Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод згладжування меж області нанесення цифрового водяного знаку на великому зображенні

(тема)

Виконав:

студент II курсу, групи СПм-20-2

Францевський І.В.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

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

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: проф. Торба А.А.
(посада, прізвище, ініціали)

Допускається до захисту

В. о. зав. кафедри ЕОМ _____ Волк М.О.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

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

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Францевському Іллі Владиславовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод згладжування меж області нанесення цифрового водяного знаку на великому зображенні

затверджена наказом по університету від "24" березня 2022 р. № 413 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 18 травня 2022 р.

3. Вхідні дані до роботи Тип обладнання – процесор Apple Silicon M1, велике зображення для згладжування меж області цифрового водяного знаку, мова програмування Python

4. Перелік питань, що потрібно опрацювати у роботі

1) аналіз проблеми та огляд існуючих рішень
2) вибір технології розробки та інструментальних засобів
3) розробка алгоритму
4) розробка програмного модулю
5) тестування програмного модулю
6) висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області	28.03.22-07.04.22	
2	Аналіз інформативних ознак, методів та	07.04.22-15.04.22	
	алгоритмів згладжування меж ЦВЗ		
3	Вибір технологій розробки та	15.04.22-22.04.22	
	інструментальних засобів		
4	Розробка алгоритму для реалізації завдання	22.04.22-29.04.22	
5	Розробка та тестування програмного модулю	29.04.22-11.05.22	
6	Оформлення матеріалів кваліфікаційної роботи	11.05.22-14.05.22	
7	Подання кваліфікаційної роботи на	14.05.22-15.05.22	
	рецензування		

Дата видачі завдання 28 березня 2022 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Торба А.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 65 с., 16 рис., 1 дод., 7 джерел.

ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, ЗГЛАДЖУВАННЯ, МЕТОД, НАНЕСЕННЯ, LSB, FSAA.

Метою кваліфікаційної роботи є розробка алгоритму згладжування меж області нанесення цифрового водяного знаку на наданих зображеннях, роблячи його більш стійким до атак.

У ході виконання кваліфікаційної роботи був проведений аналіз існуючих рішень, їх переваги, недоліки та сформовано вимогу до алгоритму.

Також під час якого аналізу виявилося, що забезпечення стійкості до атак видалення є більш менш вирішеним завданням, то забезпечення стійкості до геометричних атак і локальних змін зображення все ще мало вивчено, тому на вивчення останнього був зроблений фокус.

ABSTRACT

Master’s thesis: 65 pages, 16 figures, 1 appendix, 7 sources.

DIGITAL WATERMARK, ANTI-ALIASING, TECHNIQUE, USAGE, LSB, FSAA.

The major goal of this thesis is the development of an algorithm for anti-aliasing between areas of applying a digital watermark on these images, making it more resistant to attacks.

It order to developed described algorithm existing solutions were investigated, their advantages, disadvantages and formed the requirements of the needed algorigthm.

During the analysis, it turned out that the safety of stability before attacks from a distance is pretty resolved task, when the safety of stability before geometric attacks and local changes in the image is still not enough improved, so the focus is on the rest of the damage.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЦВЗ – цифровий водяний знак

ЗСЛ – зорова система людини

LSB – найменш значущий біт (англ., Least Significant Bit)

FSAA – повноекранне згладжування (англ., Full Scene Anti-Aliasing)

SSAA – згладжування суперсемплінгу (англ., Supersampling Anti-Aliasing)

MSAA – згладжування кількох зразків (англ., Multisample Anti-Aliasing)

OGSSAA – надмірна вибірка згладжування з впорядкованими ґратами (англ., Ordered Grid Supersample Anti-Aliasing)

FXAA – швидке наближене згладжування (англ., Fast Approximate Anti-Aliasing)

ISB – середньо важливий біт (англ., Intermediate Significant Bit)

MSB – найбільш важливий біт (англ., Most Significant Bit)

ВСТУП

Завдання захисту інтелектуальної власності на сьогодні не тільки не втрачає своєї актуальності, але стає ще більш затребуваною через безперервне зростання обсягів цифрової інформації та ширшого використання Інтернету. Поширення впровадження цифрових водяних знаків (ЦВЗ) у цифрові контейнери для захисту прав власності призводить до необхідності розробки методів, більш стійких до активних атак та природних спотворень у каналі обробки та передачі.

З розвитком методів застосування ЦВЗ атаки на стеганоконтейнери стають все більш вигадливими. Активні атаки та природні спотворення можуть призвести до двох видів модифікації контейнера-зображення: шумоподібні (зміна значень пікселів) та геометричні (просторова зміна розташування пікселів).

