had}$ слід віднести до символічних, що дозволяє значно зекономити час на проведення обчислень за сформованими коефіцієнтами при відліках g_i імпульсної характеристики деградації та перед коефіцієнтами β_{ij} добутків цих коефіцієнтів. Враховуючи обмежену довжину імпульсної характеристики деградації коефіцієнти μ_{ij} та $\theta_{i,j}$ можна згенерувати один раз, і для різних імпульсних характеристик підставленням значень g_i одразу ж отримати матриці $\bar{\bar{G}}_{2Had}$ та $\bar{\bar{G}}_{Had}$.

Наявність при обчисленнях матриць $\bar{\bar{G}}_{2Had}$ та $\bar{\bar{G}}_{Had}$ чисельними методами спряжене з великою кількістю операції додавань та віднімань тих самих виразів призводить до накопичення великої похибки. Символьний

алгоритм є вільним від цього недоліку.

Формування матриці $\bar{\bar{G}}_{2Had}$ не є самоціллю. Для реставрації образу необхідно знайти обернену матрицю $\left[\bar{\bar{G}}_{2Had} + \frac{1}{\lambda} \cdot \bar{\bar{c}}_{2Had} \right]$ в (2.69) при різних значеннях коефіцієнта варіації λ .

2.8.4 Обернення матриці для реалізації алгоритму реставрації

Матриці $\bar{\bar{G}}$, $\bar{\bar{c}}$ є циркулянтними, що й забезпечує блочно-діагональний вигляд матриць $\bar{\bar{G}}_{2Had}$, $\bar{\bar{c}}_{2Had}$, $\bar{\bar{G}}_{1Had}$ та діагональний вигляд матриць перетворення Фур'є $\bar{\bar{G}}_{2F}$, $\bar{\bar{c}}_{2F}$ від $\bar{\bar{G}}$, $\bar{\bar{c}}$.

Так, нормований (діленням кожного рядка матричного оператора $\bar{\bar{F}}$ на $\sqrt{N}$) матричний оператор Фур'є $\bar{\bar{F}}_H$ можна представити у вигляді добутку двох матричних операторів

$$\bar{\bar{F}}_H = \bar{\bar{P}}^T \cdot \bar{\bar{Had}}; \bar{\bar{F}}_H^* = \bar{\bar{Had}}^T \cdot \bar{\bar{P}}^*, \quad (2.78)$$

де $\bar{\bar{Had}}$ — нормований матричний оператор дискретного перетворення Адамара; $\bar{\bar{P}}^T$ — нормований матричний оператор кратного ортогонального перетворення; * — знак комплексного спряження. З (2.78) отримуємо

$$\bar{\bar{P}}^T = \bar{\bar{F}}_H \cdot \bar{\bar{Had}}^T; \bar{\bar{P}}^* = \bar{\bar{Had}} \cdot \bar{\bar{F}}_H^*; \bar{\bar{P}}^T \cdot \bar{\bar{P}}^* = \bar{\bar{P}}^* \cdot \bar{\bar{P}}^T = \bar{\bar{E}}, \quad (2.79)$$

де $\bar{\bar{E}}$ — одинична матриця.

Для того, щоб розробити алгоритм приведення матриці $\bar{\bar{P}}^T$ до блочно-діагонального виду, потрібно враховувати відповідність номерів елементів в рядку матриці Адамара з номерами елементів матриці Фур'є.

Для прикладу приведемо порядок номерів елементів матриць, коли їх порядок N дорівнює 4, 8 і 16.

$N = 4$

$\bar{\bar{Had}}$	$\bar{\bar{F}}$	алгоритм
-------------------	-----------------	----------

0	0	
1	2	2^1
2	1	2^0
3	3	3×1

$N = 8$

$\overline{\overline{Had}}$	$\overline{\overline{F}}$	алгоритм
0	0	
1	4	2^2
2	2	2^1
3	6	3×2
4	1	2^0
5	3	3×1
6	5	5×1
7	7	7×1

$N = 16$

$\overline{\overline{Had}}$	$\overline{\overline{F}}$	алгоритм
0	0	
1	8	2^3
2	4	2^2
3	12	3×4
4	2	2^1
5	6	3×2
6	10	5×2
7	14	7×2
8	1	2^0
9	3	3×1
10	5	5×1
11	7	7×1
12	9	9×1
13	11	11×1
14	13	13×1
15	15	15×1

	0		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0																																	
1																																	
2																																	
3																																	
4																																	
5																																	
6																																	
7																																	
8																																	
9																																	
10																																	
11																																	
12																																	
13																																	
14																																	
15																																	
16																																	
17																																	
18																																	
19																																	
20																																	
21																																	
22																																	
23																																	
24																																	
25																																	
26																																	
27																																	
28																																	
29																																	
30																																	
31																																	

Рис.2.5 Матрица $\bar{\bar{P}}$ 32-го порядку ($\bar{\bar{P}} = \bar{\bar{F}}_n \times \bar{\bar{H}}\bar{\bar{a}}\bar{\bar{d}}^T$)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0																																
1																																
2																																
3																																
4																																
5																																
6																																
7																																
8																																
9																																
10																																
11																																
12																																
13																																
14																																
15																																
16																																
17																																
18																																
19																																
20																																
21																																
22																																
23																																
24																																
25																																
26																																
27																																
28																																
29																																
30																																
31																																

Рис.2.6 Матриця $\bar{P}$ 32-го порядку, після перестановки елементів в рядках

Для формування елементів матриці $\bar{\bar{P}}$ знаходяться символічні залежності, після чого, для достатньо прозорих і легко програмованих для безпосереднього формування матриць $\bar{\bar{G}}_{2Had}$, $\bar{\bar{c}}_{2Had}$, знайти символічні залежності добутків

$$\bar{\bar{D}} = \bar{\bar{P}}^T \cdot \bar{\bar{G}}_{2Had} \cdot \bar{\bar{P}}^* \quad (2.80)$$

які мають вигляд діагональних матриць (зручних і для обернення в символічному вигляді), не буде складно.

Результат обчислення матриці $\bar{\bar{P}}^T$ має просту блочно-діагональну структуру (як видно з рис.2.5), що дозволяє у подальшому в символічному вигляді реалізувати обчислення за виразом (2.69).

Покажемо це на прикладі підматриць-блоків діагоналі невисоких порядків. Так, перший блок діагоналі (з номерами рядків та стовпців 0,0) має елемент, що дорівнює 1. Другий елемент діагоналі (з номерами рядків та стовпців 1,1) теж дорівнює 1. Відзначене вірно, якщо порядок матриці $\bar{\bar{P}}^T$ дорівнює двом. Якщо порядок матриці $\bar{\bar{P}}^T$ дорівнює чотирьом, другий елемент діагоналі буде в першому рядку, але вже в другому стовпці (з номером 2). Для матриці восьмого порядку елемент першого рядка знаходиться вже в $(2 \cdot 2 = 4)$ в стовпці з номером 4 і т.д. Третій елемент діагоналі — це матриця другого порядку, яка має вигляд (якщо порядок матриці $\bar{\bar{P}}^T$ дорівнює чотирьом)

$$\bar{\bar{P}}^T_{(2,3),(1,3)} = \cos \pi/4 \cdot \begin{bmatrix} e^{-j\pi/4} & e^{j\pi/4} \\ e^{j\pi/4} & e^{-j\pi/4} \end{bmatrix},$$

тобто в цьому випадку ненульові елементи 2, 3 рядків знаходяться в стовпцях 1, 3. Якщо порядок матриці збільшити вдвічі, то номери стовпців теж збільшаться вдвічі (2, 6). Тому у подальшому будемо наводити мінімальні значення номерів стовпців, що відповідає випадку, коли відповідні рядки мають номери, максимальні для даного формату матриці $\bar{\bar{P}}^T$.

Так підматриця четвертого порядку

$$\bar{P}^T_{(4\dots 7),(1,3,5,7)} = \cos \pi/4 \cdot \quad (2.81)$$

$$\begin{bmatrix} \cos \pi/8 \cdot e^{-j3\pi/8} & \cos 3\pi/8 \cdot e^{-j\pi/8} & \cos 3\pi/8 \cdot e^{j\pi/8} & \cos \pi/8 \cdot e^{j3\pi/8} \\ j \sin \pi/8 \cdot e^{-j3\pi/8} & j \sin 3\pi/8 \cdot e^{-j\pi/8} & -j \sin 3\pi/8 \cdot e^{j\pi/8} & -j \sin \pi/8 \cdot e^{j3\pi/8} \\ j \cos \pi/8 \cdot e^{-j3\pi/8} & j \cos 3\pi/8 \cdot e^{-j\pi/8} & -j \cos 3\pi/8 \cdot e^{j\pi/8} & -j \cos \pi/8 \cdot e^{j3\pi/8} \\ -\sin \pi/8 \cdot e^{-j3\pi/8} & -\sin 3\pi/8 \cdot e^{-j\pi/8} & -\sin 3\pi/8 \cdot e^{j\pi/8} & -\sin \pi/8 \cdot e^{j3\pi/8} \end{bmatrix}.$$

Аналогічно, підматриця восьмого порядку має елементи першого рядка (множник $\cos \pi/4$ винесено за знак матриці)

$$\begin{aligned} p_{8,1} &= \cos \pi/16 \cdot \cos 2\pi/16 \cdot e^{-j7\pi/16}; & p_{8,3} &= \cos 3\pi/16 \cdot \cos 6\pi/16 \cdot e^{-j5\pi/16}; \\ p_{8,5} &= -\cos 5\pi/16 \cdot \cos 10\pi/16 \cdot e^{-j3\pi/16}; & p_{8,7} &= -\cos 7\pi/16 \cdot \cos 13\pi/16 \cdot e^{-j\pi/16}; \\ p_{8,9} &= p_{8,7}^*; & p_{8,11} &= p_{8,5}^*; & p_{8,13} &= p_{8,3}^*; & p_{8,15} &= p_{8,1}^*. \end{aligned}$$

Елементи першого стовпця (починаючи з $p_{9,1}$)

$$\begin{aligned} p_{9,1} &= j \sin \pi/16 \cdot \cos 2\pi/16 \cdot e^{-j7\pi/16}; \\ p_{10,1} &= j \cos \pi/16 \cdot \sin 2\pi/16 \cdot e^{-j7\pi/16}; \\ p_{11,1} &= -\sin \pi/16 \cdot \sin 2\pi/16 \cdot e^{-j7\pi/16}; \\ p_{12,1} &= j \cos \pi/16 \cdot \cos 2\pi/16 \cdot e^{-j7\pi/16}; \\ p_{13,1} &= -\sin \pi/16 \cdot \cos 2\pi/16 \cdot e^{-j7\pi/16}; \\ p_{14,1} &= -\cos \pi/16 \cdot \sin 2\pi/16 \cdot e^{-j7\pi/16}; \\ p_{15,1} &= -j \sin \pi/16 \cdot \sin 2\pi/16 \cdot e^{-j7\pi/16}. \end{aligned}$$

Усі елементи кожного з рядків (8...15) мають ті самі функції, що й перший елемент рядка, але їх аргументи відповідно $\pi/16, 2\pi/16; 3\pi/16, 6\pi/16; 5\pi/16, 10\pi/16; 7\pi/16, 14\pi/16; 9\pi/16, 18\pi/16; 11\pi/16, 22\pi/16; 13\pi/16, 26\pi/16; 15\pi/16, 30\pi/16$. Знаки перед функціями отримуємо множенням знака (1, -1, j, -j) перед елементом першого стовпця на 1, 1, -1, -1, -1, -1, 1, 1, а аргументи при експоненті змінюються від $-j7\pi/16$ (з кроком $2\pi/16$) до $+j7\pi/16$. Знаки перед функціями першого стовпця для перших двох рядків 1 та j відповідно, а для другої пари рядків утворюються множенням першої пари на j. Тригонометричні функції вздовж по стовпцю змінюються наступним чином. Множник з найменшим

аргументом ($\pi/16$) послідовно вздовж стовпця, починаючи з $\cos \pi/16$ міняється на $\sin \pi/16$, знову на $\cos \pi/16$ і т.д. Множник з подвоєним аргументом є функцією, яка повторюється двічі вздовж стовпця, тобто $\cos \pi/16, \cos \pi/16, \sin \pi/16, \sin \pi/16, \cos \pi/16, \cos \pi/16$ і т.д.

