Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Захист даних стеганографічними методами на базі використання структурної надмірності опису контейнерів
(тема)

Виконав:
студент 2 курсу, групи *ІМІм-19-2*
Жуков В.В.
(прізвище, ініціали)

Спеціальність *172. Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. Костромицький А. І.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2021 р.

Не містить відомостей, заборонених
до відкритого публікування

Керівник_____ /*А.І.Костромицький*

Студент _____ / *В.В.Жуков*

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти другий (магістерський)

Спеціальність *172. Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«_15_» *березня* 20 21 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Жукову Віктору Володимировичу*

(прізвище, ім'я, по батькові)

1. Тема роботи *Захист даних стеганографічними методами на базі використання структурної надмірності опису контейнерів*

затверджена наказом університету від _12_ __березня__2021 р. № __350 Ст__

2. Термін подання студентом роботи до екзаменаційної комісії _25_ _травня_ 2021 р.

3. Вихідні дані до роботи *Дослідити принципи функціонування стегосистем. Розглянути принцип роботи ряду стандартизованих методів та визначити їхні недоліки. Виконати аналіз методу маскування на базі використання структурних особливостей сегментів зображень, та режими його функціонування. Розрахувати можливу швидкість надсилання мережею біт прихованого повідомлення у різних режимах для відеоконтейнеру формату HDReady*

4. Перелік питань, що потрібно опрацювати в роботі *Вступ*

1. Ключові питання та завдання методів стеганографічного приховування даних

2. Стандартизовані методи та алгоритми маскування даних

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *слайди презентації в форматі Power Point (назва та мета роботи, ключові питання та завдання методів стеганографічного приховування даних, тандартизовані методи та алгоритми маскування даних, метод маскування даних на базі використання структурних особливостей та надмірності сегментів зображень, оцінка продуктивності методу маскування даних на базі використання структурних особливостей сегментів зображень)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ключові питання та завдання методів стеганографічного приховування даних		
2	Стандартизовані методи та алгоритми маскування даних		
3	Метод маскування даних на базі використання структурних особливостей та надмірності сегментів зображень		
4	Оцінка продуктивності методу маскування даних на базі використання структурних особливостей сегментів зображень		
5	Висновки		
6	Оформлення пояснювальної записки		

Дата видачі завдання *15 березня* 2021 р.

Студент _____ *В.В.Жуков*
(підпис)

Керівник роботи _____ *доц. Костромицький А.І*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 90 с., 23 рис., 17 посилань, 1 додаток

Мета роботи – дослідження методів маскування даних з використанням мультиконтейнерів для підвищення безпеки даних обмеженого доступу у ході передавання відкритими каналами інфокомунікаційних систем.

Досліджено принципи побудови стегосистем. Розглянуто підходи до побудови стеганографічних алгоритмів, орієнтованих на графічне середовище. Виконано дослідження методу непрямої інкапсуляції даних, що використовує особливості структурного опису трансформованих сегментів контейнеру. Показано переваги застосування дослідженого методу на випадок використання мультиконтейнерів для різних режимів вбудовування секретних даних. Розраховано теоретично можливі швидкості передавання біт інкапсульованого повідомлення для різних режимів функціонування досліджуваного методу.

МАСКУВАННЯ ДАНИХ, РОБАСТНА СТЕГАНОГРАФІЯ, JPEG, ГРУПА КАДРІВ, LSB, ЄМНІСТЬ СТЕГОСИСТЕМИ, ХЕШ-ФУНКЦІЯ

THE ABSTRACT

Explanatory note: 90 p., 23 fig., 17 reference, 1 app.

Object of work - study the methods of data masking using multi-containers to increase the security of restricted access data during the transmission of open channels of infocommunication systems.

The principles of stegosystem construction are studied. Approaches to the construction of steganographic algorithms focused on the graphical environment are considered. A study of the method of indirect data encapsulation using the features of the structural description of the transformed segments of the container is performed. The advantages of using the researched method in case of using multicontainers for different modes of embedding secret data are shown. The theoretically possible bit rates of the encapsulated message for different modes of operation of the studied method are calculated.

DATA MASKING, ROBUST STEGANOGRAPHY, JPEG, PERSONNELGROUP, LSB, STEGOSYSTEM CAPACITY, HASH FUNCTION

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ADSL	Asymmetric Digital Subscriber Line	Технологія передавання даних
RGB	Red, green, blue	Трьохколірна модель
YCrCb	Y, Chromatic Red, Chromatic Blue	Яскравісно-хроматична колірна модель
MPEG	Motion Pictures Expert Group	Сімейство стандартів відео кодування
LSB	Less Significant Bit	Найменш значущий біт – біт молодшого розряду
BPM	Batmap	Технологія опису графічних даних без стиснення
JPEG	Joint Photographic Expert Group	Технологія кодування зображень

ВСТУП

Процес розвитку інформаціно-комунікаційних систем та мереж, мережевої інфраструктури та технологій передавання, обробки і аналізу даних є, у сутності череда постійно змінюючих один одного етапів виникнення проблемних питань, та етапів їх вирішення.

Від початку становлення, та у перші роки функціонування інфокомунікаційних мереж одна з головних проблем стосувалася занизької пропускної спроможності мережевих каналів та, відповідно, у свою чергу породжувала цілу низку питань, кожне з яких вимагало свого рішення – це і необхідність удосконалення технологій передачі, і розробка відповідних мережевих протоколів, і створення більш потужного обладнання мережевих та кінцевих вузлів. У міру рішення означеної проблематики виникала необхідність, по-перше, розширення спектру базових мережевих послуг, що, головним чином складався з передавання файлів, електронної пошти та текстових месенджерів на кшталт QIP, ICQ та подібних. Це питання свого часу також було успішно вирішене з широким утілення ADSL на ділянці мережі доступу. У решті решт, пізніше вирішення потребував широкий спектр проблем, що стосувалися функціональності веб-додатків на мобільних пристроях, забезпечення сталого потокового відео та аудіо мовлення, тощо.

На сьогодні одним з ключових питань з переліку найголовніших, що потребують нагального вирішення є забезпечення належного рівня захищеності даних у ході їх трансляції мережею або зберігання [1,2]. Дана проблематика є гострою майже для усіх категорій користувачів та сервісів на базі мереж. Це стосується:

- збереження особистих даних користувачів;
- захисту платіжних операцій, що виконуються через системи онлайн-банкінгу;
- підтримки сталого каналу взаємодії між об’єктами критичних систем;
- гарантування захищеності, автентичності та цілісності даних як у системах загального призначення, так і у системах, функціональність яких є стратегічно важливою для суспільства та держави;
- захисту даних та мережевої інфраструктури організацій та установ від дій зловмисників.

Одним з найбільш перспективних підходів, що потенційно здатен вирішити усі перелічені завдання, полягає у широкому застосуванні технологій маскування даних. Даний підхід набув утілення у вигляді систем стеганографічного захисту. Відтак, напрямки досліджень у галузі методів стегозахисту є на сьогодні актуальними. Це, у свою чергу, зумовлює актуальність тематики даної атестаційної роботи.

1 КЛЮЧОВІ ПИТАННЯ ТА ЗАВДАННЯ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ

1.1 Головні напрямки застосування стеганографічних методів

Загальний перелік завдань, вирішенню якого сприяють методи стегозахисту інформації, у загальному випадку зводиться до наступних класів [1, 3]:

- забезпечення аутентичності та достовірності даних;
- збереження цілісності даних;
- приховане зберіганням даних, доступ до яких має обмежене коло осіб;
- приховане передавання інформації.

Розглянемо окремо зазначені класи завдань.

1.1.1 Забезпечення автентичності, достовірності та цілісності даних

У загальному випадку під терміном ***цілісність даних*** мається на увазі, що унаслідок виконання тієї чи іншої операції відносно них, дані не було змінено.

Такою операцією може бути передача, зберігання або відтворення даних. Іншими словами, це можна розуміти як те, що дані залишаються у тому вигляді, у якому вони були створені.

При цьому, ***аутентичність даних*** є властивістю, яка гарантує, той чи інший інформаційний суб'єкт чи ресурс є ідентичним оголошеному [1].

У свою чергу, ***достовірність даних*** є властивістю даних не мати у своєму складі прихованих помилок.

Одним з найбільш ефективних на сьогодні підходом щодо забезпечення ***цілісності та автентичності*** даних є нанесення спеціалізованих маркерів, наявність яких може бути виявлено лише за наявності відповідного алгоритму.

При цьому, виявлення змісту таких маркерів є можливим лише за умови що відомим є не лише сам алгоритм, але також і секретний ключ, на базі якого здійснюється інтерпретація нанесеного маркеру.

Найчастіше таким маркером є цифрових водяний знак, або цифровий відбиток. (ЦВ). Їх використовують зазвичай з метою захисту від тиражування для запобігання випадків несанкціонованого використання [3].

Останнім часом це є гостро актуальним, чому сприяє постійний розвиток та удосконалення мультимедійних технологій та засобів.

На тлі цього, з одного боку, зростає обсяг мультимедійного контенту а з іншого – зростає на нього попит.

У підсумку має місце суттєве загострення проблематики, пов’язаної з захистом авторських прав, та прав на інтелектуальну власності, поданої у цифровому вигляді.

З початком розвитку мультимедійних технологій першочергово привертали до себе увагу усі ті переваги, що дають підходи, спрямовані на опис та розповсюдження мультимедійного контенту у цифровому форматі представлення.

Але зараз значна частина з них знецінюється, оскільки крадіжка чи модифікація такого контенту не є складним завданням.

Для того, щоб протидіяти крадіжкам та незаконному використанню таких даних розробляються відповідні методи захисту. З-поміж них одним з найбільш ефективних є підхід, який передбачає вбудовування у захищуваний об'єкт ЦВ.

Такі цифрові відбитки, у свою чергу, поділяються на видимі та невидимі.

При цьому, найчастіше використовуються саме невидимі цифрові відбитки.

У свою чергу, зчитування та подальший аналіз ЦВ здійснюється за допомогою спеціалізованого декодером. За підсумком цього далі приймається рішення про те, є цифровий відбиток коректним, чи ні.

Найчастіше такі цифрові відбитки містять у собі унікальну кодову послідовність, дані власника або автору, тощо.

При цьому, у переважній більшості випадків на базі ЦВ забезпечується захист відеоматеріалів, аудіоданих та зображень.

Застосовується вбудовування двох типів невидимих ЦВ – унікальних маркерів, та маркерів, що можуть тиражуватися.

Відповідно, у першому випадку виробник може відстежувати кожну копію свого продукту, тоді як у другому випадку маркер слугує для інформування про належність того чи іншого продукту певному виробникові.

При цьому, у випадку зміни продукту, тобто, виконання несанкціонованої його модифікації, зміні також підлягає невидимий ЦВ, що може бути відстежень відповідними засобами – вже згаданим раніше декодером ЦВ, чи ПЗ, яке використовується для їх зчитування.

У випадку необхідності забезпечення достовірності даних, може здійснюватися нанесення спеціалізованої маркерної сітки з певним кроком. Такий крок є достатньо дрібним, щоб забезпечити (наприклад, у випадку зображення) нею перекриття не менш, ніж 80-90% площі одиниці мультимедійного продукту.

Правила нанесення маркерної сітки та особливості її побудови є відомими, тобто, у випадку її спотворення, що може бути визначено під час сканування, робиться висновок про те, що спотворенню було піддано сам об’єкт захисту.

1.1.2 Приховане зберіганням даних, доступ до яких має обмежене коло осіб

У випадку необхідності організації файлосховища, де поряд з даними відкритого типу можуть зберігатися секретні дані, може бути застосовано один з наступних підходів, а саме [4]:

- шифрування даних з обмеженим доступом з можливістю їх зчитування для осіб, які мають у своєму розпорядженні секретний ключ для дешифрування;
- блокування засобами адміністрування доступу до логічних чи фізичних розділів файлової системи, де зберігаються секретні дані;
- маскування даних з обмеженим доступом.

Першим двом з наведених заходів захисту властивий головний недолік, який полягає у тому, що зловмиснику апріорі відомо про існування інформації секретного характеру. Тобто, такі дані стають об’єктом цілеспрямованої атаки.

У свою чергу, коли мова йде про маскування секретної інформації, факт її наявность відпочатку невідомий, що свідчить на користь безумовної переваги та результативності даного підходу.

Маскування приховуваних даних зазвичай виконується шляхом їх інкапсуляції (вбудовування) у дані відкритого типу.

1.1.3 Приховане передавання інформації

Як і у випадку зберіганням даних, доступ до яких має обмежене коло осіб, приховане передавання інформації передбачає вбудовування біт секретного повідомлення у деякий носій [1, 4]. Такий носій зветься ***контейнером стеганографічної системи.***

Однією з головною вимогою до контейнеру є високий рівень ϖ надмірності його опису. Це забезпечує можливість вбудовування достатньої кількості приховуваних біт без значного порушення його цілісності, що може бути суттєвим для стійкості стегосистеми проти методів її виявлення – ***стегоаналізу***. З цього міркування контейнерами найчастіше стають:

- аудіо дані;
- кадри відео потоку;
- статичні зображення.

Контейнер, що не має зовнішніх ознак присутності прихованих даних, надсилається розподіленим середовищем приймачеві, який володіючи відповідним стеганографічним алгоритмом, та маючи у розпорядженні секретний ключ, вилучає частину, або повне секретне повідомлення. При цьому, оскільки зовнішні ознаки того, що той чи інший об’єкт є контейнером не спостерігаються, це є умовою захищеності стегоканалу. Для цього випадку загальна структурна схема стегосистеми наведена рис.1.1.

Так, у процесі приховування бере участь стегокодер, який, виконує розміщення біт секретного повідомлення у контейнер.

При цьому, принцип розміщення таких біт визначається ***алгоритмом маскування.***

На сьогодні рівень стійкості стегосистеми, тобто, ймовірність виявлення заповненого контейнеру напряму залежить від ефективності стеганографічного алгоритму (алгоритму маскування).

У свою чергу, ***ключ*** визначає множину опцій стегоалгоритму, та режим його функціонування, якщо це передбачено принципом функціонування алгоритму.

У той же час, алгоритми, що передбачають використання стегоключів, отримують додатковий рівень захисту від викриття за рахунок ускладнення механізмів інкапсуляції.

Відповідно до цього, у загальному випадку процес стегоаналізу також ускладнюється.

Більшість класичних алгоритмів не використовує секретних ключів.

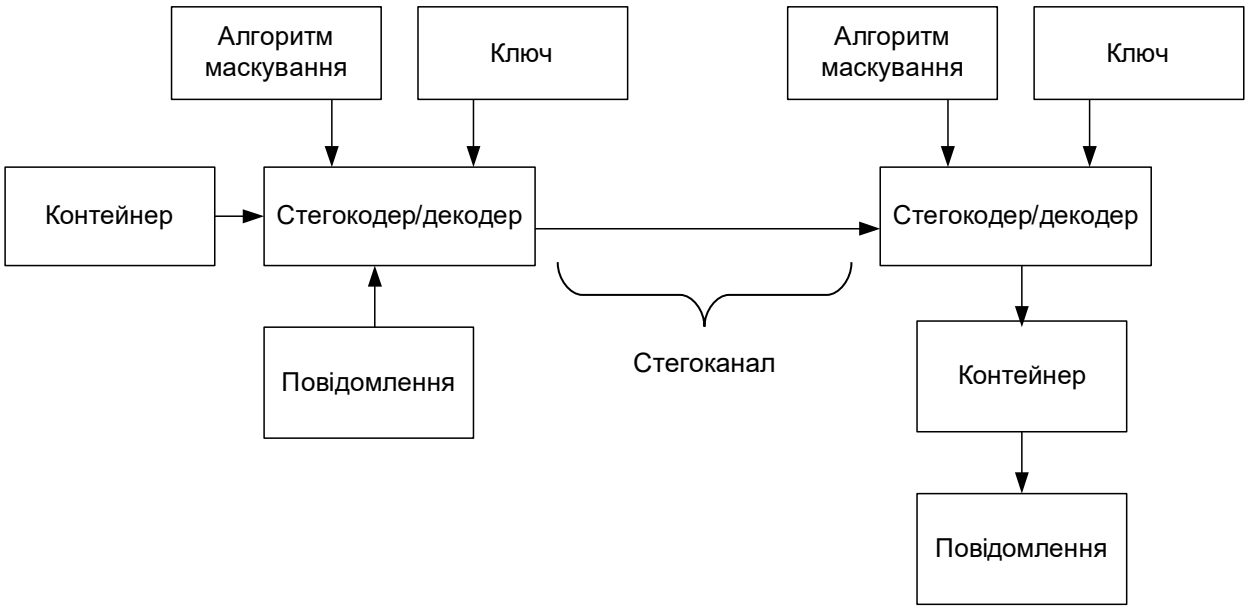


Рисунок 1.1 – Загальна структурна схема стегосистеми у класичному варіанті побудови

На прийомному боці стегокодер виконує процес декапсуляції, тобто, вилучення біт секретного повідомлення. Для цього спочатку за характерними ознаками виявляється заповнений контейнер, а далі безпосередньо з нього виокремлюються вбудовані дані. Як у процесі розпізнавання контейнеру, так і у процесі вилучення даних з нього окрім стегокодеру беруть участь стегоалгоритм та, відповідно, секретний ключ.