До спотворень першого виду, переважно, призводять атаки, створені задля видалення водяного знаку. Вони засновані на припущенні, що ЦВЗ є шумом, що статистично описується. До таких атак відносяться: шумова фільтрація контейнерів, перемодуляція, стиск із втратами (квантування), усереднення та колізії. Більшість існуючих систем ЦВЗ є стійкими до цих атак.

Геометричні атаки прагнуть змінити ЦВЗ шляхом внесення просторових чи тимчасових спотворень. Геометричні атаки легко здійсненні та призводять до неефективності багатьох систем ЦВЗ через втрату синхронізації водяного знаку у контейнері. Відновлення синхронізації потребує застосування спеціальних методів і є складним завданням [1].

Актуальною задачею є розробка метода згладжування меж області нанесення цифрового водяного знаку на зображеннях великого розширення, який зможе забезпечити більший рівень захисту та дозволить досягти кращого результату для роботи із зображеннями зазначеного розміру.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Цифровий водяний знак

Цифровий водяний знак (ЦВЗ) – це спеціальна мітка, що вбудовується у цифровий контент з метою аутентифікації та захисту авторських прав. Цифрові водяні знаки, стосовно зображень, як правило, невидимі, тобто оригінальне зображення і зображення, що містить ЦВЗ, візуально не відрізняються зорової системою людини (ЗСЛ).

Основні відмінності цифрових водяних знаків від звичайних (паперових) полягають у тому, що, по-перше, ЦВЗ невидимі (існує лише кілька випадків застосування видимих ЦВЗ), а по-друге, завдання зловмисника полягає не в найточнішій імітації водяного знаку, а, навпаки, у його знищенні.

Вимога невидимості необхідна, передусім, щоб зловмисник не зміг виявити ЦВЗ візуально (оскільки у разі його завдання спрощується).

Зазвичай ЦВЗ під час впровадження у графічні контейнери розподіляють у всьому зображенні. Це сприяє більшій стійкості ЦВЗ до деяких геометричних атак, наприклад, усічення. Проти інших атак типу афінних перетворень (масштабування, зміна пропорцій, поворот на деякий кут) такий підхід у базовій формі застосовувати практично марно.

Атаки такого роду не знищують сам ЦВЗ, однак, наводять зображення до такого виду, що детектор просто не може витягти водяний знак. Атаки, що видаляють ЦВЗ (фільтрація, перемодуляція, стиснення з втратами тощо), діють проти вбудованого повідомлення, тобто, спрямовані на знищення або псування ЦВЗ шляхом маніпулювання маркованим зображенням. У цьому методи застосування ЦВЗ, стійкі до незначної фільтрації, розробити порівняно не так складно. Більше істотна фільтрація, що видаляє ЦВЗ, викликає візуальні спотворення, помітні для ЗСЛ. Таким чином, є

актуальною задача виділення таких областей у зображенні, до модифікацій яких ЗСЛ сприйнятлива. І тут використання ЦВЗ у подібні області сильно зображення не змінить, оскільки ЦВЗ є повідомлення досить невеликого розміру. Тоді як фільтрація даних областей, необхідна видалення ЦВЗ, внесе істотні візуальні спотворення і, отже, сенс використання такого зображення для зловмисника буде втрачено.

Цифрові водяні знаки бувають трьох видів: робасні, або стійкі (маю на увазі, що такі ЦВЗ повинні бути стійкі до будь-яких впливів на них); крихкі (змінюються або руйнуються при незначній модифікації контейнера); напівтендітні (стійкі по відношенню до одних впливів і нестійкі по відношенню до інших). Стійкі ЦВЗ використовуються, коли автор хоче, щоб ідентифікаційний код, логотип компанії та ін. збереглися за максимальних спотворень контейнера. Крихкі ЦВЗ, поряд з електронним цифровим підписом, застосовуються для перевірки цілісності електронних документів. Алгоритми вбудовування крихких ЦВЗ відрізняються від інших особливою чутливістю до будь-яких спотворень та ефективні при вирішенні задачі контролю цілісності та захисту від фальсифікації. У разі напівкрихких ЦВЗ зображення, наприклад, може бути переведено в інший формат або стисло, але вирізати або вставити в нього фрагмент не можна; для аудіотреку можна змінити звук частот, але не можна прибрати голос виконавця [2].

1.2 Класифікація атак

ЦВЗ повинні задовольняти суперечливим вимогам візуальної (аудіо) непомітності та робастності до основних операцій обробки сигналів. Надалі без втрати спільності припускатимемо, що як контейнер використовується зображення.