Аналогічно, для матриці $\bar{P}^T$ 32-го порядку матриця $\bar{P}^T_{(16...31),(1,3,5,7,9,11,13,15,...31)}$ формується безпосередньо за знайденими вище закономірностями (номери стовпців ненульових елементів, обчислені для матриці вдвічі меншого формату подвоюються). Для цього побудуємо перший елемент першого стовпця додаткової (для подвоєного формату), множник $\cos \pi/4$ виносимо за знак матриці

$$p_{16,1} = \cos \pi/32 \cdot \cos 2\pi/32 \cdot \cos 4\pi/32 e^{-j15\pi/32}.$$

Далі вздовж кожного з рядків аргументи перших множників добутку тригонометричних функцій мають в чисельниках множники перед π , які дорівнюють 3, 5, 7, ... $N/2-1$, $N/2-1, \dots, 7, 5, 3, 1$. Друга тригонометрична функція в добутку має подвоєний аргумент, третя — помножений на 4 і т.д. Експоненти мають аргументи, починаючи від $-(N/2-1)$, які зростають з кроком $2\pi/N$ до значення $+(N/2-1)$, де N — порядок матриці $\bar{P}^T$ (в даному випадку $N=32$). Знаки перед добутком тригонометричних функцій вздовж рядка до стовпця з номером $N/2-1$ змінюються наступним чином: $+1, +1, -1, -1, +1, +1, -1, -1, \dots$ і т.д. Починаючи зі стовпця з номером $N/2$, усі множники слід замінити на протилежні. Ці знаки (вздовж рядка) слід для різних рядків (вздовж стовпця) помножити на 1, j (перша пара рядків) наступну пару рядків слід помножити на $j, -1$, (що відповідає множенню першої пари знаків на j). Отриману четвірку знаків слід помножити на j і отримати множники $j, -1, -1, -j$. Отриману вісімку знаків слід знову помножити на j і т.д. Тригонометричні функції вздовж кожного стовпця чередуються наступним чином. Функції з мінімальним аргументом чередуються за кожним кроком, тобто якщо в першому рядку підматриці першим множником

є функція $\cos(2n - 1)/N$, то наступною є $\sin(2n - 1)/N$, а потім знову $\cos(2n - 1)/N$. Функції, починаючи з $\cos 2(2n - 1)/N$ чередуються що два кроки, а функції, починаючи з $\cos 4(2n - 1)/N$ — що чотири кроки і т.д.

Отже, запропонований символічний алгоритм формування матриці $\bar{P}^T$ є достатньо простим. Переставленням стовпців матриця $\bar{P}^T$ зводиться до блочно-діагональної. Тоді кожен блок діагоналі цієї матриці та спряженої транспонованої можна множити праворуч та ліворуч на відповідний до нього блок діагоналі матриць $\bar{G}_{2Nad}$, $\bar{C}_{2Nad}$, $\bar{G}_{1Nad}$. Результатом такого множення буде діагональна підматриця.

Для приведення матриці $\bar{P}^T$ до блочно-діагонального виду в програмному середовищі MatLab був написаний цикл, за допомогою якого можна швидко формувати матриці високих порядків.

Розглянемо тепер можливості безпосереднього формування елементів діагональної матриці $\bar{D}$.

2.8.5 Обчислення діагональної матриці

Оскільки добуток (2.78) дає діагональну матрицю, то у подальшому будемо обчислювати лише діагональні елементи. Обчислення діагональних елементів $d_{i,i}$ матриці $\bar{D}$ для кожного блока діагоналі можна організувати за виразом

$$d_{i,i} = [1]^T \cdot \{(\bar{P}_i^* \cdot \bar{P}_i^T) \odot \bar{G}_{2Nad\text{блока}}\} \cdot [1] \quad (2.82)$$

де $\bar{P}_i^*$, $\bar{P}_i^T$ — i -ті стовпець та рядок відповідних блоків матриць $\bar{P}^*$ та $\bar{P}$; T — знак транспонування; $\odot$ — знак множення, такого, при якому кожен елемент матриці $\bar{P}_i^* \cdot \bar{P}_i^T$ множиться на відповідний йому елемент матриці $\bar{G}_{2Nad\text{блока}}$; $*$ — знак комплексного спряження; $[1]$ — стовпець одиниць.

Так, для підматриць другого четвертого порядку (2.79), матимемо для першого діагонального елемента

$$\begin{aligned} \bar{P}_1^* \cdot \bar{P}_1^T &= [\cos \pi/8 \cdot e^{j3\pi/8} - j \sin \pi/8 \cdot e^{j3\pi/8} - j \cos \pi/8 \cdot e^{j3\pi/8} - \sin \pi/8 \cdot \\ &e^{j3\pi/8}]^T \cdot [\cos \pi/8 \cdot e^{-j3\pi/8} \quad j \sin \pi/8 \cdot e^{-j3\pi/8} \quad j \cos \pi/8 \cdot e^{-j3\pi/8} \quad -\sin \pi/8 \cdot \\ &e^{-j3\pi/8}] = \\ &\begin{bmatrix} \cos \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & j \cos \frac{\pi}{8} \cdot \sin \frac{\pi}{8} & j \cos \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & -\cos \frac{\pi}{8} \cdot \sin \frac{\pi}{8} \\ -j \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & \sin \frac{\pi}{8} \cdot \sin \frac{\pi}{8} & \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & -j \sin \frac{\pi}{8} \cdot \sin \frac{\pi}{8} \\ -j \cos \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & \cos \frac{\pi}{8} \cdot \sin \frac{\pi}{8} & \cos \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & j \cos \frac{\pi}{8} \cdot \sin \frac{\pi}{8} \\ -\sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & -j \sin \frac{\pi}{8} \cdot \sin \frac{\pi}{8} & -j \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} & \sin \frac{\pi}{8} \cdot \sin \frac{\pi}{8} \end{bmatrix}. \end{aligned} \quad (2.83)$$

Оскільки для блока $\bar{\bar{G}}_{2Надблока}$ (2.82) елементи $G_{1,2}, G_{1,3}, G_{2,1}, G_{3,1}, G_{2,4}, G_{3,4}, G_{4,2}, G_{4,3}$ дорівнюють нулю, матрицю (2.82) можна записати у вигляді

$$\begin{bmatrix} \cos \pi/8 \cdot \cos \pi/8 & 0 & 0 & -\cos \pi/8 \cdot \sin \pi/8 \\ 0 & \sin \pi/8 \cdot \sin \pi/8 & \sin \pi/8 \cdot \cos \pi/8 & 0 \\ 0 & \cos \pi/8 \cdot \sin \pi/8 & \cos \pi/8 \cdot \cos \pi/8 & 0 \\ -\sin \pi/8 \cdot \cos \pi/8 & 0 & 0 & \sin \pi/8 \cdot \sin \pi/8 \end{bmatrix}. \quad (2.84)$$

Нехай для визначеності імпульсну характеристику деградації образу описано вісімкою дискретних відліків g_i , тоді, блок четвертого порядку матриці $\bar{\bar{G}}_{2H}$ має вигляд

$$\bar{\bar{G}}_{2Надблока} = \begin{bmatrix} G_{1,1} & 0 & 0 & -G_{1,4} \\ 0 & G_{2,2} & G_{1,4} & 0 \\ 0 & G_{1,4} & G_{1,1} & 0 \\ -G_{1,4} & 0 & 0 & G_{2,2} \end{bmatrix}, \quad (2.82)$$

де $G_{1,1} = \beta_0 + \beta_1 + 0 - \beta_3 - 2\beta_4 - \beta_5 + 0 + \beta_7$;

$G_{2,2} = \beta_0 - \beta_1 + 0 + \beta_3 - 2\beta_4 + \beta_5 + 0 - \beta_7$;

$G_{1,4} = 0 + \beta_1 + 0 - \beta_3 + 0 - \beta_5 + 0 + \beta_7$,

причому $\beta_0 = \sum_{k=0}^{S-1} g_k^2$; $\beta_1 = \sum_{k=0}^{S-2} g_k \cdot g_{k+1}$; $\beta_2 = \sum_{k=0}^{S-3} g_k \cdot g_{k+2}$; $\dots$ $\sum_{k=0}^0 g_k \cdot g_{S-1} = g_k \cdot g_{S-1}$; $S \leq N$ [73,74].

Тоді результат обчислень за виразом (3.17) має вигляд

$d_{1,1} = \beta_0 + \sqrt{2} \cdot \beta_1 + 0 - \sqrt{2} \cdot \beta_3 - \beta_4 - \sqrt{2} \cdot \beta_5 + 0 + \sqrt{2} \cdot \beta_7$;

$$d_{4,4} = d_{1,1}; d_{3,3} = \beta_0 + 0 + 0 + 0 - 2\beta_4 + 0 + 0 + 0; d_{2,2} = d_{3,3} \text{ і т.д.}$$

Аналогічно, для матриці восьмого порядку.

Висновки до розділу

1. Задача реставрації образів (одновимірних та двовимірних) має велике значення в сучасній техніці, медицині тощо. Ця задача в математичному плані відноситься до некоректних математичних задач (тобто таких, які, якщо мають розв'язок, то мають їх велику кількість). Тому її розв'язання базується на використанні апріорної інформації про реставрований образ.

2. Реставрація за об'єктивним критерієм полягає на використанні наперед заданого критерію співпадіння реставрованого образу з дійсним зображенням. Об'єктивні критерії обираються з ряду відомих критеріїв суб'єктивно. Тому порівняння результатів реставрації різними методами повинно виконуватися за єдиним обраним об'єктивним критерієм.

3. Серед існуючих на наш час методів реставрації образів на фоні адитивного шуму найбільш простими, але і достатньо ефективними є методи, основані на використанні ортогональних перетворень.

4. Метод умовної деконволюції оснований на використанні інформації тільки про одну реалізацію образу і про енергію адитивного шуму, яка також може бути оцінена по тій самій реалізації образу. При цьому реставрація образу в натуральних координатах приводить до громіздких матричних рівнянь, розв'язання яких вимагає ПЕОМ надзвичайно високої продуктивності та швидкодії. Саме тому більш прийнятним є розв'язання задачі реставрації в області перетворення Фур'є.

5. Дискретне перетворення Фур'є має певні недоліки, які можуть впливати на

якість отриманого реставрованого образу, які полягають в обмеженій кількості трансформант перетворення, що призводить до виникнення ефекту Гібса («розмивання» границь графоелементів).

6. Вільними від ефекту Гібса (хоча і зі спотвореннями іншого характеру, але за рахунок обмеженої розрядності операндів) є методи, основані на використанні функцій Уолша–Адамара, Хаара і т.д. Тому актуальним є створення алгоритмів реставрації образів з використанням таких ортогональних перетворень.

7. Отримано вираз для обчислення спектру Адамара реставрованого за методом умовної деконволюції одновимірному сигналу (образу). Безпосередні обчислення за наведеними матричними операторами спряжені з впливом на точність дублікацій (додавання та віднімання в процесі обчислень однакових виразів), що приводить до складностей (мала швидкодія, накопичення операційної похибки) при формуванні відповідних матричних операторів.

8. Матриця деградації образу є блочно-діагональною (з порядком найбільшого блоку $N/2$, де N — порядок матриці деградації), тому задача обернення матриці є так само складною, як і в випадку реставрації в натуральних координатах.

9. Використання символьних залежностей при формуванні матриці G_{2N}^{-1} потребує мінімально можливої кількості операцій множення та додавання, дозволяє ліквідувати вплив дублікацій.

10. Використання інформації про жорстку структуру одержуваних матриць довільного порядку дозволяє обчислювати лише їх ненульові елементи, що значно зменшує кількість арифметичних операцій, усуває дублювання, які виникають при безпосередньому перемноженню матриць перемноженні матриць.

11. Використання операторів кратного перетворення дозволяє значно спростити задачу обернення матриці при реставрації образу приведенням її до діагонального вигляду.

З ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА ДЛЯ БОРОТЬБИ З АКТИВНИМИ СТЕГANOГРАФІЧНИМИ АТАКАМИ

Стеганографічні атаки передбачають навмисне спотворення сигналу або зображення для приховування інформації. Метод умовної деконволюції в базисі перетворення Адамара може бути використаний для виявлення і усунення таких спотворень. Ось як можна реалізувати цей метод для боротьби з активними стеганографічними атаками.

Загальна схема:

1. Перетворення зображення або сигналу в базис Адамара.
2. Аналіз спектру Адамара для виявлення аномалій.
3. Застосування умовної деконволюції для відновлення оригінального сигналу.
4. Зворотне перетворення в часову область або простір зображення.

Приклад реалізації на Python:

```
1. Завантаження і попередня обробка зображення
import numpy as np
import matplotlib.pyplot as plt
from scipy.linalg import hadamard
from scipy.ndimage import convolve
def load_image(path):
    from PIL import Image
    img = Image.open(path).convert('L')
    img = np.array(img)
    return img
def normalize_image(image):
```

```

return image / 255.0

image_path = 'path_to_image.png'
image = load_image(image_path)
image = normalize_image(image)
plt.imshow(image, cmap='gray')
plt.title("Original Image")
plt.show()

```

Цей код завантажує зображення з вказаного шляху, конвертує його в чорно-біле зображення, нормалізує його значення пікселів і відображає його за допомогою бібліотеки `matplotlib`.

Спочатку у коді імпортуються потрібні бібліотеки: `numpy` для роботи з масивами, `matplotlib.pyplot` для візуалізації даних, `scipy.linalg` для генерації матриці Гадамарда та `scipy.ndimage` для згладжування зображення.

Далі визначається функція `load_image(path)`, яка завантажує зображення з вказаного шляху, конвертує його в тони сірого і повертає його у вигляді масиву `numpy`.

Наступна функція `normalize_image(image)` нормалізує значення пікселів зображення, діленням на 255.

Вказується шлях до зображення `image_path`.

Завантажується зображення за допомогою функції `load_image(image_path)`.

Нормалізуються значення пікселів зображення викликом `normalize_image(image)`.

Зображення відображається за допомогою `plt.imshow()`, вказується колірна карта `'gray'` для відображення чорно-білого зображення, задається заголовок і викликається `plt.show()` для відображення зображення.