Отже, можна зазначити, що умі стеганографічні методи зводяться у загальному випадку до двох течій.

Методи стеганографічного захисту, що належать першій течії, передбачають, що зловмисник не повинен ні за яких обставин виявити факт існування вбудованих даних. Сюди відносяться стегоалгоритми, які забезпечують масковане передавання і зберігання інформації.

Водночас, для другої течії, що поєднує методи, які спрямовані на маркування продуктів у цифровому вигляді, наявність тих чи інших вбудованих даних зовсім не є таємницею [1, 4, 5].

У цьому полягає ключова відмінність даних течій.

1.2 Використання стеганографічних систем зловмисником

З розвитком технологій маскування даних розширився також діапазон застосування стеганографічних алгоритмів.

На сьогодні стеганографічни методи нерідко є одним з компонентів APT (Advanced Percistant Threat) – так званої «розвинутої стійкої загнози. APT являє собою комплекс організаційно-технічних заходів з боку зловмисника, що мають на меті [2]:

- проникнення до мережі, що є для зловмисника об’єктом інтересу;
- «закріплення» на зайнятих позиціях;
- пошук та отримання конфіденційної або стратегічної інформації, що може знаходитися у межах цільової мережі;
- отримання повного контролю над атакованою мережею;
- виведення із ладу мережевої інфраструктури та файлосховищ.

Загальний сценарій APT з використанням стеганографічних технологій є наступним:

1. Надсилання до цільової мережі файла-збірника. Такий файл може проникнути до мережі, минаючи більшість засобів захисту, оскільки він не містить у собі ділянок коду, що може бути розпізнаний як зловмисний. Найчастіше таке може відбуватися під час оновлення ПЗ. При цьому, виконуваний файл з пакету оновлення може замінюватися модифікованим файлом з тією ж назвою та цілком функціональним.

Модифікація полягає у тому, що файл, окрім основних функцій, може виконувати приховані.

2. Пошук файлом-збірником файлу-клієнту. Файл-клієнт також надходить у мережу, відносно якої розгортається APT, минаючи засоби кіберзахисту, оскільки він не має характерних ознак присутності зловмисного коду.

Частіше за все фіксувалися випадки, коли у ролі файлу-клієнту виступало зображення JPEG невеликої роздільної здатності. Таке зображення містило у собі деяке інкапсульоване повідомлення, після вилучення якого та відповідного трансформування файлом-збірником отримувався файл зі зловмисним кодом. При цьому, мережеві екрани та засоби кіберзахисту не фіксували небезпеки.

1.3 Критерії ефективності алгоритмів приховування даних

Показники, що можуть свідчити відносно продуктивності тих чи інших алгоритмічних рішень щодо побудови методів стегозахисту, можуть у загальному випадку бути класифіковані у 2 групи.

Першу групу складають параметри, що показують, наскільки ефективним буде функціонування стегосистеми на базі того чи іншого алгоритму. Сюди, зокрема, відносяться [5, 6]:

- ступінь захищеності L_p даних;
- відносна ємність C стегосистеми;
- показник швидкодії S алгоритму.

При цьому, одним з ключових параметрів, що ілюструє ефективність того чи іншого підходу до маскування інформації є ступінь захищеності L_p секретного повідомлення, або його частини (на випадок використання мультиконтейнерів).

Зараз даний параметр може розглядатися з 2 позицій.

У першому випадку під ступенем захищеності мається на увазі відношення ймовірності γ_{um} викриття повідомлення засобами стегоаналізу, або за участю експерта, до ймовірності γ_m успішної передачі повідомлення.

Це еквівалентно виразу:

$$L_p = \frac{\gamma_{um}}{\gamma_m} \times 100\% \qquad (1.1)$$

У другому випадку ступінь захищеності може бути виражено як час τ, який необхідний зловмиснику для того, щоб виявити наявність заповненого контейнеру.

На цей випадок величина L_p сприймається як функціонал від часу τ зламу стегосистеми, тобто:

$$L_p = \psi(\tau) \qquad (1.2)$$

Зрозуміло, що для виразів (2.1) та (2.2) умовою ефективності стеганографічного алгоритму є $\gamma_{um} \to 0$, або $\tau \to \infty$

Наступним показником, що свідчить про ефективність алгоритму маскування, є відносна ємність стегосистеми.

Фізична сутність даного поняття відображає відсоток даних d_m прихованого повідомлення у загальній кількості біт d_{all} на опис контейнеру. Це може бути показано виразом:

$$C = \frac{d_m}{d_{all}} \times 100\%. \quad (1.3)$$

Для даного показника діапазон допустимих значень задається з виходячи з вимог відносно:

- необхідного рівня L_p захищеності даних;
- типу контейнерів, що використовуються;
- особливостей алгоритму приховування.

У загальному випадку справедливою є наступна залежність:

$$C \uparrow \rightarrow L_p \downarrow \quad (1.4)$$

Тобто, коректним буде зазначити, що зазначені величини є взаємно оберненими, відтак збільшення рівня L_p захищеності даних можу бути досягнено у т.ч. зменшенням рівня C ємності контейнеру.

У свою чергу, показник швидкодії S алгоритму показує, скільки біт D може бути оброблено алгоритмом за одиницю часу t роботи, тобто:

$$S = \frac{D}{t} = \frac{D}{t_a + t_{tr} + t_b}, \quad (1.5)$$

де t_a - час підготовчого етапу обробки, за який виконується аналіз даних приховуваного повідомлення та аналіз особливостей контейнеру;

t_{tr} - час на трансформування даних приховуваного повідомлення до вигляду, який може бути вбудовано у контейнер;

t_b - час на вбудовування приховуваних даних у контейнер.

Показник S швидкодії є ключовим для стегосистем, що використовуються для маскування даних у реальному часі. При цьому, для систем, що не

передбачають маскування даних з наступною передачею у мережу, параметр S не є критичним.

У підсумку, загальні вимоги до ефективності функціонування стегосистеми на базі того чи іншого алгоритму можуть бути задані наступним співвідношенням:

$$L_p, C, S \rightarrow \max \tag{1.6}$$

У свою чергу, другу групу показників формують параметри, що показують можливість утілення алгоритму маскування на базі тієї чи іншої апаратної або програмної платформи. Сюди відносяться:

- обчислювальна складність χ алгоритму;
- ресурсоємність Ξ алгоритму.

Існування вимог щодо даних показників викликане тим, що:

- у ряді випадків має забезпечуватися обробка великих масивів даних у реальному часі; відтак від архітектури алгоритму будуть залежати вимоги щодо обчислювальної потужності системи;
- за умов, що для ефективного функціонування потужність процесорної системи не є критичною для ряду алгоритмів, водночас деякі з них можуть потребувати значних ресурсів RAM та/або ROM-пам’яті для зберігання проміжних результатів обчислень.

В ідеалі необхідно забезпечити виконання наступної нерівності:

$$\chi \rightarrow \min \,\&\, \Xi \rightarrow \min \tag{1.7}$$

у цьому випадку створюються умови для можливості реалізації алгоритму на базі апаратно-програмних платформ низької обчислювальної потужності.

Також для стегосистеми є справедливою наступна залежність:

$$\varpi \uparrow \rightarrow L_p \uparrow \vee C \uparrow . \tag{1.8}$$

Така залежність має враховуватися при вибору контейнеру.

1.4 Урахування критерію цілісності при виборі контейнеру для стегосистеми

Раніше зазначалося, що контейнер повинен мати значний рівень надмірності опису для того, щоб бути ефективним для маскування даних. На підставі цього найбільш підходячими типами контейнерів визначалися кадри відео, окремі статичні зображення та аудіодані [3].

Разом з тим, зазначений критерій не є єдиним. Другим, не менш важливим критерієм, є стійкість контейнеру до спотворень інформації у наслідок інкапсуляції. Інакше кажучи, файл, який слугує контейнером, після інкапсуляції має зберігати цілісність – тобто, має зберігатися можливість обробки такого контейнеру відповідними додатками як до, так і після інкапсуляції.

Відповідність цьому критерію деяких поширених типів файлів наведено табл. 1.1.

Таблиця 1.1 – Відповідність критерії цілісності для деяких файлів поширених типів

Тип файлу	**Відповідність критерію цілісності**	**Примітка**
1	**2**	**3**
Текстові файли, гіпертекст	+	Пряма інкапсуляція помітно спотворює текстові дані. Тому можливе застосування виключно методів, що вбудовують дані шляхом маніпуляції деякими текстовими параметрами, непомітними спостерігачу (наприклад, змінюють кількість пробілів)
Файли MS Office	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе

Продовження таблиці 1.1

1	2	3
Файли, що можуть виконуванися (exe, cmd, bat)	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе
Lib, dll, so (файли бібліотек)	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе
Файли зображень	+++	
Аудіо	+++	
Відеокадри	+++	
Архіви (Zip, 7z, rar)	-	Додустимим є архівація контейнеру. Пряме використання у якості контейнеру файлів даних типів неможливе
Елекронні книги та документи (pdf, fb2, djvu)	-	Контейнером може формуватися з текстового чи графічногофайлу на етапі, що передує його конвертації. Пряме вбудовування даних у файли означених типів неможливе
Системні та конфігураційні файли (sys, reg, ini)	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе

Отже, як видно з аналізу табл. 1.1, критерію цілісності відповідають ті ж самі типи файлів, яким відповідають найбільші значення надмірності опису.

1.5 Вибір контейнеру за критерієм раціонального використання пропускної здатності каналів мережі

Третім критерієм, який має враховуватися у ході вибору контейнеру для стегостистеми, є критерій раціонального використання пропускної здатності каналів мережі [3-5].

Важливість даного критерію пояснюється тим, що у категорії графічних (включаючи сюди також відеокадри) та аудіофайлів існують формати, що попри один і той же рівень інформативності можуть суттєво відрізнятися один від одного за розмірами.

Наприклад, аудіофайл, що містить одні і ті ж самі дані, може бути подано як у форматі MP3, так і у форматі WAV. Проте у першому випадку його розмір при параметрах кодування 128 кБіт/с та 44,1 кГц приблизно буде займати 1 МБ для 1 хвилини аудіо. На випадок же WAV-файлу за тих же самих умов його розмір буде сягати 38-45 МБ.

У свою чергу, говорячи про графічні контейнери, виконаємо порівняння форматів BMP та JPEG. Якщо графічний файл JPEG розміром 2560x1600 при 24-розрядній палітрі має розмір 1,6 МБ, по файл такогож самого змісту та рівня якості, поданий у вигляді BMP, займатиме на диску уже 11, 7 Мб. Відповідно, для його передавання мережею потрібно забезпечити набагато вищу бітову швидкість.

Свого часу для форматів WAV та BMP було створено велику кількість алгоритмів маскування, що базувалися, головним чином, на виконанні прямого вбудовування секретних даних. Це пояснюється легкістю реалізації стегоалгоритмів для контейнерів даних типів.

Разом з тим, присутність таких файлів у каналі зв’язку, до того ж, якщо їх передача є далеко не одиничною, само по собі викликає підозру та привертає до себе увагу. Такі файли у першу чергу можуть стати об’єктами для стегоаналізу.

2 СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ

2.1 Загальні підходи до реалізації алгоритмів маскування даних

На сьогодні уся множина алгоритмів і методів стегозахисту даних як для зберігання, так і для трансляції мережею, умовно може бути розподілена на 2 ключові групи [3, 6, 7].

Перша група містить підходи, що відзначаються достатньою простотою, підчас – тривіальністю реалізації, та базуються на розміщенні даних повідомлення, яке має бути приховано, у спеціалізованих полях файлів та ділянках файлонакопичувачів, що зазвичай не використовуються.

Такі рішення, попри простоту реалізації, мають досить низький рівень L_p стійкості до виявлення.

Сюди відносяться:

1. Алгоритми, що використовують поля коментарів графічних та аудіо файлів. Існування таких алгоритмів можливе завдяки наявності у складі ряду файлів означених типів – а зокрема – JPEG та MP3 спеціалізованих сегментів.

Такі сегменти початково призначалися для внесення даних технологічного характеру та даних мета опису файлів.

У випадку MP3 це – інформація про запис, автора, жанр, та інші. Також передбачено поле, куди можуть вноситися текстові дані довільного змісту та формату.

У свою чергу, JPEG має у своєму складі спеціалізований сегмент коментарів, де також можуть зберігатися текстові дані.

Я і у випадку MP3, тут присутня певна кількість полів, де передбачено зберігання інформації певних форматів – дата знімку, технічні дані знімку, модель камери.

Разом з тим, передбачено наявність поля загального коментарю, де може розміщуватися довільний текст.

2. Використання доріжок, щ є доступними для зчитування, але не сприймаються операційною системою. Це, зокрема, може бути резервна область накопичувача.

3. Методи запису даних, що приховуються, у невикористовувані

локації оптичних носіїв (CD, DVD, Blue-ray та ін.)

4. Алгоритми маскування даних у вільних зонах накопичувачів. Зазвичай у рамках даного підходу передбачено використання вільних локацій останнього кластеру файлу, а також використання вільних кластерів без запису у таблиці розміщення файлів відповідних даних про те, що мі кластери містять інформацію.

До другої групи підходів відносяться методи, що базуються на використанні надмірності опису файлів деяких типів. Це, у першу чергу, файли графічного типу та аудіо.

На відміну від алгоритмів першої групи, дані методи забезпечують суттєво вищий рівень L_p захищеності маскованої інформації.

Далі розглянемо характерні методи стеганографічного маскування даних зі складу кожної з зазначених груп.

2.2 Приклади стандартизованих підходів до маскування даних

2.2.1 Використання полів коментаря JPEG

Розглянемо структуру файлу JPEG на прикладі Google favicon (рис. 2.1)

Тут центральна частина наведеної структури являє собою безпосередньо дані у шістнадцятеричному представленні, у правій колонці знаходиться hex-інтерпретатор [8].