Звернемося знову до системи вбудовування повідомлень шляхом модифікації молодшого біта (LSB) пікселів, розглянутої вище. Майже будь-який спосіб обробки зображень може призвести до руйнування значної

частини вбудованого повідомлення. Наприклад, розглянемо операцію обчислення ковзного середнього по двох сусідніх пікселів (a+b)/2, що є найпростішим прикладом низькочастотної фільтрації. Нехай значення пікселів a та b можуть бути парними або непарними з ймовірністю p=1/2. Тоді й значення молодшого біта зміниться після усереднення в половині випадків. До того ж ефект може призвести і зміна шкали квантування, скажімо, з 8 до 7 біт. Аналогічний вплив надає стиснення зображень із втратами. Більш того, застосування методів очищення сигналів від шумів, що використовують оцінювання та віднімання шуму, призведе до спотворення переважної більшості біт прихованого повідомлення.

Існують також і набагато згубніші для ЦВЗ операції обробки зображень, наприклад, масштабування, повороти, усічення, перестановка пікселів. Ситуація посилюється ще й тим, що перетворення стегоповідомлення можуть здійснюватися не лише порушником, а й законним користувачем, або є наслідком помилок під час передачі каналом зв'язку.

Розглянемо атаки, специфічні для систем ЦВЗ. Можна виділити такі категорії атак проти таких стегосистем.

1 Атаки проти вбудованого повідомлення - спрямовані на видалення або псування ЦВЗ шляхом маніпулювання стего. Методи атак, що входять до цієї категорії, не намагаються оцінити і виділити водяний знак. Прикладами таких атак можуть бути лінійна фільтрація, стиснення зображень, додавання шуму, вирівнювання гістограми, зміна контрастності тощо.

2 Атаки проти стегодетектора – спрямовані на те, щоб утруднити або унеможливити правильну роботу детектора. При цьому водяний знак у зображенні залишається, але втрачається можливість його прийому. До цієї категорії входять такі атаки, як афінні перетворення (тобто масштабування, зрушення, повороти), усічення зображення, перестановка пікселів тощо.

3 Атаки проти протоколу використання ЦВЗ – переважно пов'язані

зі створенням помилкових ЦВЗ, хибних стего, інверсією ЦВЗ, додаванням кількох ЦВЗ.

4 Атаки проти самого ЦВЗ – спрямовані на оцінювання та вилучення ЦВЗ із стегоповідомлення, наскільки можна без спотворення контейнера. У цю групу входять такі атаки, як змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації та інші.

Слід зазначити, що класифікація атак не є єдино можливою і повною. Крім того, деякі атаки (наприклад, видалення шуму) можуть бути віднесені до кількох категорій.

Відповідно до цієї класифікації всі атаки на системи вбудовування ЦВЗ можуть бути поділені на чотири групи:

- атаки, створені задля видалення ЦВЗ;
- геометричні атаки, спрямовані на спотворення контейнера;
- криптографічні атаки;
- атаки проти протоколу вбудовування і перевірки ЦВЗ.

1.2.1 Атаки, спрямовані на видалення ЦВЗ

До цієї групи відносяться такі атаки, як очищення сигналів-контейнерів від шумів, перемодуляція, стиск із втратами (квантування), усереднення та колізії. Ці атаки засновані на припущенні, що ЦВЗ є статистично описуваним шумом. Очищення від шуму полягає у фільтрації сигналу з використанням критеріїв максимальної правдоподібності або максимуму апостериорної ймовірності. Як фільтр, що реалізує критерій максимальної правдоподібності, може використовуватися медіанний (для ЦВЗ, що має розподіл Лапласа) або усереднений (для розподілу Гауса) фільтр, які застосовані в програмному пакеті StirMark. За критерієм максимуму апостеріорної ймовірності найкращим буде адаптивний фільтр Вінера (якщо як модель контейнера використовується нестаціонарний гаусовский процес),

а також порогові методи очищення від шуму (м'який і жорсткий пороги), які мають багато спільного з методами стиснення з втратами.

Стиснення з втратами та очищення сигналів від шумів значно зменшують пропускну здатність стегоканалу, особливо для гладких областей зображення, коефіцієнти перетворення яких можуть бути «обнулені» без помітного зниження якості відновленого зображення.