Отже, цей код завантажує, обробляє і відображує чорно-біле зображення.

2. Перетворення Адамара

```
def hadamard_transform_2d(image):
```



```

H = hadamard(image.shape[0])
return H @ image @ H
def inverse_hadamard_transform_2d(transformed_image):
H = hadamard(transformed_image.shape[0])
return H @ transformed_image @ H / (transformed_image.shape[0] ** 2)
transformed_image = hadamard_transform_2d(image)
plt.imshow(np.log1p(np.abs(transformed_image)), cmap='gray')
plt.title("Hadamard Transformed Image")
plt.show()

```

Функція `hadamard_transform_2d` приймає на вхід зображення і виконує двовимірне перетворення Хадамара. Вона створює матрицю Хадамара, потім множить зображення на неї з обох сторін і повертає перетворене зображення.

Функція `inverse_hadamard_transform_2d` приймає на вхід перетворене зображення і виконує зворотнє двовимірне перетворення Хадамара. Вона також створює матрицю Адамара, потім множить перетворене зображення на неї з обох сторін і ділить на квадрат розміру перетвореного зображення.

Після цього код виконує перетворення Адамара для зображення і виводить логарифмоване абсолютне значення перетвореного зображення за допомогою функції `plt.imshow`.

3. Виявлення аномалій та умовна деконволюція

```

def detect_anomalies(transformed_image, threshold):
anomalies = np.abs(transformed_image) > threshold
return anomalies

def conditional_deconvolution_2d(transformed_image, anomalies,
regularization_param):
corrected_transform = np.copy(transformed_image)
corrected_transform[anomalies] /= regularization_param
return corrected_transform

```

```

anomalies = detect_anomalies(transformed_image, threshold=10)
regularization_param = 0.1
corrected_transform =
conditional_deconvolution_2d(transformed_image, anomalies,
regularization_param)
plt.imshow(np.log1p(np.abs(corrected_transform)), cmap='gray')
plt.title("Corrected Hadamard Transformed Image")
plt.show()

```

Функція `detect_anomalies` приймає трансформоване зображення та порогове значення як вхідні дані. Вона ідентифікує аномалії в трансформованому зображенні шляхом порівняння абсолютних значень пікселів з пороговим значенням і повертає масив аномалій.

Функція `conditional_deconvolution_2d` приймає трансформоване зображення, масив аномалій та параметр регуляризації як вхідні дані. Вона створює копію трансформованого зображення, потім коригує значення пікселів відповідно до масиву аномалій шляхом ділення на параметр регуляризації та повертає скориговане трансформоване зображення.

Потім створюється масив аномалій за допомогою функції `detect_anomalies` з трансформованим зображенням та пороговим значенням. Встановлюється параметр регуляризації.

Потім викликається функція `conditional_deconvolution_2d` з трансформованим зображенням, масивом аномалій та параметром регуляризації, і результат записується в змінну `corrected_transform`.

І, нарешті, викликається функція `plt.imshow` для відображення логарифма абсолютних значень скоригованого трансформованого зображення із кольоровою мапою 'сірий' та заголовком "Виправлене трансформоване зображення Адамара".

4. Зворотне перетворення в часову область

```

restored_image = inverse_hadamard_transform_2d(corrected_transform)
plt.imshow(restored_image, cmap='gray')
plt.title("Restored Image")
plt.show()

restored_image = inverse_hadamard_transform_2d(corrected_transform)

```

Цей код виконує зворотнє перетворення Гадамара над скоригованим зображенням або даними, які були піддані перетворенню Гадамара. Результатом є відновлене зображення після застосування зворотного перетворення.

`plt.imshow(restored_image, cmap='gray')` - цей код відображає відновлене зображення на графіку з використанням сірої кольорової карти.

`plt.title("Restored Image")` - задає заголовок для графіку, який відображається як "Відновлене зображення".

`plt.show()` - показує графік з відновленим зображенням. Таким чином, цей код використовується для візуалізації відновленого зображення після застосування зворотного перетворення Гадамара до скоригованих даних.

Висновки до розділу

Метод умовної деконволюції в базисі перетворення Адамара може бути ефективним інструментом для боротьби зі стеганографічними атаками, які спотворюють сигнал або зображення. Використання цього методу дозволяє виявити і усунути такі спотворення, відновлюючи оригінальну інформацію.

4.ЕКОНОМІЧНА ЧАСТИНА МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Магістерська кваліфікаційна робота присвячена вирішенню проблеми підвищення стійкості зображень до спотворень, спричинених активними стеганографічними атаками. Основною метою дослідження є розробка та обґрунтування методів умовної деконволюції у базисі перетворення Адамара для ефективного захисту цифрових зображень.

У рамках роботи проведено аналіз сучасних методів стеганографії та атак на них, визначено основні вразливості існуючих підходів. Запропоновано новий метод умовної деконволюції, який використовує перетворення Адамара, що дозволяє покращити стійкість зображень до атак, зберігаючи при цьому якість переданої інформації.

Економічна частина кваліфікаційної роботи розглядає економічну ефективність виконання частини пошукових робіт, тобто теоретичних та експериментальних досліджень впровадження розроблених методів.

4.1. Проведення наукового аудиту науково-дослідної роботи

Проведення наукового аудиту науково-дослідної роботи є важливим етапом у забезпеченні якості та наукової значимості досліджень. Науковий аудит спрямований на всебічну оцінку наукових результатів, їхньої відповідності поставленим цілям, а також дотримання встановлених методологічних та етичних стандартів.

Аудит забезпечує об'єктивну перевірку достовірності отриманих даних, відповідність методів дослідження сучасним науковим вимогам, а також оцінює

можливості практичного застосування результатів. Важливою складовою наукового аудиту є аналіз ефективності використання ресурсів та витрат, включаючи амортизаційні відрахування на основні засоби, що використовувалися у процесі дослідження.

Метою проведення наукового аудиту є не лише виявлення можливих недоліків чи помилок, але й надання рекомендацій щодо підвищення якості та результативності науково-дослідної роботи. Це дозволяє вдосконалювати дослідницькі процеси, підвищувати їх ефективність та забезпечувати високу наукову цінність проведених досліджень.

Науковий аудит є невід'ємною частиною наукової діяльності, сприяючи збереженню високих стандартів у дослідженнях, підвищенню довіри до отриманих результатів та забезпеченню сталого розвитку наукової сфери [16].

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи

Ступінь новизни	Характеристика ступеня новизни	Ступінь новизни, бали		
		Коротков Сергій Станіславович, доцент кафедри комп'ютерної інженерії ДУІКТ	Замрій Ірина Вікторівна, професор кафедри інженерія програмного забезпечення, ДУІКТ	Савченко Віталій Анатолійович, професор, директор інституту кібербезпеки та захисту інформації, ДУІКТ
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджено або поставлено під	9	8	10

	сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг порівняно з існуючим			
--	--	--	--	--

Таблиця 4.2 – Показники рівня теоретичного опрацювання НДР

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Коротков Сергій Станіслав ович, доцент кафедри комп'ютерної інженерії ДУІКТ	Замрій Ірина Вікторівна, професор кафедри інженерії програмного забезпечення, ДУІКТ	Савченко Віталій Анатолійович, професор, директор інституту кібербезпеки та захисту інформації, ДУІКТ
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	40	45	55

Показник, який характеризує науковий ефект, визначається за формулою:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 9 + 0,4 \cdot 46,7 = 24,1$$

Завдяки традиційному підходу у виконанні досліджень за темою магістерської кваліфікаційної роботи та розробці нового алгоритму та методу вдалося досягти

достатнього рівня показника наукового ефекту [16].

4.2. Розрахунок витрат на здійснення науково-дослідної роботи

4.2.1. Витрати на оплату праці

Витрати на основну заробітну плату дослідників (Z_o) розраховують відповідно до посадових окладів працівників, за формулою:

$$Z_o = \sum_{i=1}^k \frac{M_{ni} \cdot t_i}{T_p},$$

де k – кількість посад дослідників, залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – кількість днів роботи конкретного дослідника, дн.;

T_p – середня кількість робочих днів в місяці, $T_p = 21 \dots 23$ дні. Проведені розрахунки бажано звести до таблиці.

Таблиця 4.3 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Кількість днів роботи	Витрати на заробітну плату, грн
<i>Керівник проекту</i>	20000	714,28	28	20000
<i>Відповідальний виконавець</i>	12000	428,57	28	12000
<i>Інженер I категорії</i>	9800	350	28	9800
Всього				41800

Інших категорій робітників на етапі досліджень та проведення експериментів не передбачено, тому $Z_p = 0$.

4.2.2. Додаткова заробітна плата дослідників та робітників

Додаткова заробітна плата розраховується як 10 ... 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{\text{дод}} = (З_0 + З_p) \cdot \frac{H_{\text{дод}}}{100\%}$$

де $H_{\text{дод}}$ – норма нарахування додаткової заробітної плати.

$$З_{\text{дод}} = 41800 \cdot \frac{10\%}{100\%} = 4180 \text{ грн}$$

4.2.3. Відрахування на соціальні заходи

До статті «Відрахування на соціальні заходи» належать відрахування внеску на загальнообов'язкове державне соціальне страхування та для здійснення заходів щодо соціального захисту населення (ЄСВ – єдиний соціальний внесок).

Нарахування на заробітну плату дослідників та робітників розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_{\text{н}} = (З_0 + З_p + З_{\text{дод}}) \cdot \frac{H_{\text{зп}}}{100\%}$$

де $H_{\text{зп}}$ – норма нарахування на заробітну плату.

$$З_{\text{н}} = 10115,60 \text{ грн}$$

4.2.4. Витрати на Комплектуючі вироби

Таблиця 4.4 – Витрати на матеріали

Найменування комплектуючих	Ціна за 1 шт, грн	Кількість, шт	Сума, грн
Офісний папір	250	5	1250
Канцелярське приладдя	150	10	1500
Usb-накопичувач	300	3	900
Всього			3650

4.2.5. Програмне забезпечення для наукових (експериментальних) робіт

Для проведення експериментів та отримання результатів моделювання в даній роботі використовується ПЗ Matlab. Вартість однієї ліцензії на одне робоче місце коштує на 4000 грн/рік, для виконання НДР потрібно 1шт ліцензій.

До балансової вартості програмного забезпечення входять витрати на його інсталяцію, тому ці витрати беруться додатково в розмірі 10...12% від вартості програмного забезпечення.

Балансову вартість програмного забезпечення розраховують за формулою:

$$B_{\text{прг}} = \sum_{i=1}^k C_{i\text{прг}} \cdot C_{i\text{прг}} \cdot K_i$$

де $C_{i\text{прг}}$ – ціна придбання одиниці програмного засобу цього виду, грн;

$C_{prg.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1, 10 \dots 1, 12$);

k – кількість найменувань програмних засобів.

Таблиця 4.5 – Витрати на програмне забезпечення

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Matlab	1	4000	4400
Всього			4400

4.2.6. Витрати за статтею «Амортизація обладнання, програмних засобів та приміщень»

Для економічного розрахунку витрат на амортизацію необхідно знати:

Вартість придбання основних засобів.

Нормативний термін експлуатації основних засобів.

Основні засоби

ПК (ноутбук)

Вартість: 20,000 грн

Термін амортизації: 3 роки (36 місяців)

Програмне забезпечення (новопридбане)

Вартість: 4,400 грн

Термін амортизації: 2 роки (24 місяці)

Програмне забезпечення, яке встановлене на ПК (ОС Windows, Прикладний пакет Microsoft Office і т.д.)

Вартість: 30,000 грн

Термін амортизації: 2 роки (24 місяці)

Системний блок

Вартість: 15,000 грн

Термін амортизації: 3 роки (36 місяців)

Монітор

Вартість: 5,000 грн

Термін амортизації: 3 роки (36 місяців)

Метод розрахунку

Для розрахунку амортизаційних відрахувань використовується прямолінійний метод амортизації, за яким вартість основного засобу рівномірно розподіляється на весь нормативний термін його експлуатації.

Формула для розрахунку амортизації на місяць:

$$A = \frac{C}{T},$$

де: А – амортизаційні відрахування на місяць, С – вартість основного засобу, Т – термін амортизації (у місяцях).