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  FF D8 FF FE 00 04 3A 29 FF DB 00 43 00 A0 6E 78  яШяю..:)яЫ.C. nx
00000010  8C 78 64 A0 8C 82 8C B4 AA A0 BE F0 FF FF F0 DC  Њxd Њ,ЊґЄ sряярЬ
00000020  DC F0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  Ьряяяяяяяяяяяяяя
00000030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  яяяяяяяяяяяяяяяя
00000040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF DB 00  яяяяяяяяяяяяяяЫ.
00000050  43 01 AA B4 B4 F0 D2 F0 FF FF FF FF FF FF FF FF  C.ЄґґрТряяяяяяяя
00000060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  яяяяяяяяяяяяяяяя
00000070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  яяяяяяяяяяяяяяяя
00000080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  яяяяяяяяяяяяяяяя
00000090  FF FF FF C0 00 11 08 00 10 00 10 03 01 22 00 02  яяяА.........".."
000000A0  11 01 03 11 01 FF C4 00 15 00 01 01 00 00 00 00  .....яД.........
000000B0  00 00 00 00 00 00 00 00 00 00 03 02 FF C4 00 1A  ............яД..
000000C0  10 01 00 02 03 01 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 01 00 12 02 11 31 21 FF C4 00 15 01 01 01 00  ......1!яД......
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 FF  ...............я
000000F0  C4 00 16 11 01 01 01 00 00 00 00 00 00 00 00 00  Д...............
00000100  00 00 00 00 11 00 01 FF DA 00 0C 03 01 00 02 11  .......яЪ.......
00000110  03 11 00 3F 00 AE E7 61 F2 1B D5 22 85 5D 04 3C  ...?.®зат.Х"…].<
00000120  82 C8 48 B1 DC BF FF D9                          ‚ИН±ЬїяЩ
```

Рисунок 2.1 – Приклад внутрішньої структури файлу Google favicon.jpg

На рис. 2.1 маркер FF D8 означає початок файлу [9]. Маркер DQT (FF DB) є міткою для зчитування таблиці квантування, маркер SOF0 (FF CO) свідчить про те, що файл закодовано у режимі Baseline, DHT (FF C4) – маркер таблиці Хафмана.

У свою чергу, маркер COM (FF FE) вказує на початок секції коментарів. Наступні 2 байта, у даному випадку це – 00 04 – вказують на довжину секції коментарю.

Далі йде безпосередньо сам коментар – 3A 29. Це є кодами символів «:» та «)», тобто, у коментар додано текст «:)».

Сам файл Google favicon.jpg у восьмикратному збільшенні показано рис. 2.2.

Рисунок 2.2 – Зовнішній вигляд файлу Google favicon.jpg

Таким чином, контейнерами вже з причини особливостей формату побудови файлу можуть бути зображення JPEG.

Існування поля коментарів дає змогу розміщувати у середині файлів текстові дані.

У той же час, для такого способу приховування забезпечується низький рівень L_p захищеності даних.

Це пояснюється, по-перше, відомістю даного способу, а по-друге, існуванням великої кількості програмних засобів для зчитування JPEG-коментарів (рис.2.3) [8].

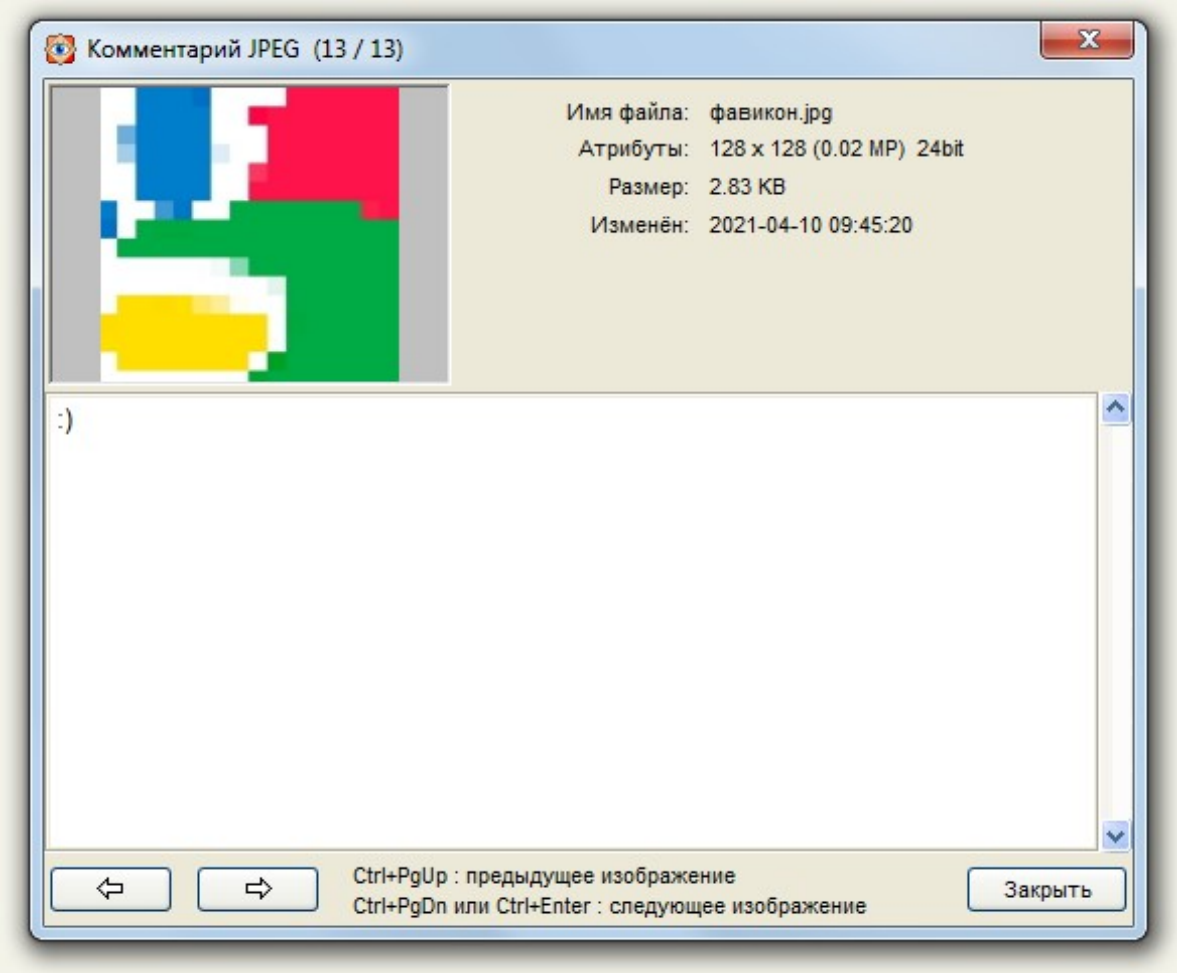


Рисунок 2.3 – Зчитування JPEG-коментарів за допомогою програмного засобу Fast Stone Image Viewer

2.2.1 Метод останнього біта (LSB-метод)

Одним з шляхів забезпечення високих показників L_p є урахування властивостей системи візуального сприйняття людини. Для цього ряд методів маскування використовує присутню у рамках контейнерів психовізуальну надмірність [10-12].

Розглянемо зображення, подане у 256 градаціях сірого, тобто з питомою швидкістю кодування 8 біт/піксель.

Добре відомо, що око людини не здатний помітити зміну молодшого значущого біта. Ще в 1989 році було отримано патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біта.

У даному випадку детектор аналізує тільки значення цього біта для кожного пікселя, а зір людини, навпаки, сприймає тільки старші 7 біт. Даний метод простий у реалізації і ефективний.

Сутність методу полягає у використанні 8-го біту $b(8)_{(x,y)}$, що належить сегменту з координатами (x,y), який буде використано для розміщення біту приховуваного повідомлення.

Для цього попередньо повідомлення конвертується у двійковий формат, зручний для запису побітно.

Далі, пропускаючи заголовок файлу, та ділянки службових даних біти повідомлення можуть розміщуватися у контейнер (рис. 2.4).

Рисунок 2.4 – Області графічного файлу-контейнеру, які потенційно може бути використано для маскування даних на базі LSB

Контейнер, у свою чергу, за допомогою прекодера переводиться у двійковий опис, після чого змістовна частина (без заголовків та маркерних сегментів) розбивається на байти, кожен з яких відповідає одному двійково поданому пікселю.

Після цього у кожному байті модифікується останній біт, змінюючись бітом двійковій послідовності, яка описує повідомлення, що має бути масковане. Дану функцію виконує стегокодер.

У такий спосіб, за умови, що контейнером є зображення у градаціях сірого, може бути використано до 1/8 розміру файлу зображення.

У свою чергу, якщо у ролі контейнера виступає RGB-зображення, теоретично може бути використано кожен з колірних каналів – відповідно, R, G та B. Таким чином може оброблятися BMP-контейнер.

Разом з тим, оскільки поширеність BMP-контейнерів у мережі незначна у наслідок їх значних розмірів, більш доцільними для використання у рамках LSB є контейнери JPEG.

При цьому, замість RGB використовується палітра YCrCb, що містить яскравісний Y канал та два хроматичних, відповідно, канали Cr та Cb.

У даному випадку, беручи до уваги особливості людського зору – а саме – можливість розпізнавати навіть незначні градації яскравості - використовувати компоненти каналу Y не рекомендується. Замість цього може бути застосовано канали Cr та Cb. Тобто, на цей випадок ємність стегосистеми може складати до 1/12 розміру файлу зображення.

Разом з тим, на випадок контейнерів насиченого та середньо-насиченого типів може бути використано 2 наймолодші біти для модифікації. Тобто, ємність C стегосистеми при цьому зросте вдвічі – то 1/6 розміру змістовної частини файлу зображення.

Алгоритм, за яким здійснюється модифікація молодших біт контейнеру, у загальному вигляді може бути зображено наступною схемою (рис.2.5).

Математично такий процес модифікації біт LSB задається наступним виразом:

$$\begin{cases} b(\ell)_{(x,y)} := 0 \mid b'(k)_{(i,j)} = 1 \,\&\, b(\ell)_{(x,y)} = 0 \\ b(\ell)_{(x,y)} := 1 \mid b'(k)_{(i,j)} = 1 \,\&\, b(\ell)_{(x,y)} = 1 \end{cases}, \qquad (2.1)$$

$$\ell = \overline{1;\Lambda},\ k = \overline{1;K}$$

де $b'(k)_{(i,j)}$ - біт секретного повідомлення, який необхідно вбудувати у контейнер шляхом модифікації одного з його LSB-біт;

$b(\ell)_{(x,y)}$ - вихідний біт молодшого розряду.

Як можна бачити з виразу (2.1), за умови, що LSB-біт $b(8)_{(x,y)}$ контейнеру дорівнює біту $b'(k)_{(i,j)}$ секретного повідомлення, біт $b(8)^{(i,j)}_{(x,y)}$ залишається незмінним.

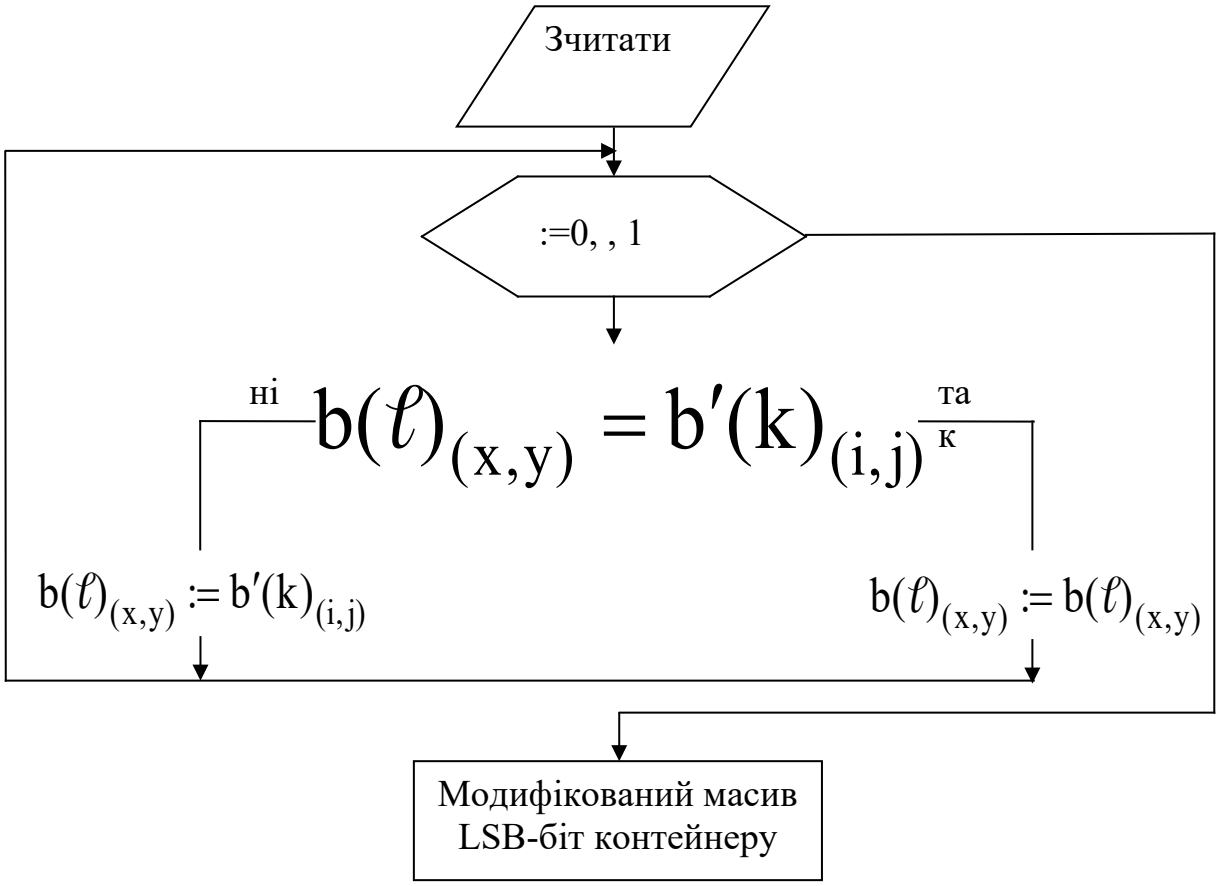


Рисунок 2.5 – Загальний алгоритм модифікації молодших біт контейнеру на базі LSB-підходу

На схемі 2.5 величина θ_{hb} - кількість біт повідомлення, що має бути масковано.

При цьому, для того, щоб міг коректно функціонувати алгоритм, зображений рис. 2.5, має задовольнятися наступна вимога:

$$\Lambda = K . \qquad (2.2)$$

Таким чином, попереднім кроком необхідно виконати розрахунок доступної кількості Λ біт у межах контейнеру.

Якщо брати до уваги, що теоретично для модифікації може бути застосовано будь-який LSB-біт контейнеру, загальна схема визначення

величини Λ, та, відповідно, вибору режиму модифікації LSB-біт буде такою, як показано рис. 2.6.

Математично даний принцип вибору моделі M модифікації молодших біт може бути подано наступним чином:

$$\begin{cases} M = \{B(\xi)_{Cr}\} \mid \Lambda \geq K \\ M = \{B(\xi)_{Cr} \curlyvee B(\xi)_{Cb}\} \mid \dfrac{K}{\Lambda} \leq 2 \\ M = \{B(\xi)_{Cr} \curlyvee B(\xi)_{Cb} \curlyvee B(\xi-1)_{Cr}\} \mid \dfrac{K}{\Lambda} \leq 3 \\ M = \{B(\xi)_{Cr} \curlyvee B(\xi)_{Cb} \curlyvee B(\xi-1)_{Cr} \curlyvee B(\xi-1)_{Cb}\} \mid \dfrac{K}{\Lambda} \leq 4 \end{cases}, \qquad (2.3)$$

де $B(\xi)_{Cr}$ та $B(\xi)_{Cb}$ - множини біт ξ - го розряду каналів Cr та Cb відповідно;

$B(\xi-1)_{Cr}$ та $B(\xi-1)_{Cb}$ - множини біт $(\xi-1)$ - го розряду каналів Cr та Cb відповідно.

Застосування методу останнього біта у класичній реалізації має недолік, який полягає у тому, що модифікація LSB-біт вносить помітні зміни у структуру наймолодшого (або кількох наймолодших) розрядів [13, 14].

Звичайно, такі зміни непомітні для зору людини (рис.2.7), проте вони легко виявляються одним з найпростіших алгоритмів стегоаналізу, а саме – методом візуальної атаки (рис.2.8).

Відповідно, з цієї причини метод останнього біта зараз не використовується у чистому вигляді. Натомість його використовується як технологічний базис для розробки більш сучасних алгоритмів маскування, що базуються на загальних засадах LSB.

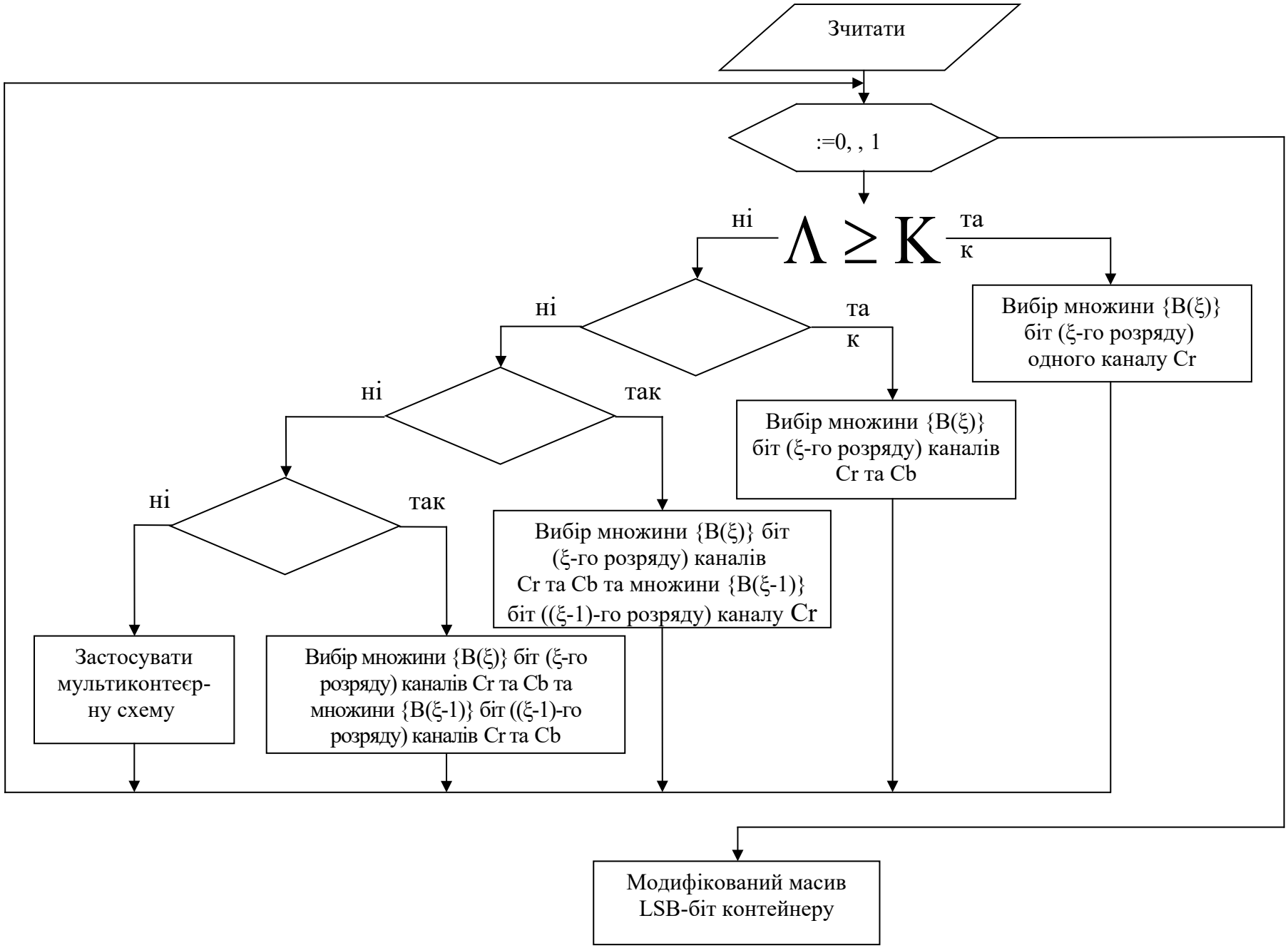


Рисунок 2.6 – Схема вибору режиму модифікації LSB-біт

Рисунок 2.7 – Графічний контейнер JPEG (1366x768), що містить частину поеми «Іліада»

Рисунок 2.8 – Сукупність наймолодших біт графічного контейнеру JPEG виявлена у результаті візуальної атаки

2.2.3 Метод маскування даних на базі дискретного косинусного перетворення

Як і попередньо розглянутий метод останнього біта, даний метод використовує у якості кнтейнерів JPEG-файли. Але, на відміну від методу останнього біту, метод маскування даних на базі дискретного косинусного перетворення відзначається суттєво нижчою ємністю С контейнеру [11, 12].

Так, якщо для методів LSB-орієнтованих може забезпечуватися показник ємності до 1/6 контейнеру, даний метод передбачає можливість інкапсуляції 2 біт у $b'(k)_{(i,j)}$ у трансформований блок $s_{x,y}$.

Перевагою даного методу є те, що переважна більшість програм перегляду файлів, написаних за стандартними рекомендаціями, а також алгоритмів стегоаналізу, не зданті виявити факт модифікації.

Це пояснюється наступним:

- метод не передбачає безпосередню зміну одного біта, коли необхідно внести у контейнер 1 біт $b'(k)_{(i,j)}$ приховуваного повідомлення;

- відсутні типові ознаки модифікації (незмінні наймолодший розряд, статистичні характеристики та ін.).

За ідеєю методу, інкапсуляція біт секретного повідомлення здійснюється у контейнер після етапу дискретного косинусного перетворення (рис.2.9).

При цьому, якщо у трансформованому блоці $s_{x,y}$ різниця абсолютних значень компонент перевищує деяку величину ε, вважається, що такий блок $s_{x,y}$ буде здійснювати передачу 0.

Якщо ж різниця абсолютних значень компонент менше деякого від'ємного значення $(-\varepsilon)$, відповідно, передається символ 1.

Математично це може бути показано наступним виразом:

$$\begin{cases} \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| > \varepsilon \rightarrow b'(k)_{(i,j)} = 0 \\ \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| < -\varepsilon \rightarrow b'(k)_{(i,j)} = 1 \end{cases}, \qquad (2.4)$$

де $\eta(ch)_{x,y}^{(max)}$ та $\eta(ch)_{x,y}^{(min)}$ - величини максимального та мінімального значень компонент у перетвореному блоці $s_{x,y}$ каналу ch відповідно.

Так як розподіл значення величини ε у межах кадру носить довільний характер, для того, щоб на базі виразу (2.4) можна було налагодити процес інкапсуляції біт секретного повідомлення, очевидно, що значення ε потребує корегування відповідно до закону зміни самого повідомлення.

Рисунок 2.9 – Місце етапу маскування даних на базі дискретного косинусного перетворення у загальному каскаді JPEG-перетворень

З зазначеного виходить, що для того, щоб забезпечити цілісність вихідного контейнеру та візуальну його незмінність у результаті інкапсуляції, модифікація значень компонент може здійснюватися виключно у каналах Cr та Cb, оскільки зміни у яскравісному каналі можуть бути помітними.

При цьому, необхідність попереднього корегування величин $\eta(ch)_{x,y}^{(max)}$ та $\eta(ch)_{x,y}^{(min)}$ визначається наступним співвідношенням:

$$\begin{cases} \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| < \varepsilon \\ \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| > -\varepsilon \end{cases} \quad (2.5)$$

У разі, якщо співвідношення (2.5) для будь-якого трансформованого блоку $s_{x,y}$ довільного змісту є справедливим, відповідно, величини $\eta(ch)_{x,y}^{(max)}$ та $\eta(ch)_{x,y}^{(min)}$ необхідно змінити на величину $\Delta\eta$, що визначається як:

$$\Delta\eta = \varepsilon - \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| \quad (2.6)$$

При цьому, розглядаються такі випадки, як:

- зміні підлягає одна з величин - $\eta(ch)_{x,y}^{(max)}$ або $\eta(ch)_{x,y}^{(min)}$;

- модифікуються певним тином обидві величини $\eta(ch)_{x,y}^{(max)}$ та $\eta(ch)_{x,y}^{(min)}$.

Очевидно, що у ряді випадків зміна значення $\eta(ch)_{x,y}^{(max)}$ вище деякого порога, що залежить від особливостей змісту самого сегменту, може викликати візуально помітне спотворення.

На цей випадок, з одного боку, доцільним є виконання змін компонент $\eta(ch)_{x,y}^{(min)}$, які при цьому відповідають ВЧ-складовій трансформованого блоку. Це пояснюється тим, що модифікація високочастотних компонент або взагалі присутність або виключення їх з опису сегменту не вносить суттєвих візуальних викривлень.

З іншого боку, зазвичай зміна величини $\eta(ch)_{x,y}^{(min)}$ здійснюється тоді, коли є потреба інкапсуляції одиничного елементу, а при вбудовуванні символу 0 виконується (за потреби) зміна максимальної компоненти $\eta(ch)_{x,y}^{(max)}$.

Тоді для того, щоб усунути ймовірність візуальних змін у ході інкапсулювання, контейнером вибирається зображення формату JPEG, що має високу ступінь насиченості.

У підсумку загальний алгоритм вбудовування приховуваних даних на базі дискретного косинусного перетворення буде мати вигляд, як показано рис.2. 10.

У свою чергу, вилучення вбудованих даних з контейнеру на прийомному боці здійснюється на базі наступного співвідношення:

$$\begin{cases} b'(k)_{(i,j)} = 0 \mid \left|\eta(ch)_{x,y}^{(max)}\right| > \left|\eta(ch)_{x,y}^{(min)}\right| \\ b'(k)_{(i,j)} = 1 \mid \left|\eta(ch)_{x,y}^{(max)}\right| < \left|\eta(ch)_{x,y}^{(min)}\right| \end{cases} \quad (2.7)$$

На відміну від класичного LSB, даний метод приховування секретних повідомлень на базі графічних контейнерів сьогодні застосовується. З його допомогою здійснюється нанесення ЦВЗ (цифрових водяних знаків).

Модифікацією розглянутого методу може вважатися т.з. метод *Langelaar.*

Як і базовий метод на базі ДКП, метод Langelaar функціонує на рівні обробки трансформованих сегментів $s_{x,y}$ та містить у собі такі кроки, як:

1. Генерація псевдовипадкової двійкової маски з одиничних та нульових елементів $\text{rand}(x,y) \in \{0,1\}$.

2. Поділ трансформованого блоку $s_{x,y}$ на 2 частини - $s(1)_{x,y}$ та $s(2)_{x,y}$ залежно від згенерованої маски.

3. Обчислення середнього значення яскравості для субблоку $s(1)_{x,y}$ за виразом:

$$\overline{\eta}(Y)_{x,y} = \frac{\sum_{x=1}^{8-\alpha}\sum_{y=1}^{8-\beta}\overline{\eta}(Y)_{x,y}}{(8-\alpha)(8-\beta)}, \quad (2.8)$$

де α та β – величини, на які розмір субблоку $s(1)_{x,y}$ менший початкового блоку $s_{x,y}$.

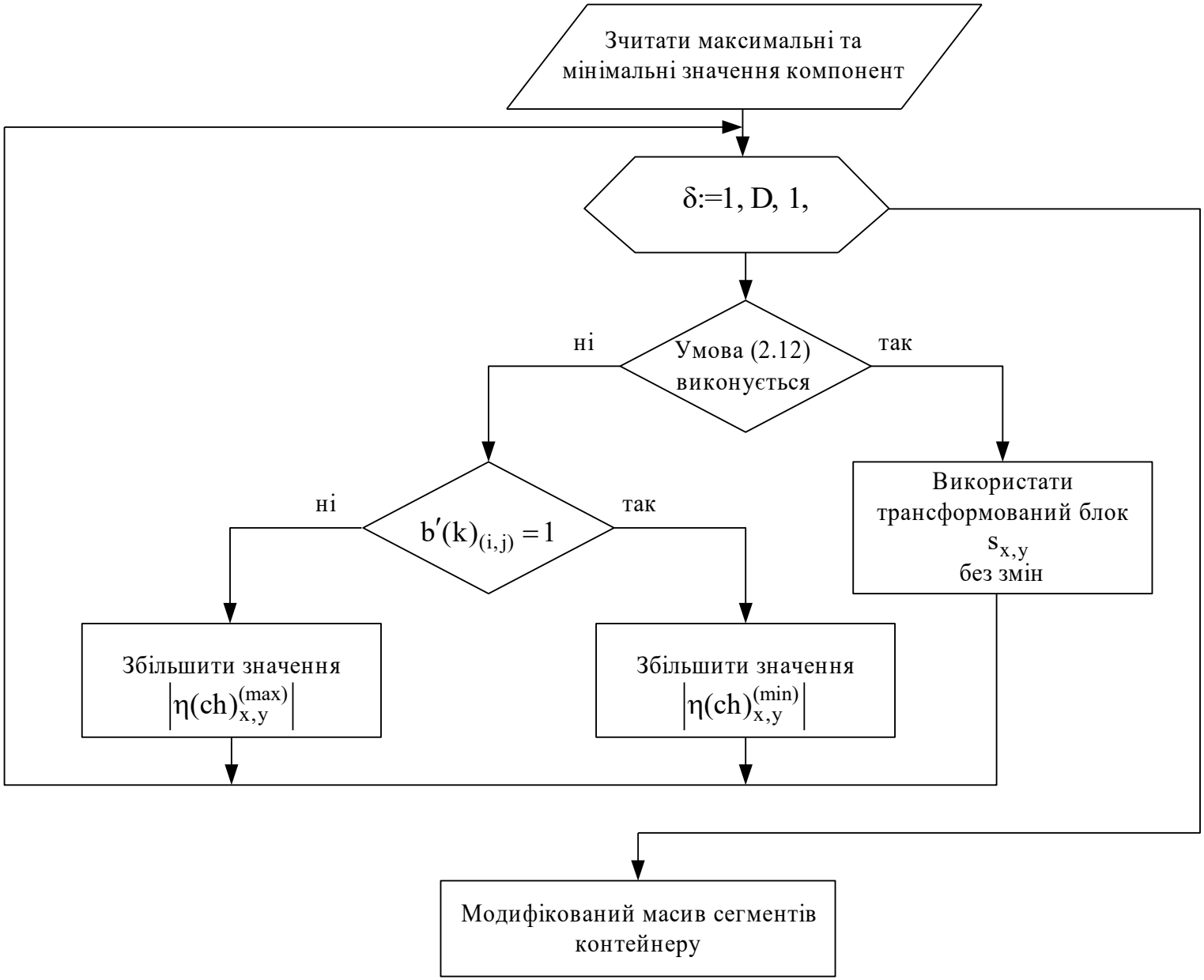


Рисунок 2.10 – Загальна схема алгоритму вбудовування приховуваних даних на базі дискретного косинусного перетворення за встановленою величиною ε

Відповідно, середнє значення яскравості для субблоку $s(2)_{x,y}$ визначається наступним чином:

$$\overline{\eta}(Y)_{x,y} = \frac{\sum_{x=1}^{\alpha}\sum_{y=1}^{\beta}\overline{\eta}(Y)_{x,y}}{\alpha\beta}. \quad (2.9)$$

4. Встановлення порогового значення Φ. Після цього біт $b'(k)_{(i,j)}$ секретного повідомлення інкапсулюється у сегмент на базі наступного принципу:

$$b'(k)_{(i,j)} = \begin{cases} 1, \mid s(1)_{x,y} - s(2)_{x,y} > \Phi, \\ 0, \mid s(1)_{x,y} - s(2)_{x,y} < -\Phi. \end{cases} \quad (2.10)$$

Якщо умова, задана співвідношенням (2.10), не виконується, значення компонент яскравості субблока $s(2)_{x,y}$ змінюється.

Відповідно, для вилучення біта $b'(k)_{(i,j)}$ прихованого повідомлення на прийомному боці виконується розрахунок середніх величин яскравості для субблоків $s(1)_{x,y}$ та $s(2)_{x,y}$. Далі вилучення біта $b'(k)_{(i,j)}$ здійснюється на базі наступного співвідношення:

$$b'(k)_{(i,j)} = \begin{cases} 1, \mid s(1)_{x,y} - s(2)_{x,y} > 0, \\ 0, \mid s(1)_{x,y} - s(2)_{x,y} < 0. \end{cases} \quad (2.11)$$

Беззаперечною перевагою розглянутого методу є складність виявлення факту наявності заповненого контейнеру. У той же час, його головним недоліком є погана робастність (стійкість до перетворень). У підсумку це обмежує застосовуваність даного алгоритму маскування даних.

Додамо, що метод маскування даних на базі дискретного косинусного перетворення є залежним від застосовуваних контейнерів [14]. Рівень захищеності даних на його базі визначається особливостями змісту графічного контейнеру і у окремих випадках забезпечується значною мірою,

прте непоодинокими є випадки, коли деякі контейнери зазнавали помітного людським зором стотворення у наслідок інкапсулювання даних (рис.2.11).

Рисунок 2.11 – Приклад візуального спотворення контейнеру

За викладеним матеріалом можна зазначити наступне:

- розглянуто ключові дві групи загальних підходів до побудови стегосистем;
- показано, що група методів, яка базується на розміщенні приховуваних даних у межах не використовуваних ділянок файлосховищ, та у спеціалізованих сегментах файлів, характеризується низьким рівнем захищеності інформації і тому сьогодні, як практичний інструмент маскування даних, не використовуються;
- досліджено ключові засади функціонування методів, що використовують надмірність опису файлів деяких типів для розміщення даних, які має бути масковано; доведено, що стандартизованим методам, що відносяться до даної групи, властивий набагато вищий рівень захищеності даних, проте на сьогодні добре відомі як принципи їх функціонування, так і характерні ознаки, за якими у ході стегоаналізу може бути виявлено

заповнений контейнер. Це властиво, зокрема, для методів, які передбачають модифікацію молодшого розряду двійкового опису зображення. Разом з тим, алгоритм, який виконує інкапсуляцію біт секретного повідомлення у компоненти сегменту після ДКП, виходячи з його характеристик, з одного боку, характеризується суттєво вищим рівнем захищеності даних, а з іншого – недостатнім рівнем робастності (стійкості до перетворень).

Таким чином, більшість поширених методів стегозахисту, з причини існуючих для них обмежень та недоліків, на сьогодні може бути застосовано виключно як базис для розробки більш досконалих алгоритмів маскування.

3. МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ

3.1 Обгрунтування доцільності використання графічних мільтиконтейнерів як базису для методу маскування даних

Серед зазначених раніше показників, що характеризують продуктивність стеганографічного алгоритму, були наступні:

- відносна ємність стегосистеми;
- показник швидкодії алгоритму;
- обчислювальна складність алгоритму;
- ресурсоємність алгоритму.

Разом з тим, для того, щоб однозначно стверджувати про продуктивність того чи іншого стегоалгоритму, необхідно також ураховувати додаткову специфіку, таку, як:

- орієнтованість алгоритму на обробку контейнерів певного типу;
- використання моноконтейнерів, чи контейнерів потокового класу.

Як зазначалося раніше, найбільш ефективними зараз можна вважати алгоритми, які орієнтуються на використання графічних JPEG-контейнерів. Це пояснюється тим, що [11-13, 15, 16]:

- файли типу JPEG мають дуже широку застосовуваність у мережі, та поширюються як самостійні об’єкти, так і як складники гіпертексту;
- розмір файлів JPEG є одними з найнижчих серед існуючих графічних форматів, при цьому роздільна здатність зображення може бути досить високою, що дозволяє вбудовувати у такий контейнер значну кількість біт секретного повідомлення;
- надмірність опису JPEG є досить високою, та включає у себе щонайменше психовізуальну, кодову та структурно-комбінаторну надмірності.

У той же час, створюються умови, у яких доцільним для використання є мультиконтейнери, або контейнери потокового типу.

Цьому сприяє, з одного боку, постійно зростаючий відсоток відео у мережі, а з іншого боку - збільшення обсягу даних, що потребують приховування.

При цьому, понад 90% відео у мережі кодується на базі технологій MPEG. У цьому випадку на рівні обробки потоку кадрів використовуються загальні засади JPEG-перетворення.

Це дає змогу розглядати відеопотік MPEG як множину потенційних контейнерів.

Разом з тим, як було визначено у розділі 2, стандартизовані методи стеганографії обмежені у застосування або з причини низької робастності, або з причин легкого викриття існуючими засобами стегоаналізу.

У таких умовах актуальними є підходи до маскування даних у графічних контейнерах, яким не властиві недоліки існуючих стегоалгоритмів.

3.2 Вибір частотної області сегменту у його спектральному описі для інкапсуляції даних

Розглянемо приклад блоку $s_{x,y}$, який було попередньо піддано ортогональному перетворенню та квантуванню (рис.3.1) [9].

38	29	14	25	6	8	0	0
27	7	9	11	9	0	0	8
21	14	7	0	7	6	0	0
19	10	0	5	0	0	0	0
5	0	0	10	0	0	0	0
11	0	0	0	5	0	0	0
5	5	7	0	0	0	0	0
0	6	6	5	0	0	0	0

НЧ-область;

головна діагональ

Рисунок 3.1 – Приклад блоку $s_{x,y}$ після виконання ортогонального перетворення та квантування

Як видно з рис. 3.1, округлення з порогом 5, до блоку $s_{x,y}$ було застосовано округлення з порогом ν_{th} рівним 5, так як компоненти, величина яких менше 5, відсутні.

При цьому, у межах НЧ-області присутні компоненти, які є найбільш інформативними.

На базі них може бути сформовано загальні обриси фрагменту зображення.

У свою чергу, компоненти області середніх частот, що умовно містяться нижче НЧ-області та у зоні головної діагоналі, деталізують зображення, наповнюючи його дрібними деталями.

У той же час, ВЧ-складові не несуть критичної інформації для того, щоб забезпечувати семантичну цілісність зображення.

Тому компоненти ВЧ-області квантуються найбільше.

Зображення, де ВЧ-складова відквантована незначно, містить велику кількість найдрібніших фрагментів, діаметри яких не перевищують 1-2 пікселя (рис.3.2).

За ідеологією JPEG максимальне скорочення первинної кількості біт для представлення вихідного зображення забезпечується на етапі квантування, що фактично являє собою по елементний поділ значень компонент $\eta(ch)_{x,y}$ на відповідний коефіцієнт квантування $\vartheta(ch)_{x,y}$.

Тобто, підсумкова величина $\eta'(ch)_{x,y}$ компоненти у результаті квантування визначатиметься як:

$$\eta'(ch)_{x,y} = \frac{\eta(ch)_{x,y}}{\vartheta(ch)_{x,y}}. \qquad (3.1)$$

При цьому, такі коефіцієнти формують матрицю квантування, де величини $\vartheta(ch)_{x,y}$ розподіляються наступним чином:

$$\varphi(\eta(ch)_{x,y}) \uparrow \rightarrow \vartheta(ch)_{x,y} \uparrow, \qquad (3.2)$$

де $\varphi(\eta(ch)_{x,y}$ - частота компоненти $\eta(ch)_{x,y}$ на позиції (x,y) у блоці.

Рисунок 3.2 – Приклад зміни деталізації фрагментів зображення для незначного а) та високого б) рівнів пригнічення ВЧ-складової

Також справедливою є залежність між коефіцієнтами квантування на одній і тій же позиції (x,y) для хроматичних компонент та компонент

яскравості:

$$\vartheta(Y)_{x,y} < \vartheta(Cr)_{x,y}, \vartheta(Cb)_{x,y} \quad (3.3)$$

Збільшення величини $\vartheta(ch)_{x,y}$ за принципом, описаним виразом (3.2) при цьому сприяє найбільшому пригніченню ВЧ-складової та у підсумку – забезпеченню максимального коефіцієнта стиснення.

Як бачимо з аналізу рис.3.2, збільшення рівня пригнічення ВЧ-складової позбавляє зображення деталізації, але семантична значимість при цьому не втрачається.

Виняток становлять випадки застосування надвисоких степенем стиснення, коли спостерігається руйнування структури зображення унаслідок проявлення ефекту мазаїки та ефекту Гібса.

Як свідчить статистика [5, 9, 11], у складі більшості трансформованих блоків $s_{x,y}$, що попередньо підлягали квантуванню та округленню, ймовірність появи значущих компонент знижується за рухом від головної діагоналі до компоненти АС (що знаходиться у правому нижньому куті блоку).

При цьому, поява ненульових компонент для ВЧ-області спостерігається суттєво нижче, ніж для зони середніх частот.

Така частота появи залежить від особливостей змісту фрагменту зображення.

Ще однією важливою особливістю є те, що квантування, або повністю обнулення компонент $\eta(ch)_{x,y}$ нижче головної діагоналі не вносить помітних спотворень у відновлений фрагмент зображення.

Таким чином, зона кількох діагоналей нижче головної попередньо трансформованого та квантованого з округленням блоку $s_{x,y}$, з одного боку, статистично може мати входження значущих компонент, що відрізняються невисокими амплітудами.

З іншого боку, усунення або модифікація присутніх у даній зоні компонент не приводить до візуальних змін у вихідному зображенні.

З цього міркування дана область (рис.3.3) може розглядатися як потенційно прийнятна для вбудовування даних секретного повідомлення.

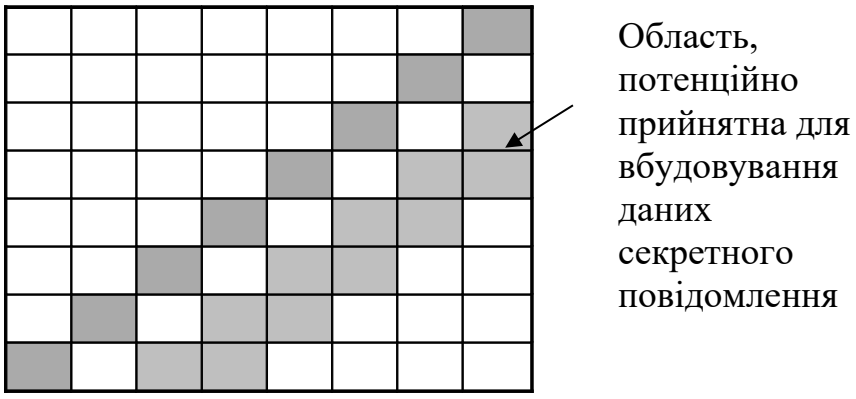


Рисунок 3.3 – Локалізація ймовірної частотної зони для інкапсулювання біт приховуваного повідомлення

Інакше кажучи, поява значущих компонент у ВЧ-області викликає підозру, тому з цієї точки зору більш підходячою є частина трансформованого блоку, наведена рис.3.3.

Розглянемо умови, за яких може бути побудовано алгоритм стеганографічного приховування даних на базі модифікації локальної зони ВЧ-СЧ-компонент трансформованого блоку.

3.3 Умови, у яких існує потенційна можливість реалізації алгоритму стеганографічного приховування даних на базі модифікації локальної зони ВЧ-СЧ-компонент трансформованого блоку

Для зменшення ймовірності виявлення заповненого контейнеру необхідно, щоб для нього, у порівнянні з пустим контейнером, забезпечувалося:

- візуальна незмінність;
- відсутність або незначні зміни статистичних характеристик.

В умовах, коли необхідно модифікувати деяку частину ВЧ-СЧ-компонент, розуміння зазначених вище умов може бути інтерпретовано, наступним чином [6, 7, 16]:

- кількість r біт $b'(k)_{(i,j)}$ приховуваного повідомлення, які може бути вбудовано у зону ВЧ-СЧ-компонент нижче головної діагоналі, має бути

суттєво меншою, ніж кількість g значущих компонент $\eta(ch)_{x,y}$ після виконання процедур квантування та округлення, тобто:

$$r << g; \tag{3.4}$$

- за наявності у зоні, потенційно прийнятній для інкапсуляції даних секретного повідомлення значущих компонент $\eta(ch)_{x,y}$, з точки зору збереження статистичних характеристик сегменту $s_{x,y}$ більш доцільною є зміна їх абсолютного значення на деяку величину $\Delta\eta$, ніж штучне внесення значущих компонент відповідно до закону зміни самого повідомлення;
- необхідно ураховувати зв'язок між кількістю g значущих компонент $\eta(ch)_{x,y}$ після виконання процедур квантування та округлення та величиною порога ν_{th} округлення, а саме:

$$\nu_{th} \uparrow \rightarrow g \downarrow . \tag{3.5}$$

Для того, щоб потенційно забезпечити високу ймовірність знаходження у межах ВЧ-СЧ-компонент нижче головної діагоналі кількість g значущих компонент, у якості контейнера доцільно використовувати кадри відеоряду, або їх окремі фрагменти, що характеризуються високою ступінню насиченості (рис.3.4).

а)

б)

в)

Рисунок 3.4 – Приклади ненасиченого а), середньо насиченого б) та насиченого зображень в)

При цьому, очевидно, що в окремих випадках насичені ділянки може бути локалізовано також у складі кадрів, яким відповідає низька насиченість.

Отже, у підсумку вбудовування даних секретного повідомлення передбачається здійснювати у ділянки зображення (сегменти $s_{x,y}$), яким відповідає високий рівень насиченості.

Таким чином, необхідно розробити інформативну ознаку, на базі якої буде виконуватися виявлення насичених ділянок.

3.4 Розробка інформативної ознака, на базі якої виконується виявлення насичених ділянок відеокадрів

Для того, щоб сприяти ефективному виявленню сегментів різного ступеню насиченості, інформативна ознака Ω має відповідати вимогам [17]:

- забезпечення оцінки насиченості трансформованих сегментів $s_{x,y}$ у реальному часі;
- створення мінімального обчислювального навантаження на систему;
- можливість виявлення сегментів насиченого, середньо-насиченого на насиченого типів незалежно від особливостей змісту оброблюваних відеокадрів;
- однозначне виявлення належності сегменту до того чи іншого класу насиченості.

У якості такої ознаки можуть розглядатися наступні показники, та їх комбінації:

- ступінь D_{spctrl} структурної складності фрагменту $s_{x,y}$;
- складність фрагменту $s_{x,y}$ у просторовому описі D_{sptl};
- величина динамічного діапазону σ амплітуд компонент у спектральному описі.

При цьому, показник D_{spctrl} структурної складності трансформованого фрагменту $s_{x,y}$ розглядається як функціонал від середньої довжини $\overline{\ell_i}$ серії нульових елементів, виявлених у межах трансформованого фрагменту $s_{x,y}$, тобто:

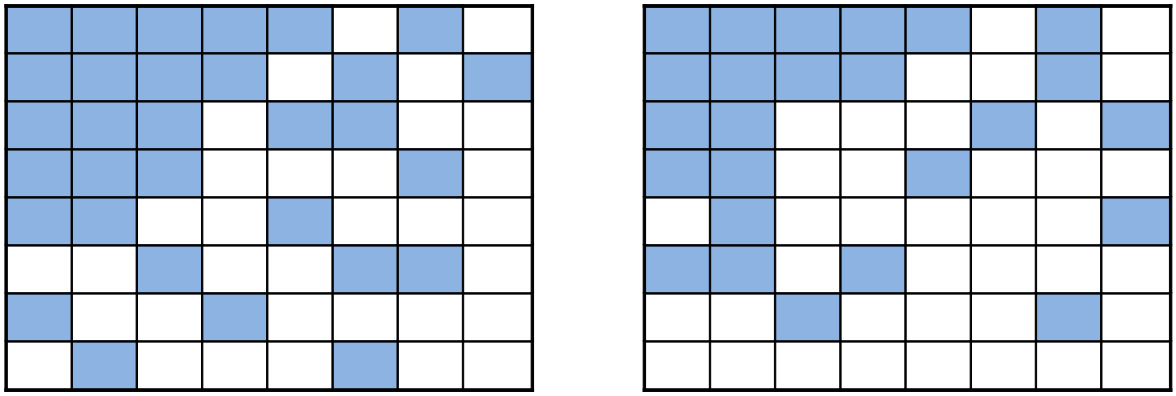
$$D_{spctrl} = f(\overline{\ell_i}) = \frac{\sum_{i=1}^{\mu_\ell} \ell_i}{\mu_\ell}, \tag{3.6}$$

де ℓ_i - довжина і-ї серії нульових елементів;

μ_{ℓ} - кількість нульових серій, виявлених у межах трансформованого фрагменту $s_{x,y}$.

Фізична сутність даного показника полягає у тому, що збільшення величини D_{spctrl} у загальному випадку означає, що значні ділянки трансформованого фрагменту $s_{x,y}$ не містять значущих компонент $\eta(ch)_{x,y}$ (рис.3.5) [11].

При цьому, у випадку $D_{spctrl} \to \min$ може бути зроблено висновок, що у структурі сегменту присутні значущі компоненти $\eta(ch)_{x,y}$, на ділянках між якими локалізуються серії нульових елементів з довжинами, що тяготіть до мінімальних. Тобто, структура такого сегменту $s_{x,y}$ вважається складною.



а) б)

Рисунок 3.5 – Приклади трансформованих сегментів різного ступеню структурної складності: високої складності а), для якого $\overline{\ell_i} \approx 2$, та низької складності б) , для якого $\overline{\ell_i} \approx 5{,}5$

У свою чергу, складність фрагменту $s_{x,y}$ у просторовому описі D_{sptl} може бути визначена на базі наступного виразу:

$$D_{sptl} = \sum_{x=1}^{8} (p(Y)_{x,y}^{(max)} - p(Y)_{x,y}^{(min)}), \qquad (3.7)$$

де $p(Y)_{x,y}^{(max)}$ та $p(Y)_{x,y}^{(min)}$ - максимальна, та, відповідно, мінімальна величина яскравості пікселя рядка у YCrCb-описі.

Інакше кажучи, показник D_{sptl} являє собою суму по 8 рядкам сегменту $s_{x,y}$ у просторовому описі різниць мінімальних та максимальних величин яскравості піскелів.

При цьому, величина динамічного діапазону σ амплітуд компонент у спектральному описі може бути обчислена як різниця добутків величин амплідут компонент НЧ-зони та компонент, що знаходяться нижче головної діагоналі сегменту $s_{x,y}$ у спектральному описі [3, 4]:

$$\sigma = \prod_{i=1}^{10} \left| \eta(ch)_{x,y}^{(i)} \right| - \prod_{j=37}^{64} \left| \eta(ch)_{x,y}^{(j)} \right|, \tag{3.8}$$

де $\prod_{i=1}^{10} \left| \eta(ch)_{x,y}^{(i)} \right|$ - добудок 10-и модулів НЧ-компонент;

$\prod_{j=37}^{64} \left| \eta(ch)_{x,y}^{(j)} \right|$ - добуток модулів компонент нижче головної діагоналі.

У загальному випадку, якщо не зазначено іншого, передбачається наявність 3 рівнів градації значень для кожного з показників - σ, D_{sptl} та D_{spctrl}. При цьому, межі кожного з рівнів визначаються відносно максимального показника, який визначається на рівні одного кадру F відео потоку. Наприклад, якщо у кадрі виявлено максимальну величину складності фрагменту $D_{sptl}^{(max)}$ у просторовому описі, яка дорівнює γ, тоді усі сегменти, даний показник для яких знаходиться у діапазоні $[\gamma; 0{,}7\gamma)$, визнаються такими, що належать до складних. Далі, сегменти, для яких $D_{sptl} \in [0{,}7\gamma; 0{,}4\gamma)$ класифікуються як середньо-складні. Врешті-решт, при $D_{sptl} \in [0{,}4\gamma; 0]$ сегмент вважається нескладним у просторовому описі. Аналогічним чином здійснюється розподіл сегментів за складністю по двом іншим показникам.

У підсумку, аналітично інформативна ознака Ω належності сегменту $s_{x,y}$ до того чи іншого класу формується як функціонал поєднання вищенаведених показників, тобто:

$$\Omega = \phi(\sigma; D_{sptl}; D_{spctrl}). \quad (3.9)$$

Водночас, у практичному аспекті рішення про віднесення сегменту $s_{x,y}$ до певного типу семантичної складності приймається на базі аналізу величин окремих його показників відповідно до наступного правила: якщо хоча б 2 з 3 параметрів відносяться до класу складних, робиться припущення про належність сегменту до множини W семантично складних. Водночас, належність 3 параметрів до класу складних означає автоматичне маркування сегменту як семантично складного (також відноситься до множини W). При цьому, складність фрагменту за параметром σ та одним з двох інших (D_{sptl} та D_{spctrl}) також дає можливість визнати його семантично складним. Математично така закономірність може бути відображена наступним співвідношенням:

$$\left.\begin{array}{c} \sigma \in M_d \ \& \ D_{sptl} \in P_d \\ \sigma \in M_d \ \& \ D_{spctrl} \in Q_d \\ \sigma \in M_d \ \& \ D_{sptl} \in P_d \ \& \ D_{spctrl} \in Q_d \end{array}\right\} \Rightarrow s_{x,y} \in W, \quad (3.10)$$

де M_d - множина сегментів, що є складними за показником σ динамічного діапазону амплітуд компонент у спектральному описі;

P_d - множина сегментів, що є складними за показником D_{sptl} складності у просторовому описі;

Q_d - множина сегментів, що є складними за показником D_{spctrl} структурної складності у спектральному представленні.

Загальна схема пошуку сукупності $\{s_{x,y}\}$ сегментів кадру, що відносяться до множини семантично-складних, ілюструється рис. 3.6.

Разом з тим, якщо сегмент $s_{x,y}$ до множини семантично складних не

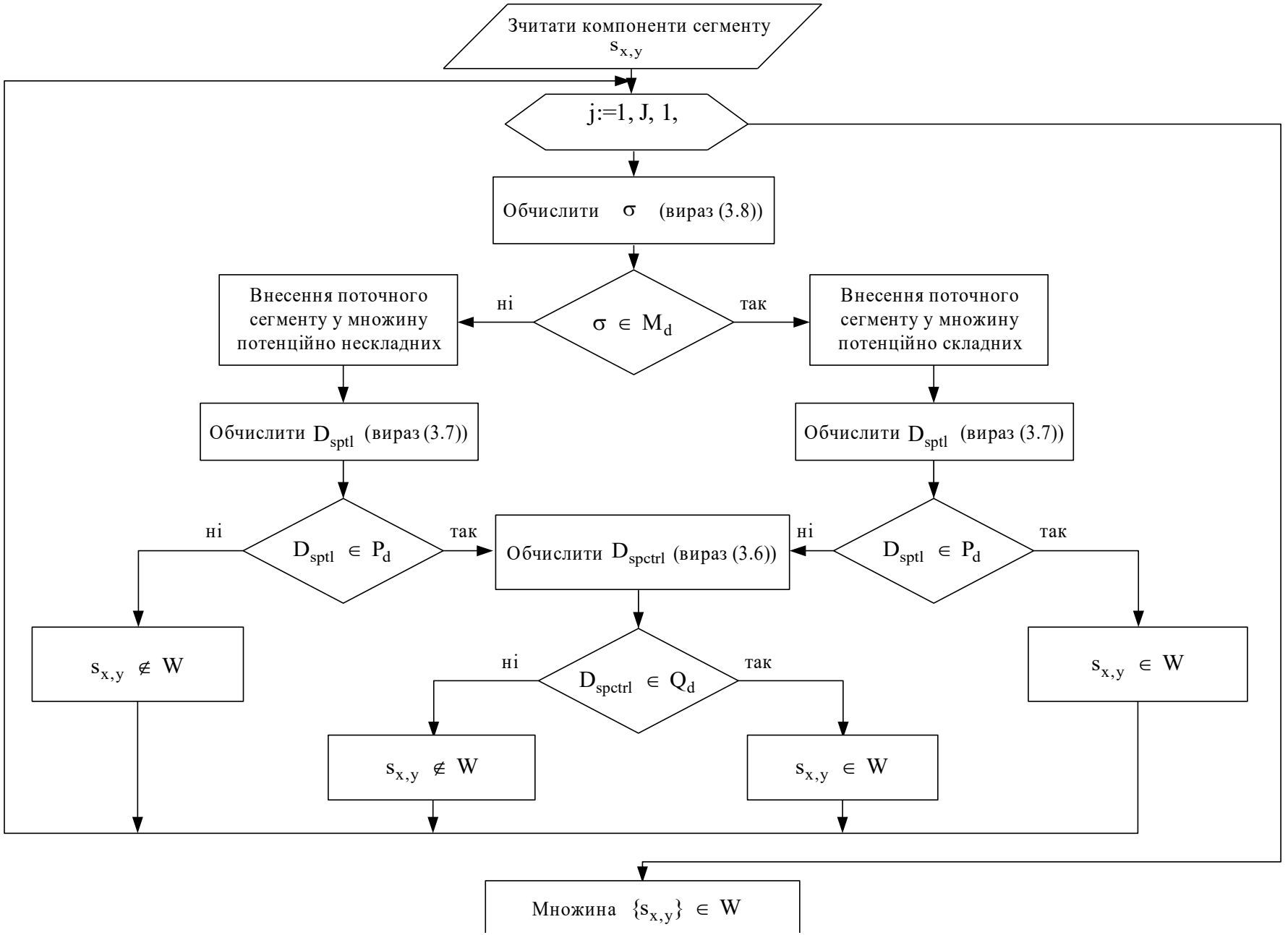


Рисунок 3.6 – Загальна схема визначення належності сегменту до множини семантично-складних

відноситься, у процесі вбудовування даних на наступних етапах обробки від участі не бере [11].

На рис. 3.10 змінна j – поточний індекс сегменту, що аналізується, J – загальна кількість сегментів у кадрі.

3.5 Процес інкапсуляції біт секретного повідомлення на базі модицікації локальної зони ВЧ-СЧ-компонент трансформованого блоку

Як було визначено раніше, потенційно прийнятними для модифікації можуть бути компоненти 3 44 по 54 позиції у лінеаризованому описі (рис.3.3) [3, 6, 7, 9].

Це відповідає координатам у двовимірному масиві сегменту $s_{x,y}$ з (3,8) по (8,4).

На початку роботи алгоритму виконується зчитування компонент у даному діапазоні.

При цьому, належність сегменту до класу семантично-складних гарантує наявність у зазначеній області тієї чи іншої кількості значимих компонент після виконання процедур квантування та округлення.

У свою чергу, після визначення сукупності значимих компонент $\eta(ch)_{x,y}$ у зазначеній області, визначається їх множина L, що може бути модифікована.

При цьому, необхідно керуватися умовою (3.4), за якою кількість r біт $b'(k)_{(i,j)}$ приховуваного повідомлення, що може бути інкапсульовано, має бути суттєво меншою, ніж кількість g значущих компонент.

Це необхідно для підвищення стійкості алгоритму до стегоаналізу. Відповідно до цього, керуючись кількістю g виявлених значущих компонент, розмірність множини L визначається як:

$$L_{size} = \text{trunc}\frac{g}{s}, \qquad (3.11)$$

де s найчастіше приймається рівним 2.

Після того, як розмірність L розраховано, виконується визначення компонент, які беруть участь у процесі інкапсуляції. До такого процесу

визначення індексів компонент, що буде включено до множини L висуваються наступні вимоги:

1. Однозначна ідентифікація модифікованих компонент на прийомному боці, що гарантує функціональність усієї стегосистеми у цілому.

2. Функціонування без необхідності використання додаткових службових даних, що зменшує вагу самого фрагменту $s_{x,y}$ та збільшує стегостійкість.

3. Простота реалізації, що сприяє зменшенню загальної обчислювальної складності алгоритму.

Тут загальними службовими даними, що не потребують додаткового виокремлення у відповідні службові поля може бути сукупність даних про особливості змісту сегменту $s_{x,y}$ - кількість одиничних нульових та значущих елементів, кількість біт $v_{x,y}$ для опису стисненого сегменту тощо.