Розрахунок амортизаційних відрахувань

ПК (ноутбук)

- Вартість: 20,000 грн
- Термін амортизації: 36 місяців
- Амортизація/місяць
- : $A_{\text{ноутбук}} = 20000 \text{ грн} / 36 \text{ місяців} = 555.56 \text{ грн/місяць}$

Програмне забезпечення (новопридбане - Matlab)

- Вартість: 4,400 грн
- Термін амортизації: 24 місяці
- Амортизація/місяць
- : $A_{\text{нове ПЗ}} = 4400 \text{ грн} / 24 \text{ місяців} = 183,33 \text{ грн/місяць}$

Програмне забезпечення, яке встановлене на ПК (ОС Windows, Прикладний пакет Microsoft Office)

- Вартість: 30,000 грн
- Термін амортизації: 24 місяці
- Амортизація/місяць
- : $A_{\text{встановлене ПЗ}} = 30000 \text{ грн} / 24 \text{ місяців} = 1250.00 \text{ грн/місяць}$

Системний блок

- Вартість: 15,000 грн
- Термін амортизації: 36 місяців
- Амортизація/місяць
- : $A_{\text{системний блок}} = 15000 \text{ грн} / 36 \text{ місяців} = 416.67 \text{ грн/місяць}$
- Вартість: 5,000 грн
- Термін амортизації: 36 місяців
- Амортизація/місяць
- $A_{\text{монітор}} = 5000 \text{ грн} / 36 \text{ місяців} = 138.89 \text{ грн/місяць}$

Загальна сума амортизаційних відрахувань на місяць на одне робоче місце

$$A_{\text{загальна}} = A_{\text{ноутбук}} + A_{\text{нове ПЗ}} + A_{\text{встановлене ПЗ}} + A_{\text{системний блок}} + A_{\text{монітор}} =$$

$$555.56 + 183,33 + 1250.00 + 416.67 + 138.89 = 2544,45 \text{ грн/місяць}$$

Загальна амортизація 1 робочого 2544,45 грн/місяць. Для виконання НДР використовується 3 робочих місця. Тобто сумарні витрати на амортизацію будуть складати 7633,35 грн/місяць

4.2.7. Витрати на електроенергію

Для проведення експериментальних досліджень наукова група використовує 3 шт ПК потужністю 300 Вт та з дисплеєм, потужність якого 40 Вт.

Тариф для юридичних осіб в Київській обл. складає 6.05 грн/кВт з урахуванням ПДВ.

Таблиця 4.6 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Системний блок ПК	1	224	1355,2
Монітор ПК	0,12	224	162,62
Всього			1517,82

Сума витрат на електроенергію спожиту за місяць, приладами, що використовуються в НДР складає 1517,82 грн.

Стаття «Службові відрядження» в даній НДР не передбачена.

Стаття «Витрати на роботи, які виконують сторонні підприємства, установи і організації» в даній НДР не передбачена.

4.2.8. Інші витрати

Витрати за статтею «Інші витрати» розраховуються як 50...100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_{\text{в}} = (Z_{\text{о}} + Z_{\text{р}}) \frac{H_{\text{ів}}}{100\%} = 41800 \cdot 0,5 = 20900 \text{ грн}$$

де $H_{\text{ів}}$ – норма нарахування за статтею «Інші витрати».

4.2.9. Накладні (загальновиробничі) витрати

$$B_{\text{нзв}} = (З_o + З_p) \cdot \frac{H_{\text{нзв}}}{100\%} = 50160 \text{ грн}$$

де $H_{\text{нзв}}=120\%$ (для даної НДР) – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

4.2.10. Витрати на проведення науково-дослідної роботи

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$\begin{aligned} B_{\text{заг}} &= З_o + З_{\text{дод}} + З_n + B_k + B_{\text{прг}} + A_{\text{сумарна}} + B_v + I_v + B_{\text{нзв}} \\ &= 41800 + 4180 + 10115,6 + 3650 + 4400 + 7633,35 + 1517,82 \\ &\quad + 20900 + 50160 = 203802,37 \text{ грн} \end{aligned}$$

4.2.11. Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів

Загальні витрати ЗВ розраховуються за формулою:

$$ЗВ = \frac{B_{\text{заг}}}{\eta} = \frac{203802,37}{0,4} = 509505,93 \text{ грн}$$

Оскільки в НДР здійснено розробку технології (методу), то приймемо $\eta = 0,4$

4.3. Оцінювання важливості та наукової значимості науково-дослідної роботи фундаментального чи пошукового характеру

Комплексний показник K_p розрахований за формулою:

$$K_p = \frac{I^n \cdot T_c \cdot R}{B \cdot t} = \frac{5^3 \cdot 3 \cdot 4}{509,5 \cdot 2} = 1,47$$

$K_p > 1$, науково-дослідну роботу можна вважати ефективною з високим науковим, технічним і економічним рівнями [16].

Висновки до розділу

На підставі проведених економічних розрахунків витрат, враховуючи, що комплексний показник оцінювання важливості та наукової значимості даної науково-дослідної роботи фундаментального чи пошукового характеру перевищує 1, можна зробити наступні висновки:

- Результати науково-дослідної роботи мають високу наукову цінність і значний вплив на розвиток ІТ галузі. Вони сприяють розширенню теоретичних основ і створюють підґрунтя для подальших досліджень і практичних розробок у сфері інформаційної безпеки цифрових зображень.

- Розроблені в НДР методи та алгоритми можуть бути в подальшому впроваджені у практичну діяльність різних підприємств і організацій, що потребують підвищеного рівня захисту цифрових зображень від стеганографічних атак. Це дозволить знизити ризики несанкціонованого доступу та модифікацій даних.

- Висока наукова значимість роботи обґрунтовує необхідність продовження досліджень у даному напрямку. Подальші розробки можуть призвести до ще більш ефективних методів захисту інформації, що підвищить рівень безпеки цифрових систем в цілому.

ВИСНОВКИ

У магістерській дисертаційній роботі вирішена актуальна наукова задача реалізація методу підвищення стійкості зображень до спотворень від активних стенографічних атак шляхом застосування методу умовної деконволюції у базисі перетворення Адамара.

Методи умовної деконволюції в базисі перетворення Адамара пропонують ефективні інструменти для підвищення стійкості зображень до спотворень, спричинених активними стеганографічними атаками. На основі проведеного в магістерській дисертації дослідження і практичної реалізації були зроблені наступні висновки:

- Перетворення Адамара дозволяє ефективно виявляти аномалії у спектральному представленні зображень. Виявлення аномалій в базисі Адамара є ключовим етапом для успішної деконволюції, що дозволяє визначити області з підозрілими спотвореннями.
- Використання регуляризаційного параметру при умовній деконволюції забезпечує стабільність інверсійного процесу. Це особливо важливо в умовах присутності шуму або неточних даних, що може бути наслідком стеганографічних атак.
- Застосування методів умовної деконволюції у базисі перетворення Адамара дозволяє відновлювати зображення з високою точністю, усуваючи значну частину спотворень, спричинених атаками. Це призводить до покращення якості відновлених зображень і забезпечує більш точне, порівняно наприклад з перетворенням Фур'є, відтворення оригінальних даних.
- З використанням в своїй основі блочно-діагональної матриці, перетворення Адамара є менш обчислювально затратним порівняно з іншими

спектральними методами, такими як перетворення Фур'є. Це дозволяє застосовувати методи умовної деконволюції в реальному часі або в умовах обмежених обчислювальних ресурсів.

- Метод умовної деконволюції в базисі перетворення Адамара є гнучким і може бути застосований до різних типів сигналів та зображень. Це робить його універсальним інструментом для широкого спектру задач в області обробки сигналів і зображень.
- Метод умовної деконволюції в базисі перетворення Адамара демонструє високу ефективність у підвищенні стійкості зображень до спотворень від активних стеганографічних атак. Подальший розвиток цього методу та його адаптація до нових викликів може значно покращити захист інформаційних систем і забезпечити більш надійне відновлення даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рибін О.І. Реставрація образів методом умовної деконволюції в області просторових частот / О.І. Рибін, В.Ю. Корольов // Вісник Технічного університету Поділля.— 2000.— С.145 — 147.
2. Ніжебецька Ю.Х Підвищення точності ортогональних перетворень для аналізу лінійних систем / Ю.Х. Ніжебецька, О.І. Рибін, О.Б. Шарпан // Наукові вісті НУТУ «КП».— 2008.— №5.— С.12— 18.
3. Рибін О.І. Аналіз лінійних систем в області трансформант кратного перетворення EIWAL / О.І. Рибін, А.П. Ткачук // Вісник НУТУ «КП». Сер. Радіотехніка. Радіоапаратобудування.— 2006.— №33.— С.31— 38.
4. Іванюк Н.О.(Лашевська) Реставрація зображень методом умовної деконволюції в базисі перетворення RTF/ Н.О. Іванюк, К.С. Солохненко, О.І. Рибін // Вісник НТУУ «КП» Сер. Радіотехніка. Радіоапаратобудування. – 2012. – № 56.— С. 25 –33 .
5. Рибін О.І. Реставрація образів за методом умовної деконволюції в області трансформант перетворення Адамара/ О.І. Рибін, Н.О. Іванюк .(Лашевська) // Вісник НТУУ «КП». Сер. Радіотехніка. Радіоапаратобудування. — 2011. — №46.— С.51 — 58.
6. Рибін О.І. Алгоритми побудови матриці деградації образу з використанням дискретного перетворення Адамара/ О.І. Рибін, Н.О. Іванюк .(Лашевська) // Вісник НТУУ «КП». Сер. Радіотехніка. Радіоапаратобудування. — 2012. — №49. — С. — 18 — 32.
7. Рибін О.І. Формування оберненої матриці деградації образу в області трансформант Адамара / О.І.Рибін, Н.О.Іванюк .(Лашевська) // Вісник

- НТУУ«КПІ» Сер. Радіотехніка. Радіоапаратобудування. – 2012. – № 52. – С. 29–37.
8. Gonzalez R. C., Woods R. E., Eddins S. L. Digital Image Processing using MATLAB. Pearson Education. 2004. ISBN 978-81-7758-898-9.
 9. Solomon C.J., Breckon T.P. Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab. Wiley-Blackwell, 2010.
doi:10.1002/9780470689776. ISBN 0470844736.
 10. Худьо В.Д. Моделювання стійкої стеганофонічної системи із заданими характеристиками мережі / В.Д.Худьо – Сучасні комп'ютерні інформаційні технології, 2016. – 177 с.
 11. Ефективні алгоритми побудови стегоконтейнерів з використанням швидкого перетворення Фур'є / Задірака В.К., Кошкіна Н.В., Мельникова С.С. – Праці міжнар. конф. “Питання оптимізації обчислень-XXXII”. – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України, 2005. –76-78с.
 12. Комп'ютерна стеганографія : навчальний посібник / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець – Вінниця: ВНТУ, 2017. - 155 с.
 13. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с
 14. Кошкіна Н.В. Ефективні спектральні алгоритми для вирішення задач цифрової стеганографії: дис. ... канд. фіз.-мат. наук: 01.05.01 / Н.В. Кошкіна. – Київ, 2005.– 139 с
 15. Іванюк Н.О. (Лащевська) Реставрація образів методом умовної деконволюції в базисі перетворення адамара:дис. «...» к.т.н. 05.12.17 / Н.О. Іванюк (Лащевська) – Київ, 2015 – 168 с.
 16. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

- 17.Рибін О.І. Аналіз лінійних систем в області трансформант перетворення Уолша-Адамара / О.І. Рибін, А.П. Ткачук // Вісник НУТУ «КП». Сер. Радіотехніка. Радіоапаратобудування.— №33.—С.14-23
- 18.Рибін О.І.Аналіз лінійних систем в області трансформант кратного перетворення EIWAL / О.І. Рибін, А.П. Ткачук // Вісник НУТУ «КП». Серія Радіотехніка. Радіоапаратобудування.— №33.— С.31—39
- 19.Рибін О.І. Аналіз лінійних систем з використанням кратних перстворень /О.І. Рибін, І.О. Рибіна, Ю.Х. Ніжебецька // Вісник НУТУ «КП». Серія Радіотехніка. Радіоапаратобудування.— №40.— С.5—12
- 20.Holub, V., Fridrich, J., & Denemark, T. (2014). *Universal Distortion Function for Steganography in an Arbitrary Domain*. EURASIP Journal on Information Security.
- 21.Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.). (2000). *Information Hiding: Techniques for Steganography and Digital Watermarking*. Artech House.
- 22.Chen, B., & Wornell, G. W. (2001). *Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding*. IEEE Transactions on Information Theory, 47(4), 1423-1443.
- 23.Barni, M., Bartolini, F., & Piva, A. (2002). *Improved Wavelet-Based Watermarking Through Pixel-Wise Masking*. IEEE Transactions on Image Processing, 10(5), 783-791.
- 24.Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press.
- 25.Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures*. Springer.
- 26.Provos, N., & Honeyman, P. (2003). *Hide and Seek: An Introduction to Steganography*. IEEE Security & Privacy, 1(3), 32-44.
- 27.Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). *Information hiding - A survey*. Proceedings of the IEEE, 87(7), 1062-1078.

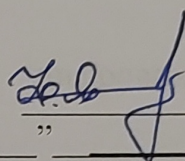
28. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography*. Morgan Kaufmann.
29. Аналіз стійкості стеганографічних систем в моделі пасивного противника / Задірака В. К., Кошкіна Н. В., Олексюк О. С. – Штучний інтелект, 2004.– 801–805 с.
30. Ефективні алгоритми побудови стегоконтейнерів з використанням швидкого перетворення Фур'є / Задірака В.К., Кошкіна Н.В., Мельникова С.С. – Праці міжнар. конф. “Питання оптимізації обчислень-XXXII”. – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України, 2005. –76-78с
31. Non-malleable cryptography /Dolev D., Dwork C., Naor M. – Proc. of twenty-third annual ACM symposium on theory of computing. – New Orleans,Lousiana, 1991. –542–552 p.
32. Towards foundatioms of cryptography: investigation of perfect secrecy /Jurgensen H., Robbins L. – J. of universal computer science, 1996. – 2, N 5. – 347– 379 p.
33. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / С.В.Мельник, С.В.Кондакова // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. –К. : Наук.-вид. відділ НА СБ України, 2010. –С. 134-138
34. Shahidan M. Abdullah, Azizah A. Manaf, and Mazdak Zamani. Recursive Reversible Image Watermarking Using Enhancement of Difference Expansion Techniques. Journal of Information Security Research. Volume 1 Number 2. June 2010. Pages 64-70.
35. Jeong, J., Chung, M.Y. & Choo H. 2008. Integrated OTP-based used authentication scheme using smart cards in home networks. Proceedings of the International Conference on System Sciences, 294-301
36. Advanced Statistical Steganalysis. R. Böhme, Springer, 2010.