Разом з тим, більш ефективним є використання розрахованих раніше величин σ, D_{sptl} та D_{spctrl}, що разом формують інформативну ознаку Ω належності сегменту до класу семантично складних. Їх використання дає такі переваги, як:

- відсутність необхідності залучення додаткових даних;
- однозначна інтерпретація на боці як передавача, так і приймача.

Отже, у таких умовах визначення індексів ψ компонент $\eta(ch)_{x,y}$, що входять до множини L у межах одного сегменту $s_{x,y}$, може обчислюватися на базі хеш-функції X від значень σ, D_{sptl}, D_{spctrl}, та L_{size}, розрахованих раніше, та секретного ключа, K, який відомий на боці передавача та приймача, тобто:

$$\psi = X(\sigma; D_{sptl}; D_{spctrl}; L_{size}; K). \qquad (3.12)$$

У виразі (3.12) ψ може приймати значення від 1 до L_{size}, та відображає позицію відповідних компонент у діапазоні від 44 по 54. Далі, значення кожної з ψ -х компонент підлягає модифікації.

У загальному випадку тут може бути використано підходи, що передбачають:

- модифікацію величини компоненти $\eta(ch)_{x,y}$ на деяке значення у

десятковому форматі опису;

- зміна біта $b(\ell)_{(x,y)}$ одного з молодших двійкових розрядів компоненти $\eta(ch)_{x,y}$ за аналогією з методом останнього біта.

Розглянемо окремо кожен з означених підходів.

У першому випадку необхідно пам'ятати, що нижня межа значень компонент $\eta(ch)_{x,y}^{(min)}$ буде не меншою, ніж встановлений попередньо поріг ν_{th} округлення, тобто $\eta(ch)_{x,y}^{(min)} \geq \nu_{th}$.

У зв'язку з цим, одним з варіантів модифікації компонент у ході інкапсуляції даних теоретично може бути підхід, який демонструється далі.

Спочатку компоненти, що віднесено до множини L, підлягають нормалізації, сутність якої може бути подано наступним виразом:

$$\eta'(ch)_{x,y} := \nu_{th} \tag{3.13}$$

Далі нормалізовані компоненти підлягають модифікації, що еквівалентно наступному співвідношенню:

$$\begin{cases} \eta(ch)_{x,y} := \eta'(ch)_{x,y} - trunc(0{,}25\eta'(ch)_{x,y}) \mid b'(k)_{(i,j)} = 1 \\ \eta(ch)_{x,y} := \eta'(ch)_{x,y} + trunc(0{,}25\eta'(ch)_{x,y}) \mid b'(k)_{(i,j)} = 0 \end{cases}, \tag{3.14}$$

де $\eta'(ch)_{x,y}$ - нормалізована компонента (величина якої попередньо приведена до значення ν_{th}).

Коефіцієнт 0,25 у виразі (3.14) вибрано на базі статистичних досліджень про середню домінуючу величину значущих компонент у зазначеному частотному діапазоні сегменту.

Даний підхід дозволяє [11]:

- виконувати однозначне розпізнавання інкапсульованого двійкового символу у компоненти множини L;
- уникнути помітних змін у статистичних характеристиках розподілу двійкових елементів у наслідок як нормалізації, так і наступної модифікації компонент;
- проводити модифікацію значень компонент без внесення

візуально помітних спотворень у підсумковий кадр.

Схема процессу визначення множини компонент, що підлягають інкапсуляції, та безпосередньо самої процедури модицікації даних ілюструється рис. 3.7.

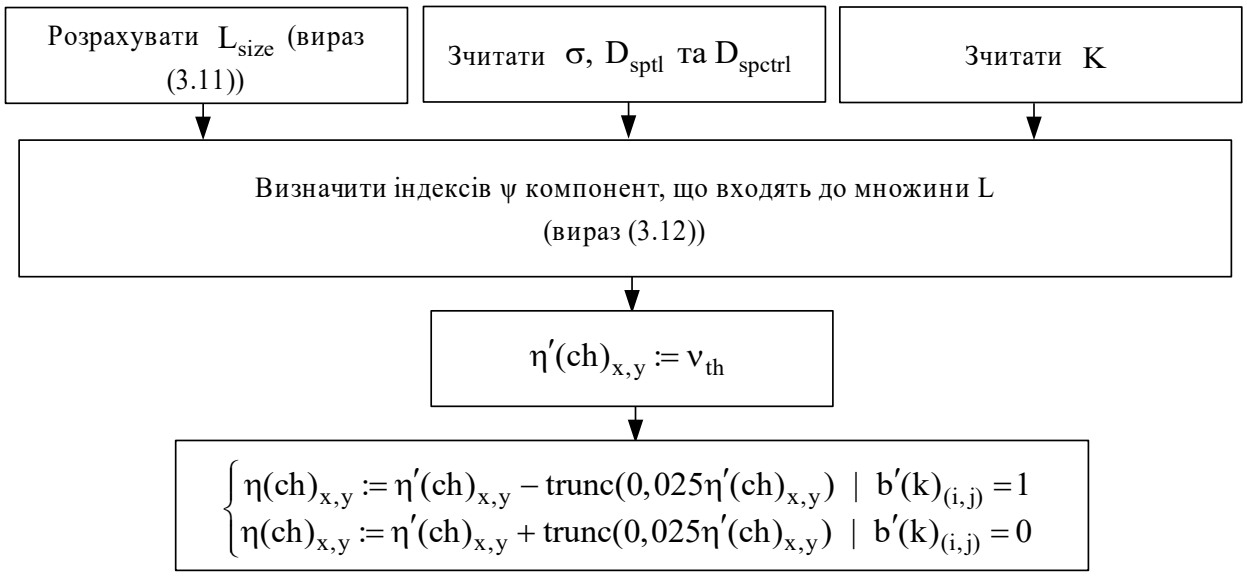


Рисунок 3.7 – Схематичний опис процесу визначення множини компонент для модифікації та безпосередньо інкапсуляції даних

У випадку ж інкапсуляції біт приховуваного повідомлення за принципами, характерними для LSB, попередньо виконується декомпозиція компоненти $\eta(ch)_{x,y}$ до множини двійкових символів відповідно до наступного виразу:

$$\begin{gathered}\eta(ch)_{x,y} = b(n)_{(x,y)}2^{n-1} + b(n-1)_{(x,y)}2^{n-2} + ...b(\ell)_{(x,y)}2^{\ell-1} + ... \\ ... + \theta 2^2 + b(1)_{(x,y)}2 + b(0)_{(x,y)}\end{gathered}, \quad (3.15)$$

$$\ell = \overline{n;0}.$$

У результаті такого перетворення компонента має вигляд множини з n біт, тобто $\eta(ch)_{x,y} = \{b(\ell)_{(x,y)}\}$, або:

$$\eta(ch)_{x,y} = \{b(n)_{(x,y)}; b(n-1)_{(x,y)}; ...; b(\ell)_{(x,y)}; ...; b(1)_{(x,y)}; b(0)_{(x,y)}\}.$$

При цьому, кількість розрядів $Z(\eta(ch)_{x,y})$, що використовуються для двійкового опису компоненти, визначається як

$$Z(\eta(ch)_{x,y}) = \ell og_2(\eta(ch)_{x,y}). \quad (3.16)$$

У випадку, якщо $Z(\eta(ch)_{x,y}) = \overline{4;5}$, модифікації може підлягати 2 біта двійкового опису компоненти, починаючи з молодшого (відповідає 3 розряду). На випадок, коли $Z(\eta(ch)_{x,y}) = 3$, модифікації підлягають біти 2 розряду. Якщо ж $Z(\eta(ch)_{x,y}) \le 2$, інкапсуляція виконується у біт 0 розряду (LSB).

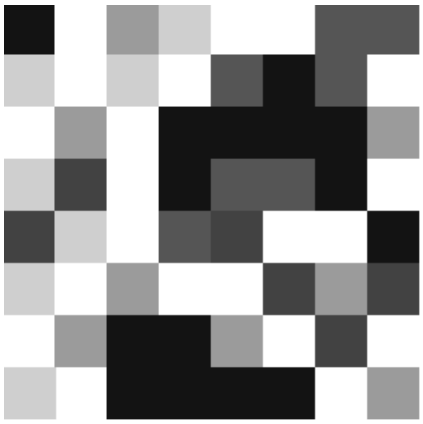
Для кожного з розглянутих випадків інкапсуляція здійснюється таким чином, що значення двійкового елементу $b(\ell)_{(x,y)}$ залишається незмінним у випадку, якщо воно дорівнює біту $b'(k)_{(i,j)}$, який необхідно вбудувати. Дана закономірність демонструється співвідношенням (2.8).

За результатами викладеного матеріалу можемо зазначити наступне:

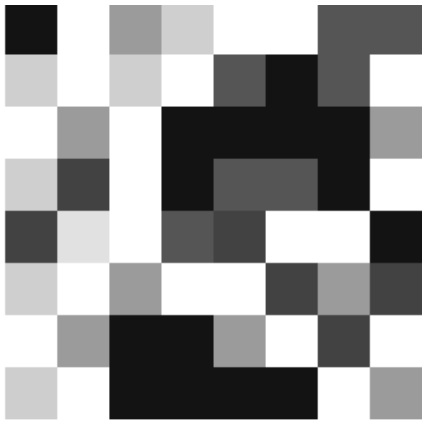
- розглянуто підхід до реалізації алгоритму інкапсуляцію даних у зони ВЧ та СЧ компонент трансформованого сегменту;
- обгрунтовано, що вибір зони стику ВЧ та СЧ компонент нижче головної діагоналі трансформованого сегменту є прийнятним для інкапсуляції біт секретного повідомлення, оскільки модифікація компонент даної частотної області, з одного боку, не викликає візуальних спотворень зображень та помітної зміни статистичних характеристик розподілу двійкових елементів, а з іншого боку, відзначається високою ймовірністю наявності значущих компонент, які і підлягають модифікації;
- показано, що для забезпечення умов наявності достатньої кількості значимих компонент у зазначеній зоні сегменту, доцільно використовувати у якості контейнерів кадри, що відносяться до категорії насичених (високо інформативних);
- досліджено спосіб визначення сегментів кадру, що входять до категорії семантично складних та, відповідно, можуть використовуватися для безпосередньої інкапсуляції даних;
- розглянуто способи виконання процесу вбудовування даних у ВЧ та СЧ компонент нижче головної діагоналі трансформованого сегменту,

зокрема, спосіб, що передбачає модифікацію десяткового значення компоненти, та спосіб, що ґрунтується на засадах LSB; зазначені способи у загальному випадку характеризуються приблизно однаковим обчислювальним навантаженням на систему, оскільки перший з них різниться виключно наявністю у своєму складі процесу нормалізації компонент а другий – операцією декомпозиції десяткової форми опису компоненти до рівня послідовності двійкових елементів.

На рис. 3.8 зображено приклад сегменту 8x8 у просторовому описі, (канал Y) у який попередньо було інкапсульовано 3 біта секретного повідомлення.



а)



б)

0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	0
0	0	0	0	0	0	0	0

в)

Рисунок 3.8 – Приклад вихідного сегменту у просторовому представленні а), сегменту, у який було вбудовано 3 біта секретного повідомлення б), матриця абсолютних різниць компонент

Як показує аналіз рис. 3.8, абсолюнте відхилення значення компонент після інкапсуляції даних відносно їх вихідних величин не перевищує 2 одиниць. У свою чергу, візуальне спотворення сегменту також не спостерігається.

4. ОЦІНКА ПРОДУКТИВНОСТІ МЕТОДУ МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ СЕГМЕНТІВ ЗОБРАЖЕНЬ

4.1 Реалізація методу на базі мультиконтейнерного підходу

Як було зазначено у розділі 3, за результатами інкапсуляції даних у десяткові або двійкові формати опису компонент за розглянутим алгоритмом, стандартизовані методи стегоаналізу не забезпечують детектування заповненого контейнеру. Інакше кажучи, розглянутий алгоритм забезпечує високий рівень L_p захищеності даних.

Також необхідно зазначити, що за існуючими статистичними даними [] семантично складний сегмент $s_{x,y}$ кадру у спектральному представленні у межах частотної зони, визначеної для інкапсулювання біт приховуваного повідомлення, після процедур квантування та округлення може міститися у середньому 5-7 значимих компонент.

Відповідно, за правилом, що подане виразом 3.11, задіюватися для модифікації може половина з них, умовно – 3. Тобто, виконується залежність (1.4), яка описує взаємозв'язок між ємністю C стегосистеми та рівнем L_p її захищеності.

Отже, якщо у межах одного сегменту може бути вбудовано у середньому 3 біти $b'(k)_{(i,j)}$, то для зображення розміром 1280x720 загальна кількість прихованих біт на базі компонент яскравості буде визначатися за виразом [11, 15]:

$$R = \frac{H}{8} \times \frac{W}{8} \times L_{size}, \tag{4.1}$$

де H та W – відповідно, висота та ширина зображення у пік селях.

Таким чином, беручи до уваги вираз (4.1), можемо розрахувати приблизну кількість даних , що може бути вбудована у зображення довільного розміру.

Так, для зображення формату FullHD (1280x720) кількість R даних, які теоретично може бути вбудовано за даних умов, становить:

$$R = \frac{1280}{8} \times \frac{720}{8} \times 3 = 43200 \text{ біт, або 5,4 кБайт.}$$

Разом з тим, навіть для високо насичених зображень відсоток семантично складних сегментів є величиною не постійною, та може варіюватися у діапазоні від 80 до 20 відсотків від загальної маси [12, 14].

Отже, для випадку, коли 80% сегментів визнано семантично складними, зображення FullHD буде містити $R = 35040$ біт, або 4.38 кБайт.

У свою чергу, якщо семантично складними у зображенні є 20% сегментів, його ємність буде рівна $R = 8640$ біт, або 1,08 кБайт. Тобто, якщо мова йде про передавання невеликого повідомлення, (наприклад, передача секретного ключа), дана ємність є цілком прийнятною. У той же час, коли є потреба:

- передавання маскованих даних великого об'єму;
- ведення прихованого чату, або сеансу аудіозв'язку;
- віддаленої взаємодії з респондентом, системами або пристроями у резидентному режимі;

тоді на цей випадок має сенс використовувати у якості контейнера не окреме зображення, а потік відеокадрів, тобто, скористатися мультиконтейнерним режимом передавання.

Розглянемо приклад відео потоку, кодованого на базі технології, що відносяться до групи MPEG (рис.4.1) [15].

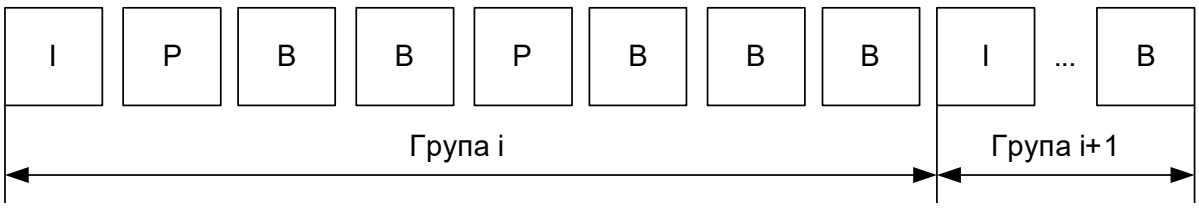


Рисунок 4.1 – Принцип, за яким виконується формування відео потоку на базі MPEG

На рис. 4.1 ділянка кадрів між двома I-кадрами, включаючи перший I-кадр у послідовності, має назву *групи кадрів.*

Таким чином до групи, окрім I-кадру, входить деяка кількість B-кадрів та щонайменше 2 P-кадри.

З усієї групи виключно I-кадр кодується повністю, тобто, його формування здійснюється на базі початкової кількості ξ сегментів $s_{x,y}$.

У свою чергу, B-кадри містять у своєму складі найменшу кількість сегментів $s_{x,y}$, оскільки їхнє головне призначення – передавання векторів руху відеосцени (тобто, зміщення об'єктів) відносно базового I-кадру. Зазвичай B-кадр містить у собі не більше, ніж 0,2ξ-0,05ξ сегментів, якщо вважати, що I-кадр побудовано за участю ξ сегментів.

При цьому, P-кадр відіграє перехідну роль між I та B кадрами – він може формуватися у середньому від 0,95ξ до 0,8ξ сегментами.

Рис. 4.1 демонструє структуру групи кадрів та відео потоку взагалі, характерну для MPEG-2.

У той же час, для технології H.264 характерним є можливість зміни кількості λ кадрів групи у діапазоні $\lambda = \overline{8;32}$.

У середньому можна вважати, що для даної технології величина λ є рівною 16, що пояснюється наступним:

- у випадку максимальної величини λ створюється надмірне навантаження на процесорну систему, у зв'язку з чим, окрім випадків високопродуктивних спецсистем даний режим не використовується;
- збільшення величини λ відносно базового значення $\lambda = 8$ забезпечує досягнення додаткового стиснення, тому більшість стандартних налаштувань кодеків H.264 передбачає значення розмірності групи кадрів значно вищою, ніж мінімальне значення.

Визначимо, кадри якого типу з групи, що формують відеопоток, можуть формувати мультиконтейнер.

З огляду на незначну кількість даних, що входять до кожного з кадрів B-типу, використовувати їх для побудови потокового контейнеру є недоцільним.

З іншого боку, недоцільно також використовувати у складі мультиконтейнеру I-кадри. Це викликано тим, що з потоку відеокадрів найлегше вилучати для подальшого аналізу кадри саме цього типу.