37. Стасюк О. І. Сучасні стеганографічні методи захисту інформації // Захист інформації. — 2011. — Т. 13. — № 1 (50). - С. 56–63.
38. Тарасов Д. О. Класифікація та аналіз безкоштовних програмних засобів стеганографії // Інформаційні системи та мережі. Вісник НУ «Львівська політехніка». — 2010. — № 673. — С. 365-374.
39. Дацюк Р.К. Метод приховування великого об'єму даних в файлах формату JPEG // «Інтелектуальний потенціал – 2020» , Хмельницький: ПВНЗ УЕП, 2020. – Частина 2. С. 37-42
40. Wu C.-P. Robust audio watermarking for copyright protection / C.-P. Wu, P.- C. Su, K.C.-C. Jay // Proceedings of SPIE, Advanced Signal Processing Algorithms, Architectures, and Implementations IX. - 1999.- Vol. 3807. - P. 387-397 17.
Полный список аудио форматов [Електронний ресурс]: Audio Coding. – Режим доступа: http://audiocoding.ru/assets/meta/2021-05-22-wav-file-structure/wav_formats.txt (дата звернення 20.02.2022).
41. Diffie W., Hellman M. E. New Directions in Cryptography. IEEE Transactions on Information Theory. 1976, V. 22, No. 6. pp. 44-54.
42. ElGamal T. On Computing Logarithms Over Finite Fields: Lecture Notes in Computer Science. Proceedings of CRYPTO'85 – Advances in Cryptology in Santa Barbara, (Santa Barbara, August 18-22, 1985), pp. 396-402.

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції “Управління
інформаційною
безпекою” кафедри МБІС
д.т.н., професор



Юрій ЯРЕМЧУК

2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ

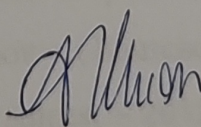
до магістерської кваліфікаційної роботи на тему:

Підвищення стійкості зображень до спотворень від активних стеганографічних атак на основі методів умовної деконволюції у базисі перетворення Адамара

08-72.МКР.007.00.138.ТЗ

Керівник магістерської кваліфікаційної роботи

к.ф.-м.н., доцент



Шиян А.А.

Вінниця – 2024 р.

1. Найменування та область застосування

Програмний засіб для підвищення стійкості зображень до спотворень від активних стеганографічних атак. Область застосування: захист цифрових зображень у системах інформаційної безпеки.

2. Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 81 від 11. 03. 2024 р.

3. Мета та призначення розробки

3.1 Мета розробки: підвищення стійкості цифрових зображень до спотворень від активних стеганографічних атак за допомогою методів умовної деконволюції у базисі перетворення Адамара.

3.2 Призначення: забезпечення захисту цифрових зображень від незаконних модифікацій та спотворень.

4. Джерела розробки

4.1. Іванюк Н.О. (Лащевська) Реставрація образів методом умовної деконволюції в базисі перетворення адамара: дис. «...» к.т.н. 05.12.17 / Н.О. Іванюк (Лащевська) – Київ, 2015 – 168 с.

4.2. Комп'ютерна стеганографія : навчальний посібник / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінєць – Вінниця: ВНТУ, 2017. - 155 с. 4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.3. Рибін О.І. Формування оберненої матриці деградації образу в області трансформант Адамара / О.І.Рибін, Н.О.Іванюк .(Лащевська) // Вісник НТУУ«КПІ» Сер. Радіотехніка. Радіоапаратобудування. – 2012. – № 52. – С. 29–37.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний та легкий у використанні інтерфейс користувача.

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків.

5.1.3 Програмний засіб повинен ефективно виявляти та відновлювати зображення після спотворення внаслідок активних стеганографічних атак.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок; у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень.

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій.

5.2.3 Програмний засіб повинен виконувати свої функції належним чином у різних умовах атак.

5.3 Вимоги до складу і параметрів технічних засобів:

- процесор – Pentium 1500 МГц або аналогічний;
- оперативна пам'ять – не менше 512 МБ;
- середовище функціонування – операційна система Windows;

вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим стандартам з техніки безпеки при користуванні комп'ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.4

7. Вимоги до технічного захисту інформації

7.1 Забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Забезпечити неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

121

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	12.03.2024	25.03.2024
2	Аналіз предметної області обраної теми	26.03.2024	08.04.2024
3	Апробація отриманих результатів	09.04.2024	15.04.2024
4	Розробка алгоритму роботи	16.04.2024	13.05.2024
5	Написання магістерської роботи на основі розробленої теми	14.05.2024	27.05.2024
6	Розробка економічної частини	28.05.2024	04.06.2024
7	Передзахист магістерської кваліфікаційної роботи	28.05.2024	04.06.2024
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	05.06.2024	06.06.2024
9	Захист магістерської кваліфікаційної роботи		10.06.2024

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- програмний додаток;
- презентація;
- відгук керівника роботи;
- відгук опонента

Технічне завдання до виконання прийняв

Лашевська Н.О.

ДОДАТОК 2

ПІДМАТРИЦЯ КОЕФІЦІЄНТІВ БЛОКУ 16-ГО ПОРЯДКУ МАТРИЦІ G_{16}^- НАД.

$$\bar{\mu}_{16,16;17,17} =$$

	16	17
16	$1, 7/8, 6/8, 5/8, 4/8, 3/8, 2/8, 1/8, 0,$ $-1/8, -2/8, -3/8, -4/8, -5/8, -6/8,$ $-7/8, -1,$ $-7/8, -6/8, -5/8, -4/8, -3/8, -2/8,$ $-1/8, 0,$ $1/8, 2/8, 3/8, 4/8, 5/8, 6/8, 7/8, \dots,$ $1, 7/8, 6/8, 5/8, 4/8, 3/8, 2/8, 1/8, 0,$ $-1/8, -2/8, -3/8, -4/8, -5/8, -6/8,$ $-7/8, -1,$ $-7/8, -6/8, -5/8, -4/8, -3/8, -2/8,$ $-1/8, 0,$ $1/8, 2/8, 3/8, 4/8, 5/8, 6/8, 7/8, \dots$	$0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, 1/8,$ $0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, -1/8, 0, -1/8, \dots,$ $0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, 1/8,$ $0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, -1/8, 0, -1/8, \dots$
17	$0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, 1/8, \dots,$ $0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, 1/8, \dots,$	$1, -7/8, 6/8, -5/8, 4/8, -3/8, 2/8, -1/8, 0,$ $1/8, -2/8, 3/8, -4/8, 5/8, -6/8,$ $7/8, -1,$ $7/8, -6/8, 5/8, -4/8, 3/8, -2/8,$ $1/8, 0,$ $-1/8, 2/8, -3/8, 4/8, -5/8, 6/8, -7/8, \dots,$ $1, -7/8, 6/8, -5/8, 4/8, -3/8, 2/8, -1/8, 0,$ $1/8, -2/8, 3/8, -4/8, 5/8, -6/8,$ $7/8, -1,$ $7/8, -6/8, 5/8, -4/8, 3/8, -2/8,$ $1/8, 0,$ $-1/8, 2/8, -3/8, 4/8, -5/8, 6/8, -7/8, \dots$

$\bar{\mu}_{18,18;19,19} =$

	18	19
18	$1, 1/8, -6/8, -1/8, 4/8, 1/8, -2/8,$ $-1/8, 0,$ $1/8, \quad 2/8, -1/8, -4/8, \quad 1/8,$ $6/8, -1/8,$ $-1, -1/8, \quad 6/8, \quad 1/8, -1/2, \quad -1/8,$ $2/8, 1/8, 0,$ $-1/8, -2/8, 1/8, 4/8, -1/8, -6/8,$ $1/8, \dots,$ $1, 1/8, -6/8, -1/8, 4/8, 1/8, -2/8,$ $-1/8, 0,$ $1/8, \quad 2/8, -1/8, -4/8, \quad 1/8,$ $6/8, -1/8,$ $-1, -1/8, \quad 6/8, \quad 1/8, -1/2, \quad -1/8,$ $2/8, 1/8, 0,$ $-1/8, -2/8, 1/8, 4/8, -1/8, -6/8,$ $1/8, \dots$	$0, 7/8, 0, -5/8, 0, 3/8, 0, -1/8, 0, -1/8,$ $0, 3/8, 0, -5/8, 0, 7/8,$ $0, -7/8, 0, 5/8, 0, -3/8, 0, 1/8, 0, 1/8,$ $0, -3/8, 0, 5/8, 0, -7/8, \dots,$ $0, 7/8, 0, -5/8, 0, 3/8, 0, -1/8, 0, -1/8,$ $0, 3/8, 0, -5/8, 0, 7/8,$ $0, -7/8, 0, 5/8, 0, -3/8, 0, 1/8, 0, 1/8,$ $0, -3/8, 0, 5/8, 0, -7/8, \dots$
19	$0, -7/8, 0, 5/8, 0, -3/8, 0, 1/8, 0,$ $1/8,$ $0, -3/8, 0, 5/8, 0, -7/8,$ $0, 7/8, 0, -5/8, 0, 3/8, 0, -1/8, 0,$ $-1/8,$ $0, 3/8, 0, -5/8, 0, 7/8, \dots,$ $0, -7/8, 0, 5/8, 0, -3/8, 0, 1/8, 0,$ $1/8,$ $0, -3/8, 0, 5/8, 0, -7/8,$ $0, 7/8, 0, -5/8, 0, 3/8, 0, -1/8, 0,$ $-1/8,$ $0, 3/8, 0, -5/8, 0, 7/8, \dots$	$1, -1/8, -6/8, 1/8, 4/8, -1/8, -2/8,$ $1/8, 0,$ $-1/8, 2/8, 1/8, -4/8, -1/8, 6/8, 1/8,$ $-1, 1/8, 6/8, -1/8, -1/2, 1/8, 2/8, -1/8,$ $0,$ $1/8, -2/8, -1/8, 4/8, 1/8, -6/8,$ $-1/8, \dots,$ $1, -1/8, -6/8, 1/8, 4/8, -1/8, -2/8,$ $1/8, 0,$ $-1/8, 2/8, 1/8, -4/8, -1/8, 6/8, 1/8,$ $-1, 1/8, 6/8, -1/8, -1/2, 1/8, 2/8, -1/8,$ $0,$ $1/8, -2/8, -1/8, 4/8, 1/8, -6/8,$

		$-1/8, \dots$
--	--	---------------

 $\bar{\bar{\mu}}_{16,18;17,19} =$

	18	19
16	$0, 1/8, 2/8, 1/8, 0, 1/8, 2/8, 1/8,$ $0, 1/8, 2/8, 1/8, 0, 1/8, 2/8, 1/8,$ $0, -1/8, -2/8, -1/8, 0, -1/8,$ $-2/8, -1/8,$ $0, -1/8, -2/8, -1/8, 0, -1/8,$ $-2/8, -1/8, \dots,$ $0, 1/8, 2/8, 1/8, 0, 1/8, 2/8, 1/8,$ $0, 1/8, 2/8, 1/8, 0, 1/8, 2/8, 1/8,$ $0, -1/8, -2/8, -1/8, 0, -1/8,$ $-2/8, -1/8,$ $0, -1/8, -2/8, -1/8, 0, -1/8,$ $-2/8, -1/8, \dots$	$0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8, \dots,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8, \dots$
17	$0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8, \dots,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8,$ $0, 1/8, 0, -1/8, 0, 1/8, 0, -1/8,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0, -1/8, 0, 1/8, 0, -1/8, 0, 1/8, \dots$	$0, -1/8, 2/8, -1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, -1/8, 2/8, -1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, 1/8, -2/8, 1/8, 0, 1/8, -2/8, 1/8,$ $0, 1/8, -2/8, 1/8, 0, 1/8, -2/8, 1/8, \dots,$ $0, -1/8, 2/8, -1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, -1/8, 2/8, -1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, 1/8, -2/8, 1/8, 0, 1/8, -2/8, 1/8,$ $0, 1/8, -2/8, 1/8, 0, 1/8, -2/8, 1/8, \dots$

Матриця $\bar{\bar{\mu}}_{16,20;19,23}$ складається з чотирьох матриць $\bar{\bar{\mu}}_{16,20;17,21}$; $\bar{\bar{\mu}}_{18,22;19,23}$ та

$\bar{\mu}_{16,22;17,23} = -\bar{\mu}_{18,20;19,21}$. Коефіцієнти μ_{ij} цих матриць мають наступний вигляд