При цьому, вилучення з потоку кадрів інших типів є комплексним та нетривіальним завданням, що потребує з боку зловмисника значно більше зусиль.

Отже, оптимальним рішенням у даних умовах є використання Р-кадрів у якості базису для мультиконтейнера, оскільки Р-кадрам, з одного боку, відповідає достатня кількість сегментів $s_{x,y}$, а з іншого боку процес аналізу Р-кадрів є значно складнішим, ніж кадрів І-типу.

4.2 Режими функціонування методу

У базовому варіанті реалізації методу для інкапсуляції даних повідомлення, що підлягає маскуванню, застосовуються усі Р-кадри з потоку. Це так званий базовий режим (БР) [3].

Також, окрім базового режиму, передбачається наявність селективного режиму (СР), у ході якого здійснюється вибір певних Р-кадрів з потоку.

При цьому, у режимі БР з початком трансляції алгоритм визначає тип кадру керуючись налаштуваннями базового кодеку, та ведучи відлік кадрів, що йдуть на обробку.

У загальному випадку беруться до уваги величини λ розмірності групи, та частота f надходження кадрів, а також закономірність формування групи кадрів, у якості чого може зглядатися ще один параметр – частота надходження δ опорних кадрів.

Найчастіше спостерігається пропорціональний розподіл, за яким на 8 кадрів у групі 2 є кадрами Р-типу. Відповідно, індекс ω_P Р-кадрів у потоці визначається на базі наступної функціональної залежності:

$$\omega_P(\text{БР}) = \phi(\omega_I; \theta) = \phi'(\lambda; f; \delta; \theta) \qquad (4.2)$$

де ω_I - індекс І-кадру (початку групи) у потоці;

θ - множина закономірностей формування групи, що залежить від конкретної застосовуваної технології кодування за принципами MPEG.

У свою чергу, для СР особливості порядку вибору Р-кадрів з потоку для інкапсуляції біт приховуваного повідомлення визначаються за участю секретного ключа К, та на базі параметричної величини Θ, яка розраховується на базі статистичних характеристик кодованого першого І-кадру у потоці.

До таких характеристик можуть, зокрема, належати:

- кількість біт R_F, необхідних для опису кодованого кадру;

- найнижча амплітуда $\eta(Y)_{1,1}$ DC-компоненти у першому I-кадрі;

- обрана модель υ колірної субдискретизації для кодування першого I-кадру у потоці.

Це еквівалентно наступному виразу:

$$\omega_P(CP) = \varphi(K;\Theta) = \varphi'(K; R_F; \eta(Y)_{1,1}; \upsilon) \quad (4.3)$$

При цьому, одна параметрична величина Θ_1, що визначається як $\Theta_1 = \phi_{param}(R_F; \eta(Y)_{1,1}; \upsilon)$, використовується не довше, ніж до моменту використання для інкапсуляції деякої кількості n_P кадрів P-типу, обраної з її використанням.

Після цього розраховується нова параметрична величина на базі першого I-кадру, що надходить на обробку після проходження усіх n_P P-кадрів, які є заповненими контейнерами.

4.3 Розрахунок швидкості надходження приховуваних даних стегоканалом на базі методу, що використовує структурні особливості сегментів зображень

4.3.1 Базовий режим

Як зазначалося раніше, у загальному випадку кодування кадрів у потоці відео здійснюється у т.ч. на базі технології JPEG.

Зокрема, відносно відеокадрів застосовуються усі технологічні етапи JPEG-перетворення, серед яких одним з ключових є етап вибору колірної субдискретизації.

При цьому, мають місце варіювання режиму колірної субдискретизації від 4:4:4 до 4:1:1 (у стандартизованому наборі).

Головною відмінністю даних режимів між собою є різна кількість n_c компонент хроматичних та яскравісних.

Так, для режиму 4:4:4 загальна кількість $n_c(Y)$ компонент яскравості та колірно-різницевих - $n_c(Cr)$ та $n_c(Cb)$ є однаковою, тобто, $n_c(Y) = n_c(Cr) = n_c(Cb)$.

Власне, запис 4:4:4 означає, що на 4 компоненти Y приходиться по 4 хроматичних синіх та хроматичних червоних компонент. Відповідно, у режимі 4:2:1 на 4 компоненти Y приходиться 2 компоненти Cb та одна компонента Cr.

У свою чергу, у режимі 4:1:1 хроматичних компонент буде ще менша кількість.

У той же час, якщо не застосовується примусового налаштування параметру υ колірної субдискретизації для кодеку, за замовчуванням кодування відео буде здійснюватися у режимі 4:2:1. Тобто, опис кадру буде здійснюватися матрицею $H \times W$ компонент яскравості та матрицями $\frac{H}{1} \times \frac{W}{2}$ хроматичною синьою (Cb) та $\frac{H}{2} \times \frac{W}{2}$ хроматичною червоною (Cr).

При цьому, застосування єдиного принципу вибору множини компонент для модифікації у кожній з площин Y, Cb та Cr не може виконуватися, оскільки при цьому:

- квантування яскравісної та колірно-різницевих компонент виконується з використанням різних матриць квантування, відповідно, кореляції між існуючою множиною значимих компонент у СЧ та НЧ зонах нижче головної діагоналі площини Y та хроматичними не гарантується;
- навіть за наявності кореляції між значущими компонентами площин Y, Cb та Cr для НЧ та НЧ зон у режимах колірної субдискретизації, відмінних від 4:4:4, хроматичні площини будуть мати суттєво меншу кількість компонент, що можуть бути використані для модифікації, відповідно, цінність компонент Cb та Cr для розширення ємності стегосистеми є сумнівною та спричинює невиправдане обчислювальне навантаження на систему.

Таким чином, незалежно від робочого режиму функціонування стегосистеми, більш доцільним є використання компонент $\eta(Y)_{x,y}$ яскравісної (Y) площини для вбудовування даних повідомлення, що приховується.

З урахуванням цього, швидкість передавання $R(БР)_t$ біт приховуваного повідомлення у режимі БР може бути розраховано за формулою:

$$R(БР)_t = \frac{H}{8} \times \frac{W}{8} \times L_{size} \times n(t)_p \times \nu_{sd} \times \nu_s, \quad (4.4)$$

де $n(t)_p$ - кількість кадрів Р-типу, що буде надіслано за одиницю часу t;

ν_{sd} - коефіцієнт, який показує, яка частина сегментів у кадрі є семантично складними; раніше вказувалося, що $\nu_{sd} = \overline{0{,}2; 0{,}8}$;

ν_s - множник, що відображає, який саме розмір у кількості сегментів відносно І-кадру має поточний Р-кадр; $\nu_{sd} = \overline{0{,}8; 0{,}95}$.

Для того, щоб мати можливість обчислити величину $R(БР)_t$, попередньо необхідно розрахувати параметр $n(t)_p$.

Так, якщо кодер кожну секунду породжує f кадрів, а розмірність групи для цього випадку складає величину λ, тоді у ході проміжку часу, що дорівнює одній секунді, надсилатиметься $n(t)_\lambda$ цілих груп кадрів, о може бути продемонстровано формулою [13]:

$$n(t)_\lambda = \mathrm{div}(\frac{f}{\lambda}). \quad (4.5)$$

Стосовно нашого випадку необхідно також розрахувати обсяг кадрів $\bar{f}$, що входить до неповної групи. Це може бути виконано на базі виразу:

$$\bar{f} = \mathrm{mod}\frac{f}{\lambda}. \quad (4.6)$$

Раніше у середньому для технологій Н.264 (а також для MPEG4 Part 10) було прийнято $\lambda = 16$.

У свою чергу, для сімейства MPEG параметр частоти надходження кадрів може становити $f = 25$, або $f = 30$.

Відповідно, на базі виразів (4.5) та (4.6) розраховуються параметри $n(t)_\lambda$ та $\bar{f}$. Тоді для випадку $f = 30$ маємо $n(t)_\lambda = \mathrm{div}(\frac{30}{16}) = 1$ та $\bar{f} = \mathrm{mod}\frac{30}{16} = 14$. Тобто, кількість $n(t)_p$ кадрів Р-типу, що надсилаються за одиницю часу, буде розраховуватися з міркування, що, як зазначалося вище,

у відео потоці означених параметрів з 8 кадрів у групі 2 буде відноситися до Р-типу.

Таким чином, для $n(t)_\lambda = 1$ кількість Р-кадрів рівнятимеся 4.

У свою чергу, для $\bar{f} = 14$ обсяг Р-кадрів, враховуючи загальну архітектуру MPEG-потоку (після останнього Р-кадру надсилається не менше двох В-кадрів), кількість кадрів Р-типу також буде рівною 4. Отже, $n(t)_p = 8$ при $f = 30$.

Значить, для кадру HD-ready на базі виразу (4.4) для випадку, коли Р-кадр містить 80% сегментів порівняно з І-кадром, та семантично складними у ньому є 20% сегментів, $R(БР)_t = \frac{1280}{8} \times \frac{720}{8} \times 3 \times 8 \times 0{,}8 \times 0{,}2 = 55296$ біт, або 6,912 кБайт.

Разом з тим, при кількості сегментів для опису Р-кадру на рівні 95% від І-кадру, та за умови, що семантично складними серед них є 80%, маємо $R(БР)_t = \frac{1280}{8} \times \frac{720}{8} \times 3 \times 8 \times 0{,}95 \times 0{,}8 = 262656$ біт, або 32,832 кБайт.

Отже, за 1 секунду при частоті надходження 30 кадрів у секунду та роздільній здатності кадру 1280x720 приблизно може бути передано від 6, 912 до 32,832 кБайт.

Тепер розрахуємо, якою може бути швидкість передавання прихованих даних на випадок, коли $f = 25$. Тоді $n(t)_\lambda = \text{div}\frac{25}{16} = 1$, а $\bar{f} = \text{mod}\frac{25}{16} = 16$. Далі, за аналогією з випадком, коли $f = 30$, бачимо, що у секундний часовий проміжок входить 4 Р-кадри з цілої групи, та 2 – з групи, яка входить у зазначений часовий інтервал частково. Тобто, на цей випадок $n(t)_p = 6$.

Отже, для кадру за 1 секунду при частоті надходження $f = 25$ та роздільній здатності кадру 1280x720 (HdReady) за умови, що Р-кадри мають у своєму складі 80% сегментів порівняно з І-кадром, та семантично складними у їх складі у середньому є 20% сегментів, $R(БР)_t = \frac{1280}{8} \times \frac{720}{8} \times 3 \times 6 \times 0{,}2 \times 0{,}8 = 41472$ біти, або 5,184 кБайт.

У свою чергу, для кадрів того ж розміру, при незмінній частоті їх надходження, розміру Р-кадрів на рівні 0,95 від опорного І-кадру та 80% семантично складних сегментах у складі кожного з них отримуємо $R(БР)_t = \frac{1280}{8} \times \frac{720}{8} \times 3 \times 6 \times 0{,}8 \times 0{,}95 = 196992$ біти, тобто, 24,624 кБайт.

4.3.2 Селективний режим

На відмін від базового режиму, для СР-режиму передбачається використання лише деяких Р-кадрів у потоці, індекси $\omega_P(CP)$ яких визначаються на базі виразу (4.3).

Таким чином, у даному режимі може бути задіяно від $(n(t)_p - 1)$ кадрів Р-типу, до 1 кадру.

Отже, максимальна швидкість $R(CP)_t$ передавання біт приховуваного повідомлення у селективному режимі, коли здійснюється трансляція відео потоку роздільної здатності HdReady, кадри Р-типу займають 95% від І-кадру, при цьому, семантично складними з них є 80%, та може бути розрахована як:

$$R(CP)_t = \frac{H}{8} \times \frac{W}{8} \times L_{size} \times (n(t)_p - 1) \times \nu_{sd} \times \nu_s . \qquad (4.7)$$

Для цього випадку при $f = 25$

$R(CP)_t = \frac{1280}{8} \times \frac{720}{8} \times 2 \times 6 \times 0{,}8 \times 0{,}95 = 131328$ біт (16,416 кБайт).

Відповідно, для випадку $f = 30$, за тих же умов - $R(CP)_t = \frac{1280}{8} \times \frac{720}{8} \times 2 \times 8 \times 0{,}8 \times 0{,}95 = 175104$ байт (21,888 кБайт).

У свою чергу, далі за тими ж принципами розраховуються найнижчі показники швидкості стегокодеру, що відповідають $n(t)_p = 1$.

Для тієї ж роздільної знатності кадрів відео потоку, $f = 25$, за умов, що Р-кадри містять 80% від І-кадру, серед них семантично складними є 20%, отримуємо $R(CP)_t = \frac{1280}{8} \times \frac{720}{8} \times 1 \times 6 \times 0{,}8 \times 0{,}2 = 13824$ біт (1, 728 кБайт).

Тепер тих самих умов, як і у попередньому випадку, але для $f = 30$

$R(CP)_t = \frac{1280}{8} \times \frac{720}{8} \times 1 \times 8 \times 0{,}8 \times 0{,}2 = 18432$ біт (2,304 кБайт).

4.4. Оцінка потенційних можливостей методу маскування щодо організації прихованих каналів потокового мовлення

За умов функціонування методу у базовому режимі, як свідчать отримані результати розрахунків, теоретично може бути забезпечено можливість для створення прихованого каналу потокового мовлення [13, 17].

Так, для базового режиму було отримано найвищий показник у 32,832 кБайт, саме таку кількість прихованої інформації може передати сетгосистема на базі розглянутого методу за секунду.

Це відповідає 262,656 кбіт/с, тобто, отримана величина у чотири разиі перевищує стандартизований рівень бітової швидкості для Skype, що відповідає достатньому рівню якості аудіо каналу.

У свою чергу, найменша можлива бітова швидкість відповідає селективному режиму за найгірших умов, та дорівнює 13,824 кбіт/с. За таких умов можливість організації каналу аудіо мовлення зберігається, утім, рівень його якості у ньому випадку буде досить низьким.