$\bar{\mu}_{16,20;17,21} =$

	20	21
16	$0, 1/8, 2/8, 3/8, 4/8, 3/8, 2/8, 1/8,$ $0, 1/8, 2/8, 3/8, 4/8, 3/8, 2/8, 1/8,$ $0, -1/8, -2/8, -3/8, -4/8,$ $-3/8, -2/8, -1/8,$ $0, -1/8, -2/8, -3/8, -4/8,$ $-3/8, -2/8, -1/8, \dots,$ $0, 1/8, 2/8, 3/8, 4/8, 3/8, 2/8, 1/8,$ $0, 1/8, 2/8, 3/8, 4/8, 3/8, 2/8, 1/8,$ $0, -1/8, -2/8, -3/8, -4/8,$ $-3/8, -2/8, -1/8,$ $0, -1/8, -2/8, -3/8, -4/8,$ $-3/8, -2/8, -1/8, \dots$	$0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8, \dots,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8, \dots$
17	$0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8, \dots,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8, \dots$	$0, -1/8, 2/8, -3/8, 4/8, -3/8, 2/8,$ $-1/8,$ $0, -1/8, 2/8, -3/8, 4/8, -3/8, 2/8, -1/8,$ $0, 1/8, -2/8, 3/8, -4/8, 3/8, -2/8, 1/8,$ $0, 1/8, -2/8, 3/8, -4/8, 3/8, -2/8,$ $1/8, \dots,$ $0, -1/8, 2/8, -3/8, 4/8, -3/8, 2/8,$ $-1/8,$ $0, -1/8, 2/8, -3/8, 4/8, -3/8, 2/8, -1/8,$ $0, 1/8, -2/8, 3/8, -4/8, 3/8, -2/8, 1/8,$ $0, 1/8, -2/8, 3/8, -4/8, 3/8, -2/8,$ $1/8, \dots$

$$\bar{\mu}_{18,22;19,23} =$$

	22	23
18	$0, -1/8, -2/8, 1/8, 4/8, 1/8, -2/8,$ $-1/8,$ $0, -1/8, -2/8, 1/8, 4/8, 1/8,$ $-2/8, -1/8,$ $0, 1/8, 2/8, -1/8, -4/8, -1/8,$ $2/8, 1/8,$ $0, 1/8, 2/8, -1/8, -4/8, -1/8,$ $2/8, 1/8, \dots,$ $0, -1/8, -2/8, 1/8, 4/8, 1/8, -2/8,$ $-1/8,$ $0, -1/8, -2/8, 1/8, 4/8, 1/8,$ $-2/8, -1/8,$ $0, 1/8, 2/8, -1/8, -4/8, -1/8,$ $2/8, 1/8,$ $0, 1/8, 2/8, -1/8, -4/8, -1/8,$ $2/8, 1/8, \dots$	$0, 1/8, 0, -3/8, 0, 3/8, 0, -1/8,$ $0, 1/8, 0, -3/8, 0, 3/8,$ $0, -1/8,$ $0, 1/8, 0, 3/8, 0, -3/8,$ $0, 1/8,$ $0, -1/8, 0, 3/8, 0, -3/8,$ $0, 1/8, \dots,$ $0, 1/8, 0, -3/8, 0, 3/8, 0, -1/8,$ $0, 1/8, 0, -3/8, 0, 3/8,$ $0, -1/8,$ $0, 1/8, 0, 3/8, 0, -3/8,$ $0, 1/8,$ $0, -1/8, 0, 3/8, 0, -3/8,$ $0, 1/8, \dots$
19	$0, -1/8, 0, 3/8, 0, -3/8,$ $0, 1/8,$ $0, -1/8, 0, 3/8, 0, -3/8,$ $0, 1/8,$ $0, 1/8, 0, -3/8, 0, 3/8, 0, -1/8,$ $0, 1/8, 0, -3/8, 0, 3/8,$ $0, -1/8, \dots,$ $0, -1/8, 0, 3/8, 0, -3/8,$ $0, 1/8,$ $0, -1/8, 0, 3/8, 0, -3/8,$ $0, 1/8,$ $0, 1/8, 0, -3/8, 0, 3/8, 0, -1/8,$ $0, 1/8, 0, -3/8, 0, 3/8,$ $0, -1/8, \dots$	$0, 1/8, -2/8, -1/8, 4/8, -1/8, -2/8, 1/8,$ $0, 1/8, -2/8, -1/8, 4/8, -1/8,$ $-2/8, 1/8,$ $0, -1/8, 2/8, 1/8, -4/8, 1/8,$ $2/8, -1/8,$ $0, -1/8, 2/8, 1/8, -4/8, 1/8,$ $2/8, -1/8, \dots,$ $0, 1/8, -2/8, -1/8, 4/8, -1/8, -2/8, 1/8,$ $0, 1/8, -2/8, -1/8, 4/8, -1/8,$ $-2/8, 1/8,$ $0, -1/8, 2/8, 1/8, -4/8, 1/8,$ $2/8, -1/8,$ $0, -1/8, 2/8, 1/8, -4/8, 1/8,$ $2/8, -1/8, \dots$

--	--	--

$$\bar{\mu}_{16,22;17,23} = -\bar{\mu}_{18,20;19,21} =$$

	22	23
16	$0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8, \dots,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8,$ $0, -1/8, -2/8, -1/8, 0, 1/8, 2/8,$ $1/8, \dots$	$0, 1/8, 0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8, 0,$ $-1/8, 0, -1/8, 0, 1/8,$ $0, -1/8, 0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8, \dots,$ $0, 1/8, 0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8, 0,$ $-1/8, 0, -1/8, 0, 1/8,$ $0, -1/8, 0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8, 0,$ $1/8, 0, 1/8, 0, -1/8, \dots,$
17	$0, -1/8, 0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8,$ $0, 1/8, 0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0,$ $-1/8, 0, -1/8, 0, 1/8, \dots,$ $0, -1/8, 0, 1/8, 0, 1/8, 0, -1/8, 0, -1/8,$ $0, 1/8, 0, 1/8, 0, -1/8,$ $0, 1/8, 0, -1/8, 0, -1/8, 0, 1/8, 0, 1/8,$ $0,$ $-1/8, 0, -1/8, 0, 1/8, \dots$	$0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $1/8,$ $0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $1/8, \dots,$ $0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $1/8,$

	$0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $-1/8,$ $0, 1/8, -2/8, 1/8, 0, -1/8, 2/8,$ $1/8, \dots$
--	---

Матриця $\bar{\bar{\mu}}_{20,20;23,23}$ також складається з чотирьох матриць $\bar{\bar{\mu}}_{20,20;21,21}$; $\bar{\bar{\mu}}_{22,22;23,23}$ та $\bar{\bar{\mu}}_{20,22;21,23} = -\bar{\bar{\mu}}_{22,20;23,21}$. Їх матриці коефіцієнтів перед відліками g_i мають наступний вигляд

$$\bar{\bar{\mu}}_{20,20;21,21} =$$

	20	21
20	$1, 5/8, 2/8, -1/8, -4/8, -3/8,$ $-2/8, -1/8, 0,$ $1/8, 2/8, 3/8, 4/8, 1/8,$ $-2/8, -5/8,$ $-1, -5/8, -2/8, 1/8, 4/8, 3/8,$ $2/8, 1/8, 0,$ $-1/8, -2/8, -3/8, -4/8, -1/8, 2/8,$ $5/8, \dots,$ $1, 5/8, 2/8, -1/8, -4/8, -3/8,$ $-2/8, -1/8, 0,$ $1/8, 2/8, 3/8, 4/8, 1/8,$ $-2/8, -5/8,$ $-1, -5/8, -2/8, 1/8, 4/8, 3/8,$ $2/8, 1/8, 0,$ $-1/8, -2/8, -3/8, -4/8, -1/8, 2/8,$ $5/8, \dots$	$0, 3/8, 0, 3/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, 3/8, 0, 3/8,$ $0, -3/8, 0, -3/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, -3/8, 0, -3/8, \dots,$ $0, 3/8, 0, 3/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, 3/8, 0, 3/8,$ $0, -3/8, 0, -3/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, -3/8, 0, -3/8, \dots$
21	$0, -3/8, 0, -3/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, -3/8, 0, -3/8,$ $0, 3/8, 0, 3/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, 3/8, 0, 3/8, \dots,$ $0, -3/8, 0, -3/8, 0, 1/8, 0, 1/8, 0, 1/8,$ $0, 1/8, 0, -3/8, 0, -3/8,$ $0, 3/8, 0, 3/8, 0, -1/8, 0, -1/8, 0, -1/8,$ $0, -1/8, 0, 3/8, 0, 3/8, \dots$	$1, -5/8, 2/8, 1/8, -4/8, 3/8,$ $-2/8, 1/8, 0,$ $-1/8, 2/8, -3/8, 4/8, -1/8,$ $-2/8, 5/8,$ $-1, 5/8, -2/8, -1/8, 4/8, -3/8,$ $2/8, -1/8, 0,$ $1/8, -2/8, 3/8, -4/8, 1/8,$ $2/8, -5/8, \dots,$

		$1, -5/8, 2/8, 1/8, -4/8, 3/8,$ $-2/8, 1/8, 0,$ $-1/8, 2/8, -3/8, 4/8, -1/8,$ $-2/8, 5/8,$ $-1, 5/8, -2/8, -1/8, 4/8, -3/8,$ $2/8, -1/8, 0,$ $1/8, -2/8, 3/8, -4/8, 1/8,$ $2/8, -5/8, \dots$
--	--	---

$$\bar{\mu}_{22,22;23,23} =$$

	22	23
22	$1, 3/8, -2/8, -3/8, -4/8, -1/8,$ $2/8, 1/8,$ $0, -1/8, -2/8, 1/8, 4/8, 3/8,$ $2/8, -3/8,$ $-1, -3/8, 2/8, 3/8, 4/8, 1/8,$ $-2/8, -1/8,$ $0, 1/8, 2/8, -1/8, -4/8, -3/8,$ $-2/8, 3/8, \dots,$ $1, 3/8, -2/8, -3/8, -4/8, -1/8,$ $2/8, 1/8,$ $0, -1/8, -2/8, 1/8, 4/8, 3/8,$ $2/8, -3/8,$ $-1, -3/8, 2/8, 3/8, 4/8, 1/8,$ $-2/8, -1/8,$ $0, 1/8, 2/8, -1/8, -4/8, -3/8,$ $-2/8, 3/8, \dots$	$0, 5/8, 0, 1/8, 0, -3/8, 0, 1/8, 0,$ $1/8, 0,$ $-3/8, 0, 1/8, 0, 5/8,$ $0, -5/8, 0, -1/8, 0, 3/8, 0, -1/8, 0,$ $-1/8, 0,$ $3/8, 0, -1/8, 0, -5/8, \dots,$ $0, 5/8, 0, 1/8, 0, -3/8, 0, 1/8, 0,$ $1/8, 0,$ $-3/8, 0, 1/8, 0, 5/8,$ $0, -5/8, 0, -1/8, 0, 3/8, 0, -1/8, 0,$ $-1/8, 0,$ $3/8, 0, -1/8, 0, -5/8, \dots$
23	$0, -5/8, 0, -1/8, 0, 3/8, 0, -1/8, 0,$ $-1/8, 0,$ $3/8, 0, -1/8, 0, -5/8,$ $0, 5/8, 0, 1/8, 0, -3/8, 0, 1/8, 0, 1/8,$ $0,$ $-3/8, 0, 1/8, 0, 5/8, \dots,$ $0, -5/8, 0, -1/8, 0, 3/8, 0, -1/8, 0,$ $-1/8, 0,$ $3/8, 0, -1/8, 0, -5/8,$ $0, 5/8, 0, 1/8, 0, -3/8, 0, 1/8, 0, 1/8,$ $0,$ $-3/8, 0, 1/8, 0, 5/8, \dots$	$1, -3/8, -2/8, 3/8, -4/8, 1/8,$ $2/8, -1/8,$ $0, 1/8, -2/8, -1/8, 4/8, -3/8,$ $2/8, 3/8,$ $-1, 3/8, 2/8, -3/8, 4/8, -1/8,$ $-2/8, 1/8,$ $0, -1/8, 2/8, 1/8, -4/8, 3/8,$ $-2/8, -3/8, \dots,$ $1, -3/8, -2/8, 3/8, -4/8, 1/8,$ $2/8, -1/8,$ $0, 1/8, -2/8, -1/8, 4/8, -3/8,$ $2/8, 3/8,$ $-1, 3/8, 2/8, -3/8, 4/8, -1/8,$ $-2/8, 1/8,$