Розглянемо ситуацію, якщо роздільну здатність потоку відеокадрів буде збільшено до FullHD (1920x1080).

Тоді для найкращих умов при використанні базового режиму отримуємо: $R(БР)_t = \frac{1920}{8} \times \frac{1080}{8} \times 3 \times 8 \times 0{,}95 \times 0{,}8 = 590976$ біт, що відповідає бітовій швидкості 590,976 кбіт/с.

Водночас, для найгіршого режиму: $R(БР)_t = \frac{1920}{8} \times \frac{1080}{8} \times 3 \times 8 \times 0{,}8 \times 0{,}2 = 124416$ біт, тобто, бітова швидкість забезпечуватиметься на рівні 124,416 кбіт/с.

Відповідно, для селективного режиму у найкращих умовах: $R(БР)_t = \frac{1920}{8} \times \frac{1080}{8} \times 2 \times 6 \times 0{,}95 \times 0{,}8 = 295488$ біт (295 кбіт/с), а для найгірших умов $R(БР)_t = \frac{1920}{8} \times \frac{1080}{8} \times 1 \times 6 \times 0{,}8 \times 0{,}2 = 31104$ біт (31кбіт/с).

Отже, якщо роздільну здатність контейнеру збільшити до формату FullHD, у селективному режимі стає можливим вести приховане аудіомовлення.

При цьому, для базового режиму за найкращих умов можливим є передавання прихованого відео потоку з частотою слідування кадрів рівною 25 та роздільною здатністю 640x480. Така можливість зумовлюється тим, що у випадку кодування відео потоку на базі H.264 його бітова швидкість приблизно буде рівною 420 кбіт/с. Відповідно, за найгірших умов можливе передавання відео з роздільною здатністю 320x240 (115-120 кбіт/с).

Проте, так як стабільний показник швидкості передавання біт прихованого повідомлення у принципі не гарантується, для підтримки каналу може додатково застосовуватися технологія на кшталт ABR, що застосовується сьогодні сервісами Google та функціонує на базі протоколу HTTPS [1].

4.5 Критичний аналіз методу маскування даних, який використовує структурні особливості сегментів зображень

У попередніх пунктах розділу виконувалася оцінка швидкості приховуваного повідомлення, що може бути розцінено як ємність стеганографічної системи. Зараз окремо виконаємо аналіз досліджуваного методу з позицій захищеності даних. Для цього розглянемо його з точки зору стегоаналізу.

Тут розглянемо можливість виявлення контейнеру за такими ознаками, як:

- дослідження змісту LSB-складової;
- аналіз структури трансформованого сегменту;
- статистичне оцінювання розподілу двійкових елементів розрядів молодших біт.

4.5.1 Дослідження змісту LSB-складової сегменту, що містить інкапсульовані біти прихованого повідомлення

На рисунку 4.2 наведено приклад відеокадрів для випадку вбудовування деякої кількості біт маскованого повідомлення, та незаповненого стегоконтейнеру.

Рисунок 4.2 – Оригінал зображення а), простори LSB пустого б) та заповненого контейнерів

Як видно з рис. 4.2, LSB-моделі тестового кадру для випадку пустого та заповненого контейнерів є ідентичними. Це виключає можливість виявлення факту прихованих даних для даного методу навіть у випадку, коли виконується інкапсуляція за LSB-сценарієм, оскільки зона модифікації є обмеженою та локалізується у межах ВЧ-СЧ компонент [8].

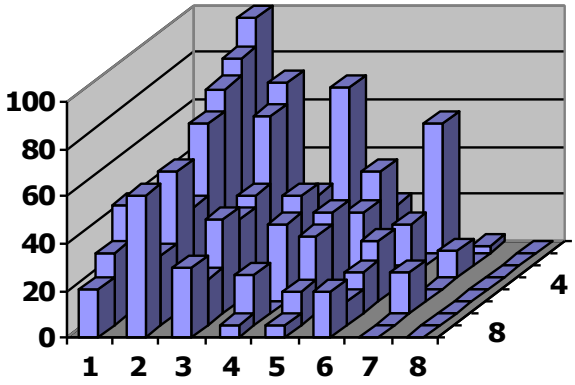
Разом з тим, локалізованість зони вбудовування даних суттєво звужує простір пошуку інкапсульованої інформації.

Тобто, як зловмисник яким-небудь чином заволодів даними про індекси діагоналей трансформованого сегменту, що беруть участь у перенесенні секретної інформації, теоретично він має можливість виявити факт її присутності, що автоматично вважається зламом стегосиситеми.

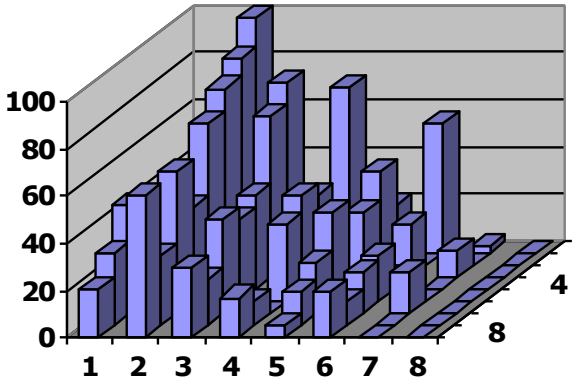
У зв’язку з цим виконаємо оцінку можливості виявлення заповненого контейнеру шляхом аналізу змісту областей СЧ-ВЧ компонент.

4.5.2 Аналіз структури трансформованого сегменту

Розглянемо один і той же трансформований сегмент насиченого зображення для випадків наявності та відсутності вбудовування біт секретного повідомлення, як показано рис. 4.3.



а)



б)

Рисунок 4.3 – Приклад трансформованого сегменту кадру з нормованими амплітудами компонент яскравості на випадок пустого контейнеру а) та випадок, коли контейнер містить у собі вбудований масив символів 0001 б)

На рисунку 3.4 компоненти, що належать головній діагоналі, локалізуються між координатами (8,1) - (1,8). Відповідно, 3 та 4 діагоналі, у межах яких було модифіковано 4 компоненти, лежать у координатах (8,4)-(4.8) та (8,5)-(5,8) відповідно.

З рисунку 4.3 бачимо, що закономірності у зміні амплітудт компонент 3 та 4 діагоналей нижче головної не простежуються. Відповідно, за таких умов структурний аналіз змісту трансформованих сегментів на віть за умов

достатньої обчислювальної потужності апаратно-програмних засобів зловмисника не дає змоги виявити факт існування контейнеру.

4.5.3 Статистичне оцінювання розподілу двійкових елементів розрядів молодших біт

З виразу (3.14), що описує процес вбудовування біт секретного повідомлення у компоненти трансформованого сегменту бачимо, що:

- вбудовування символу «0» передбачає збільшення амплітуди, нормованої відносно порогу округлення, на ¼ її значення;
- для інкапсуляції символу «1» величина компоненти зменшується на ¼ її нормованої величини.

При цьому, оскільки характер розподілу початкових величин компонент ВЧ-СЧ зон є випадковим та залежить лише від особливостей змістів сегменту, відповідно, модифікація значення компонент не веде до обов'язкового перерозподілу балансу двійкових символів як у межах розряду, так і у межах сегменту у цілому. Тобто, відносно методів статистичного аналізу для виявлення заповнених контейнерів розглянутий метод маскування також є ефективним.

ВИСНОВКИ

У ході виконання атестаційної роботи було виконано дослідження властивостей ряду класичних методів комп'ютерної стеганографії, та одного з сучасних методів, розробленого на базі класичних підходів, а саме – методу маскування даних на базі використання структурних особливостей сегментів зображень.

За результатами таких досліджень було виявлено, що:

1. Стандартизовані підходи до побудови методів стегозахисту даних не можуть гарантувати певного рівня стегостійкості у наслідок того, що:

- алгоритмічна реалізація стандартизованих методів, їх особливості застосування та характерні ознаки наявності заповнених контейнерів є відомими зловмиснику;
- щодо поширених алгоритмів маскування даних існує досить змістовна база підходів до їх викриття, реалізована на рівні певних інструментів стегоаналізу.

2. Поширені та найбільш продуктивні зі стандартизованих методів маскування даних фокусуються, головним чином, на використанні одних і тих же самих типів надмірності контейнеру.

Для випадку контейнерів графічного типу це майже завжди – психовізуальна надмірність, що дає змогу виконувати модифікацію компонент у хроматичній або яскравісній площинах.

3. Використання мультиконтейнерів, або контейнерів потокового типу, доцільне за умов стегосистем невисокого рівня ємності, коли є необхідність надсилання об'ємних маскованих повідомлень, або для створення стегоканалу, стабільного протягом деякого часового відрізку.

Разом з тим, підхід, що використовує модифікацію компонентного опису фрагментів кадру відео з урахуванням як психовізуальних, так і структурних особливостей їх побудови, потенційно здатен забезпечити високий рівень захищеності даних.

При цьому, поєднання зазначеного підходу з використанням мультиконтейнерів дозволяє додатково збільшити ємність стегосистеми та її рівень захищеності за рахунок того, що:

- модифікація значень компонент виконується для їх обмеженого

частотного діапазону, при цьому, застосовуються компоненти певного діапазону амплітуд, які, з одного боку, гарантують однозначну реконструкцію біт вбудованого повідомлення на боці прийому, а з іншого – не вносять візуально помітних спотворень у кадр; факт модифікації при цьому не виявляється ні відомими візуальними алгоритмами, ні алгоритмами, що відстежують статистичні особливості контейнерів;

- аналіз потокових контейнерів потребує значно вищих обчислювальних потужностей, ніж моно контейнери, та у більшості випадків може бути успішним лише за умови ціле направленого дослідження конкретного відео потоку, що є додатковим фактором захищеності;
- алгоритм передбачає використання хеш-функцій для визначення індексів компонент, які буде використано для інкапсуляції даних; такий алгоритм розраховує унікальну множину компонент залежно від секретного ключа та ряду характеристик сегменту, відносно якого ведеться розрахунок;
- алгоритм не використовує додаткових службових даних;
- передбачено можливість організації стегоканалу у базовому та селективному режимах, перший з яких може поступатися потенційною швидкістю передавання маскованих даних, проте забезпечує вищій рівень захисту за рахунок механізму вибору кадрів у відео потоці, які буде задіяно у якості контейнерів.

Виконано розрахунок швидкостей передавання секретного повідомлення для випадку відео потоку роздільної здатності HDReady. Проведений розрахунок свідчить, що потенційно можливий об’єм прихованих даних, який може бути надіслано за одиницю часу, окрів, власне, роздільної здатності відеопотоку залежить від:

- режиму функціонування методу маскування даних на базі урахування структурних особливостей та надмірності контейнеру;
- особливостей змісту P-кадрів, зокрема, відсотку семантично-складних сегментів, що його формують;
- фактичного розміру P-кадрів.

Так найбільша швидкість передавання біт прихованого повідомлення забезпечується на випадок застосування базового режиму роботи методу маскування.

Для роздільної здатності HDReady при частоті слідування кадрів 30 к/сек досягається максимально можлива швидкість передання прихованого повідомлення на рівні 32,832 кБайт за одиницю часу.

За тих же самих умов найменша швидкість передавання відповідає селективному режимові, яка дозволяє за одиницю часу надіслати у мережу 1,728 кБайт прихованого повідомлення.

Таким чином, усі вимоги технічного завдання виконано у повному об’ємі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Шелухин О.И., Канаев С.Д. Стеганография. Алгоритмы и программная реализация. Горячая линия – Телеком, научно-техническое издательство 2017, 592 с.
2. Стеганография в современных кибератаках | Securelist [Електронний ресурс] – Режим доступу: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090.
3. Fridrich Y. Steganography in Digital Media: Principles, Algorithms and Applicaticks. Cambridge Press, 2010. 462.
4. Шаньгин В.Ф. Информационная безопасность и защита информации. ДМК-Пресс., 2017, 702 с.
5. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: СОЛОН-Пресс, 2016, - 315 с.
6. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. - К.: МК-Пресс, 2006. - 288 с
7. Алексеев, А.П. Стеганографические и криптографические методы защиты информации : учеб. пособие по дисциплине "Информатика" / В.В. Орлов, А.П. Алексеев .— Самара : ИУНЛ ПГУТИ, 2010 .— 289 с.
8. Цифровая стеганография: Программы и другие способы реализации [Електронний ресурс] – Режим доступу: http://www.spy-soft.net/cifrovaya-steganografiya-sposoby-realizacii/
9. Р. Гонсалес, Р. Вудс. Цифровая обработка изображений — М: Техносфера, 2005 – 1007 с.
10. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : [монография] / А.Н. Фионов, Б.Я. Рябко. — М. : Горячая линия – Телеком, 2010 .— 233 с.
11. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии Защита информации. Конфидент. - СПб.: 2000, № 3.
12. Shi, Yun Q. Image and video compression for multimedia engineering: fundamentals, algorithms, and standards / Yun Q Shi, Huifang Sun.
13. Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355-372.

14. Юренский П.В. Методы статистического и нейросетевого стегоанализа скрытых каналов // Инновации в науке: научный журнал. – № 1(89). – Новосибирск., Изд. АНС «СибАК», 2019. – С. 11-13.
15. Ричардсон Ян. H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia / Ян Ричардсон. – Город. : Издательство, 2005. – 368 с.
16. Красильников Н.Н. Цифровая обработка изображений. – М.: Вузовская книга, 2011. – 320 с.
17. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Handbook of Applied Cryprography. CRC Press, 1996, 816 p.