		$0, -1/8, 2/8, 1/8, -4/8, 3/8,$ $-2/8, -3/8, \dots$
--	--	--

$$\bar{\bar{\mu}}_{20,22;21,23} = -\bar{\bar{\mu}}_{22,20;23,21}$$

	22	23
20	$0, 3/8, 6/8, 3/8, 0, -1/8, -2/8,$ $-1/8, 0, -1/8, -2/8, -1/8,$ $0, 3/8, 6/8, 3/8,$ $0, -3/8, -6/8, -3/8, 0, 1/8, 2/8,$ $1/8, 0, 1/8, 2/8, 1/8,$ $0, -3/8, -6/8, -3/8, \dots,$ $0, 3/8, 6/8, 3/8, 0, -1/8, -2/8,$ $-1/8, 0, -1/8, -2/8, -1/8,$ $0, 3/8, 6/8, 3/8,$ $0, -3/8, -6/8, -3/8, 0, 1/8, 2/8,$ $1/8, 0, 1/8, 2/8, 1/8,$ $0, -3/8, -6/8, -3/8, \dots$	$0, -3/8, 0, 3/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0,$ $-1/8, 0, -3/8, 0, 3/8,$ $0, 3/8, 0, -3/8, 0, -1/8, 0, 1/8, 0, -1/8, 0,$ $1/8, 0, 3/8, 0, -3/8, \dots,$ $0, -3/8, 0, 3/8, 0, 1/8, 0, -1/8, 0, 1/8,$ $0,$ $-1/8, 0, -3/8, 0, 3/8,$ $0, 3/8, 0, -3/8, 0, -1/8, 0, 1/8, 0, -1/8, 0,$ $1/8, 0, 3/8, 0, -3/8, \dots$
21	$0, 3/8, 0, -3/8, 0, -1/8, 0, 1/8, 0,$ $-1/8, 0,$ $1/8, 0, 3/8, 0, -3/8,$ $0, -3/8, 0, 3/8, 0, 1/8, 0, -1/8, 0,$ $1/8, 0,$ $-1/8, 0, -3/8, 0, 3/8, \dots,$ $0, 3/8, 0, -3/8, 0, -1/8, 0, 1/8, 0,$ $-1/8, 0,$ $1/8, 0, 3/8, 0, -3/8,$ $0, -3/8, 0, 3/8, 0, 1/8, 0, -1/8, 0,$ $1/8, 0,$ $-1/8, 0, -3/8, 0, 3/8, \dots$	$0, -3/8, 6/8, -3/8, 0, 1/8, -2/8, 1/8, 0,$ $1/8, -2/8, 1/8,$ $0, -3/8, 6/8, -3/8,$ $0, 3/8, -6/8, 3/8, 0, -1/8, 2/8,$ $-1/8, 0, -1/8, 2/8, -1/8,$ $0, 3/8, -6/8, 3/8, \dots,$ $0, -3/8, 6/8, -3/8, 0, 1/8, -2/8, 1/8, 0,$ $1/8, -2/8, 1/8,$ $0, -3/8, 6/8, -3/8,$ $0, 3/8, -6/8, 3/8, 0, -1/8, 2/8,$ $-1/8, 0, -1/8, 2/8, -1/8,$ $0, 3/8, -6/8, 3/8, \dots$

ДОДАТОК 3

**Лістинг програми для реставрації образів (сигналів) за методом умовної
деконволюції в базисі перетворення Адамара**

```

N=128;% довжина сигналу (кількість відліків)
% в даному прикладі експеримент проводився з сигналами форма трикутник
(програма може реалізувати реставрацію сигналів будь-якої форми)
Q=5; % асиметричність трикутника (при Q=2 трикутник симетричний)
n=2; % кількість трикутників (можна вибирати будь-яку)
T=N/n; % період
tau=T/Q; % тривалість трикутника
% сигнал формується його поступовим нарощенням від 0 до 1, потім додаємо
% спад від 1 до 0, після чого додається масив нулів

stroka_nulej=zeros(1,(T-tau)); %задаємо вектор- рядоку із нулів
stroka_narostanija=ones(1,(tau/Q));% задаємо вектор-рядок нарощення
трикутника
for x=0:1:tau/Q
    stroka_narostanija(x+1)=x*Q/tau;
end
stroka_spada=ones(1,(tau-tau/Q));% задаємо вектор-рядок спадання трикутника
for x=1:1:tau-tau/Q
    stroka_spada(x)=1-x/((tau-tau/Q));
end
signal=zeros(1,N); % формуємо сигнал
S=0;% обнулити пам'ять
for a=1:1:n

```

```

S= [ stroka_narostanija, stroka_spada, stroka_nulej, S]; % конструємо сигнал
end
while size(S)<N
    S=[S,0]; % умова, яка дозволяє змінювати вхідні («підганяє» розмір сигналу,
якщо він коротший ніж число N )
end

for a=1:1:N
    signal(a)=S(a);% («підганяє» розмір сигналу, якщо він довший ніж число N
end
v=10;
S_shum=awgn(signal,v);
S_shum_f=fft(S_shum);
% формула для енергії шуму отриманого сигнала

a=0.9;
x=0:1:63;
y=exp(-a*x); % імпульсна характеристика
%y=1./(1+a*x); % імпульсна характеристика
temp=size(y);
nuul=zeros(temp);
y=[y nuul];

IMP =y;
N=size(IMP);
N=N(2);
stolbez=rot90(rot90(rot90(IMP)));
G=stolbez;

```

```

B=stolbez;
for m=1:1:N-1
    B = circshift(B, 1);
    G=[G B];
end
    L=signal*G;
    snr=10;
    L_shum=awgn(L,snr);
    glad=0:1:127;
    c=[1 -2 1];
    temp1=size(glad);
    temp2=size(c);
    temp=temp1(2)-temp2(2);
    nuul=zeros(1,temp);
    c=[c nuul];
    Glad =c;
    N=size(Glad);
    N=N(2);
    stolbez=rot90(rot90(rot90(Glad)));
    C=stolbez;
    A=stolbez;
    for m=1:1:N-1
        A = circshift(A, 1);
        C=[C A];
    end
    Had=hadamard(N);
    F=dftmtx(N);
    F_n=F/N;

```



```

P=F_n*Had';
G2=G'*G;
C2=C'*C;
lamda=1;
Ghad=Had'*G*Had;
G2had=Had'*G2*Had;
Lhad=L*Had;
C2had=Had'*C2*Had;
A=F_n'*(G2+((1/lamda)*C2))*F_n;
A_obratnoe=inv(A);
A_had=P'*Had*A*Had*P;
Ghad_obratnoe=P'*A_obratnoe*P;
f_s_had=Lhad*Ghad_obratnoe*Ghad.';
f=f_s_had*Had;
G_f=F_n'*G*F_n;
G2_f=F_n'*G2*F_n;
L_f=L*F_n;
C2_f=F_n'*C2*F_n;
G_ff=G2_f+((1/lamda)*C2_f);
G_f_obratnoe=inv(G_ff);
f_s_f=L_f'*G_f_obratnoe*G_f.';
f_f=f_s_f*F_n;
f_novoe=awgn(f,snr);
f1=fft(S_shum);

```

**Лістинг програми для формування оберненої діагональної матриці
реставрації образів за методом умовної деконволюції**

```
// Створення масиву сигналу
long_massiv=16;
long_zadergka=0;
long_massiv_edeniz=4;
long_hvost_signala=long_massiv-long_zadergka-long_massiv_edeniz;
S_zaderganij=zeros(1,long_zadergka);
I=ones(1,long_massiv_edeniz);
S_hvost=zeros(1,long_hvost_signala);
S=[S_zaderganij, I, S_hvost];

// Спотворення сигналу за рахунок накладання імпульсної характеристики з
адитивним шумом
v=0.5;
S=awgn(S,snr);
a=1;
x=0:1:7;
y=exp(-a*x);
temp=size(y);
nuul=zeros(temp);
y=[y nuul];
IMP =y;
N=size(IMP);
N=N(2);
stolbez=rot90(rot90(rot90(IMP)));
G=stolbez;
B=stolbez;
```

```

// Створення блочно-діагональної матриці G
for m=1:1:N-1
    B = circshift(B, 1);
    G=[G B];
end
Had=hadamard(N);
F=dftmtx(N);
F_n=F/N;
P=F*Had;% визначення матриці P
m=log2(N);%Загальна кількість блоків матриці, яка необхідна для розрахунку
P_perestavlenoe=zeros(N, N); % формування нульової матриці
for n=1:1:m %задане значення кількості блоків та кількості ітерацій,
    for i=1:1:N/(2^n)% номер стовпця, який переставляється
        P_perestavlenoe(:, N/(2^n)+i)=P(:, i*(2^n)+(1-2^(n-1)));% загальна формула для
        виводу зміщеної матриці P
    end
end
P_perestavlenoe(1, 1)=P(1, 1);
P_complex=Had*F.';

G2=G.'*G;
G2had=Had*G2*Had';
A=F_n*(G2+((1/lamda)*C2))*F_n;%
A_obratnoe=inv(A);

Ghad_obratnoe=P_complex*A_obratnoe*P;
stem(abs((Ghad_obratnoe)/max(Ghad_obratnoe)))

```

**Лістинг підпрограм для реалізації символного методу формування
матриці $\overline{\overline{G}}_{1Had}$**

Операція приведення:

```
function rezalt_privedenie=privedenie (na_vhode)
na_vhode=rasschyrenie (na_vhode);
a=size (na_vhode);
a=a (2);
edeniz=zeros (1,a);
for i=1:1:a
    edeniz (1,i)=(-1)^(i+1);
end
    rezalt_privedenie=na_vhode.*edeniz;
```

Операція розширення:

```
function rezalt_rashirennij=rasschyrenie (na_vhode)
a=size (na_vhode);
a=a (2);
rezalt_rashirennij=zeros (1,2*a)
for i=1:1:a
    rezalt_rashirennij (1, (2*i-1))=na_vhode (1,i);
end
for i=2:2:2*a-1
    rezalt_rashirennij (1,i)=(rezalt_rashirennij (1,i-1)+rezalt_rashirennij (1,i+1))/2;
end
rezalt_rashirennij (1,2*a)=
    (na_vhode (1,1)+na_vhode (1,a))/2;
```

Операція розширення з приведенням:

```

function
rezalt_rashirennij=rasshirenie_s_proregivaniem(na_vhode)
a=rasschyrenie(na_vhode);
b=size(a);
b=b(2);
rezalt_rashirennij=a;
for i=1:2:b
rezalt_rashirennij(1,i)=0;
end

```

Операція приведення в два кроки:

```

function
rezalt_privedenie=privedenie_v_dva_schaga(na_vhode)
na_vhode=rasschyrenie(na_vhode);
a=size(na_vhode);
a=a(2);
edeniz=zeros(1,a);
for i=1:4:a-3
    edeniz(1,i)=1;
    edeniz(1,i+1)=1;
    edeniz(1,i+2)=-1;
    edeniz(1,i+3)=-1;
end
    rezalt_privedenie=na_vhode.*edeniz;

```

Операція приведення з розширенням в два кроки:

```

function
rezalt_rashirennij=proregivanie_s_privedeniem_v_dva_schag
a(na_vhode)
a=rasschyrenie(na_vhode);
b=size(a);
b=b(2);
rezalt_rashirennij=a;
for i=1:2:b
rezalt_rashirennij(1,i)=0;
end
    a=size(rezalt_rashirennij);
a=a(2);
edeniz=zeros(1,a);
    for i=1:4:a-3
        edeniz(1,i)=1;
        edeniz(1,i+1)=1;
        edeniz(1,i+2)=-1;
        edeniz(1,i+3)=-1;
    end
        rezalt_rashirennij=rezalt_rashirennij.*edeniz;

```

Операція інверсія:

```

function rezalt_privedenie=inversia(na_vhode)
na_vhode=rasschyrenie(na_vhode);
a=size(na_vhode);
a=a(2);
edeniz=zeros(1,a);
edeniz(1,1:a)=-1;
rezalt_privedenie=na_vhode.*edeniz;

```

**Лістинг програми реалізації методу умовної деконволюції в базисі
перетворення Адамара для боротьби з активними стеганографічними
атаками на Python**

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.linalg import hadamard
from scipy.ndimage import convolve

def load_image(path):
    from PIL import Image
    img = Image.open(path).convert('L')
    img = np.array(img)
    return img

def normalize_image(image):
    return image / 255.0

image_path = 'path_to_image.png'
image = load_image(image_path)
image = normalize_image(image)
plt.imshow(image, cmap='gray')
plt.title("Original Image")
plt.show()

def hadamard_transform_2d(image):
    H = hadamard(image.shape[0])
    return H @ image @ H

def inverse_hadamard_transform_2d(transformed_image):
    H = hadamard(transformed_image.shape[0])
    return H @ transformed_image @ H / (transformed_image.shape[0] ** 2)
transformed_image = hadamard_transform_2d(image)
```

```
plt.imshow(np.log1p(np.abs(transformed_image)), cmap='gray')
plt.title("Hadamard Transformed Image")
plt.show()
```

```
def detect_anomalies(transformed_image, threshold):
    anomalies = np.abs(transformed_image) > threshold
    return anomalies

def conditional_deconvolution_2d(transformed_image, anomalies,
    regularization_param):
    corrected_transform = np.copy(transformed_image)
    corrected_transform[anomalies] /= regularization_param
    return corrected_transform

anomalies = detect_anomalies(transformed_image, threshold=10)
regularization_param = 0.1
corrected_transform = conditional_deconvolution_2d(transformed_image, anomalies,
    regularization_param)
plt.imshow(np.log1p(np.abs(corrected_transform)), cmap='gray')
plt.title("Corrected Hadamard Transformed Image")
plt.show()
```

```
restored_image = inverse_hadamard_transform_2d(corrected_transform)
plt.imshow(restored_image, cmap='gray')
plt.title("Restored Image")
plt.show()

restored_image = inverse_hadamard_transform_2d(corrected_transform)
```


ДОДАТОК 4

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему: «Підвищення стійкості зображень до спотворень від
активних стеганографічних атак на основі методів умовної
деконволюції у базисі перетворення Адамара»

Виконала студентка групи КІТС-22мз
Лашевська Наталія Олександрівна
Керівник кваліфікаційної роботи:
Шиян Анатолій Антонович,
професор кафедри МБІС

Київ – 2024

Актуальність обраної теми

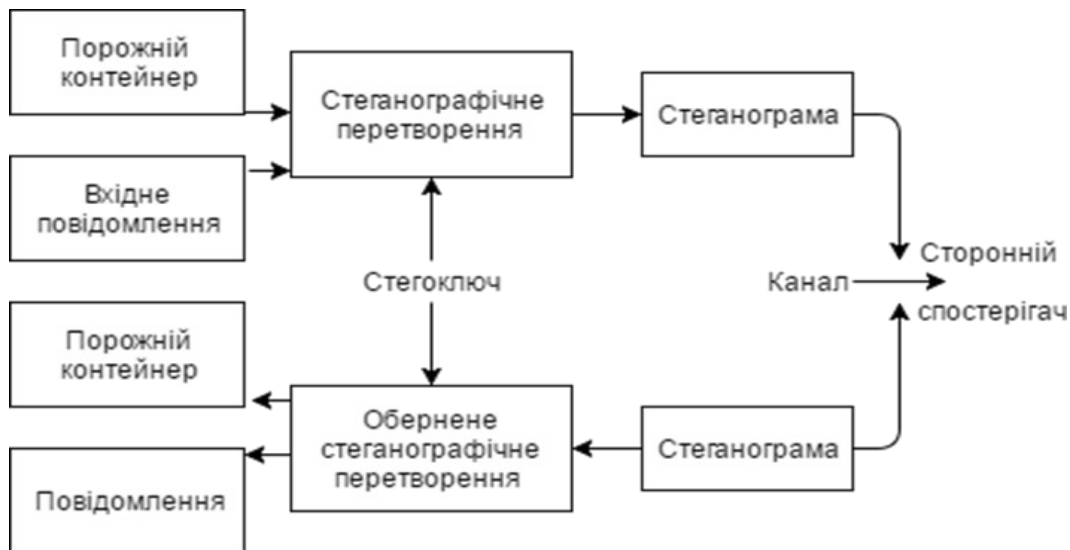
- Зростаюча кількість стеганографічних атак: У зв'язку з поширенням цифрових зображень та широкого застосування методів стеганографії, кількість активних стенографічних атак зростає. Це створює необхідність в розробці ефективних методів захисту зображень від таких атак.
- Потреба в надійних захисних методах: Збереження конфіденційності та цілісності зображень має велике значення в багатьох сферах, включаючи медицину, правоохоронну діяльність, а також в особистих комунікаціях. Отже, існує потреба в ефективних методах захисту від стеганографічних атак.
- Обмеженість існуючих методів захисту: Багато з існуючих методів захисту від стеганографічних атак можуть бути обмануті або неефективні при використанні деяких агресивних технік атаки. Умовна деконволюція у базисі перетворення Адамара може стати інноваційним підходом до вирішення цієї проблеми.
- Зростання використання цифрових технологій: З використанням цифрових технологій у всіх сферах життя зростає потреба в захисті цифрових даних, включаючи зображення, від різних видів атак. Пошук нових, більш ефективних методів захисту стає актуальною задачею.
- Таким чином, дослідження підвищення стійкості зображень до спотворень від активних стенографічних атак методом умовної деконволюції у базисі перетворення Адамара є актуальним, оскільки воно вирішує важливу проблему забезпечення безпеки та цілісності цифрових зображень у сучасному цифровому середовищі.

2

- **Метою** даної магістерської дисертації є розробка та реалізація методу підвищення стійкості зображень до спотворень від активних стенографічних атак шляхом застосування методу умовної деконволюції у базисі перетворення Адамара. Головною метою є забезпечення ефективного захисту цифрових зображень від незаконних модифікацій та спотворень, які можуть бути виконані шляхом вбудовування прихованої інформації або інших атак на стеганографічний алгоритм.
- **Об'єктом дослідження** є процес підвищення стійкості зображень до спотворень від активних стенографічних атак в сучасних радіотехнічних системах.
- **Предметом дослідження** є метод умовної деконволюції у базисі перетворення Адамара для підвищення стійкості зображень до спотворень, які виникають внаслідок активних стенографічних атак.

3

Поняття стеганографії

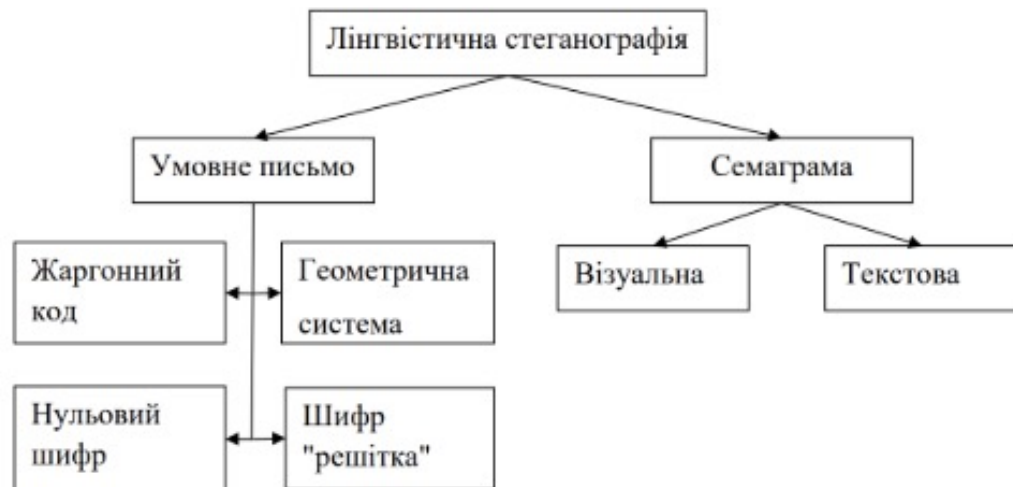


4

Види стеганографічних методів

- Лінгвістична стеганографія відображає методи приховування секретної інформації в непримітний текст, на основі застосування властивостей мови та лінгвістичних ресурсів. Умовне письмо та семиграми вважають основними категоріями лінгвістичних методи стеганографії.
- Цифрова стеганографія є одним із напрямів класичної стеганографії. Основна ідея полягає у тому, щоб приховати або вбудувати додаткову інформацію в цифрові об'єкти, при цьому викликаючи найменше спотворення. Зазвичай, такі спотворення, зважаючи на наявні формати цифрових об'єктів (зображення, відео, аудіо, текстури 3D), знаходяться нижче порогу чутливості людини, що призводить до непомітних для людського ока змін.

5



6



7

Модель аналізу загроз та оцінки стійкості стеганосистеми



8

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА

Моделлю деградації (спотворення) образу (одновимірною чи двовимірною) є в загальному випадку нелінійні та анізотропні оператори

$$L(x, y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} g(x, y, x', y') \cdot f(x', y') dx' dy' + V(x, y),$$

де $g(x, y, x', y')$ – результуюча імпульсна характеристика каналу прийому-передачі; $f(x', y')$ – сигнал, що його передають; $V(x, y)$ – адитивний шум, x, y — відповідні просторові координати.

Метод умовної деконволюції реставрації образу, за яким в натуральних координатах оцінка шуканого (реставрованого) образу може бути отримана (у випадку одновимірною образу) за виразом:

$$\hat{f} = \left[\bar{G}^T \cdot \bar{G} + \frac{1}{\lambda} \cdot \bar{c}^T \cdot \bar{c} \right]^{-1} \cdot \bar{G}^T \cdot \bar{L}$$

де $\hat{f}$ — шукана оцінка розміру $N \times 1$; $\bar{G}$ — матричний оператор дискретної згортки порядку N ; $\bar{c}$ — матричний дискретний оператор умови «гладкості» оцінки (2.20) порядку N ; $\bar{L}$ — стовпець відліків деградованого образу; λ — коефіцієнт варіації Лагранжа; T — знак транспонування.

9

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА

У випадку використання спектрів перетворення Адамара отримуємо вираз:

$$\hat{f}_{Had} = \left[\bar{G}_{2Had} + \frac{1}{\lambda} \cdot \bar{c}_{2Had} \right]^{-1} \cdot \bar{G}_{1Had}^T \cdot \bar{L}_{Had}$$

де $\hat{f}_{Had}$, $\bar{L}_{Had}$ — стовпці відліків спектрів Адамара реставрованого та деградованого образів відповідно розміру $N \times 1$; $\bar{G}_{1Had}^T$ — блочно-діагональна матриця $\bar{Had}_n \cdot \bar{G}^T \cdot \bar{Had}_n^T$; $\bar{G}_{2Had} = \bar{Had}_n \cdot \bar{G}_2 \cdot \bar{Had}_n^T$ та $\bar{c}_{2Had} = \bar{Had}_n \cdot \bar{c}_2 \cdot \bar{Had}_n^T$; $\bar{G}_{1Had} = \bar{Had}_n \cdot \bar{G}_1 \cdot \bar{Had}_n^T$ — блочно-діагональні матриці порядку N .
 $\bar{G}_{2Had} = \bar{Had}_n \cdot \bar{G}^T \cdot \bar{Had}_n^T \cdot \bar{Had}_n \cdot \bar{G} \cdot \bar{Had}_n^T$

Матриця $\bar{G}_{1Had}$ є блочно-діагональною матрицею, причому величина блоків зростає із зростанням номерів рядків матриці

10

ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА ДЛЯ БОРОТЬБИ З АКТИВНИМИ СТЕГANOГРАФІЧНИМИ АТАКАМИ

Загальна схема реалізації методу умовної деконволюції в базисі перетворення Адамара:

1. Перетворення зображення або сигналу в базис Адамара.
2. Аналіз спектру Адамара для виявлення аномалій.
3. Застосування умовної деконволюції для відновлення оригінального сигналу.
4. Зворотне перетворення в часову область або простір зображення.

11

ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДУ УМОВНОЇ ДЕКОНВОЛЮЦІЇ В БАЗИСІ ПЕРЕТВОРЕННЯ АДАМАРА ДЛЯ БОРОТЬБИ З АКТИВНИМИ СТЕГANOГРАФІЧНИМИ АТАКАМИ НА МОВІ PYTHON

```
import numpy as np
import cv2
from scipy.linalg import hadamard

# Функція для перетворення Адамара
def hadamard_transform(image):
    n = image.shape[0]
    H = hadamard(n)
    return H @ image @ H

# Функція для зворотного перетворення Адамара
def inverse_hadamard_transform(transformed_image):
    n = transformed_image.shape[0]
    H = hadamard(n)
    return (H @ transformed_image @ H) / (n ** 2)

# Функція для умовної деконволюції
def conditional_deconvolution(transformed_image, threshold=0.1):
    deconvolved_image = np.copy(transformed_image)
    deconvolved_image[np.abs(transformed_image) < threshold] = 0
    return deconvolved_image

# Завантаження зображення
image_path = 'path_to_image.png'
image = cv2.imread(image_path, cv2.IMREAD_GRAYSCALE)
image = cv2.resize(image, (512, 512))
```

```
# Перетворення Адамара
hadamard_image = hadamard_transform(image)

# Умова деконволюція
deconvolved_hadamard_image = conditional_deconvolution(hadamard_image)

# Зворотне перетворення Адамара
restored_image = inverse_hadamard_transform(deconvolved_hadamard_image)

# Збереження результату
output_path = 'restored_image.png'
cv2.imwrite(output_path, restored_image)

# Візуалізація результатів
cv2.imshow('Original Image', image)
cv2.imshow('Restored Image', restored_image)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

12

ВИСНОВКИ

- 1) В роботі проведено огляд наукових робіт та методів, пов'язаних із стеганографією, активними стенографічними атаками, умовною деконволюцією та перетворенням Адамара.
- 2) Розроблено алгоритм за методом умовної деконволюції в базисі ортогонального перетворення Адамара, який дозволив ефективно відновити оригінальне зображення після спотворення внаслідок активних стенографічних атак.
- 3) Реалізовано розроблений метод у вигляді програмного забезпечення. Реалізація на Python дозволяє легко інтегрувати цей підхід у різні системи обробки зображень.

В цілому, дослідження показало, що застосування методу умовної деконволюції в базисі перетворення Адамара є ефективним підходом для підвищення стійкості зображень до стеганографічних атак. Отримані результати підтверджують доцільність подальших досліджень у цьому напрямку та можливість практичного застосування запропонованого методу в різних галузях, де важлива захист цифрової інформації.

13

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему: «Підвищення стійкості зображень до спотворень від
активних стеганографічних атак на основі методів умовної
деконволюції у базисі перетворення Адамара»

Виконала студентка групи КІТС-22мз
Лашевська Наталія Олександрівна
Керівник кваліфікаційної роботи:
Шиян Анатолій Антонович,
професор кафедри МБІС

Київ – 2024

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ
ЗАПОЗИЧЕНЬ

Назва роботи: Підвищення стійкості зображень до спотворень від активних стеганографічних атак на основі методів умовної деконволюції у базисі перетворення Адамара

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unichesk

Оригінальність 97 %

Схожість 3 %

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку

(підпис)

Коваль Н.П.

(прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unichesk щодо роботи.

Автор роботи

(підпис)

Лашевська Н.О.

(прізвище, ініціали)

Керівник роботи

(підпис)

Шиян А.А.

(прізвище, ініціали)