Перемодуляція – порівняно новий метод, який є специфічним для атак на ЦВЗ. В даний час відомі її різні варіанти, залежно від декодера, що використовується в стегосистемі. У побудові атаки є свої нюанси для стегосистеми М-їчної модуляції, стегосистеми, що використовує завадові коди, що використовує кореляційний декодер. У будь-якому випадку вважається, що ЦВЗ впроваджений у зображення із застосуванням широкосмугових сигналів та розмножений на всі зображення. Оскільки оцінюваний декодером ЦВЗ корелюється з істинним, з'являється можливість обману декодера. Атака будується в такий спосіб. Спочатку ЦВЗ «передбачається» шляхом віднімання фільтрованої версії зображення із захищеного зображення (застосовується медіанний фільтр). «Предказаний» ЦВЗ піддається ВЧ фільтрації, усікається, множиться на два і віднімається з вихідного зображення. Крім того, якщо відомо, що при впровадженні ЦВЗ множився на деяку маску для підвищення непомітності вбудовування, атакуючий оцінює цю маску і примножує на неї ЦВЗ. Як додатковий захід з «обману» декодера є ефективним вбудовування у високочастотні області зображення (де спотворення непомітні) шаблонів, що мають негаусівський розподіл. Таким чином, буде порушена оптимальність лінійного кореляційного детектора.

Така атака буде ефективною лише проти високочастотного ЦВЗ, тому реальні ЦВЗ будуються так, щоб їхній спектр відповідав спектру вихідного зображення. Річ у тім, що оцінка виходить лише високочастотних компонент ЦВЗ. Після її віднімання низькочастотна компонента ЦВЗ залишається незмінною і дає у детекторі позитивний кореляційний відгук.

Високочастотна складова дасть негативний відгук, що у сумі дасть нуль, і ЦВЗ нічого очікувати виявлено. Як інша протидія цій атаці було запропоновано виконання попередньої низькочастотної фільтрації.

1.2.2 Геометричні атаки

На відміну від атак, видалення геометричні атаки прагнуть не видалити ЦВЗ, але змінити його шляхом внесення просторових або тимчасових спотворень. Геометричні атаки математично моделюються як афінні перетворення з невідомим декодера параметром. Усього є шість афінних перетворень: масштабування, зміна пропорцій, повороти, зсув та усічення. Ці атаки призводять до втрати синхронізації в детекторі ЦВЗ і можуть бути локальними або глобальними (тобто застосованими до всього сигналу). У цьому можливе вирізування окремих пікселів чи рядків, перестановка їх місцями, застосування якихось перетворень тощо. Подібні атаки реалізовані у програмах Unsign (локальні атаки) та Stirmark (локальні та глобальні атаки).

Існують і більш «інтелектуальні» атаки на метод синхронізації ЦВЗ, що застосовується. Основна ідея цих атак полягає у розпізнаванні методу синхронізації та руйнування його шляхом згладжування піків в амплітудному спектрі ЦВЗ. Атаки ефективні в припущенні про те, що механізм синхронізації використовуються періодичні шаблони. При цьому для забезпечення синхронізації можуть використовуватися два підходи: вбудовування піків у спектральній області або періодичне впровадження послідовності ЦВЗ. В обох випадках у спектрі утворюються піки, які руйнуються в атаці, що розглядається. Після руйнування можна використовувати інші геометричні атаки: синхронізації вже немає.

Сучасні методи вбудовування ЦВЗ робасті до глобальних атак. Вони застосовуються спеціальні методи відновлення синхронізації, мають багато з застосовуваними у техніці зв'язку. Робастність досягається за рахунок

використання інваріантних до зсуву областей, застосування опорного ЦВЗ, обчислення автокореляційної функції ЦВЗ.

Якщо забезпечення робастності до глобальних геометричних атак є більш менш вирішене завдання, то забезпечення стійкості до локальних змін зображення є відкритим питанням. Ці атаки засновані на тому, що людське око мало чутливе до невеликих локальних змін картинки.

1.2.3 Криптографічні атаки

Криптографічні атаки названі так тому, що вони мають аналоги у криптографії. До них відносяться атаки з використанням оракула, а також злому за допомогою «грубої сили». Атака з використанням оракула дозволяє створити незахищене ЦВЗ зображення за наявності у порушника детектора. У деяких роботах досліджується стійкість ЦВЗ з урахуванням розширення спектра до атаки за наявності детектора як «чорного ящика». p align="justify"> Метод полягає в експериментальному вивченні поведінки детектора для з'ясування того, на які зображення він реагує, на які - ні. Наприклад, якщо детектор виносить «м'які» рішення, тобто показує можливість наявності стего в сигналі, то атакуючий може з'ясувати, як невеликі зміни в зображенні впливають на поведінку детектора. Модифікуючи зображення піксел за пікселом, може взагалі з'ясувати, який алгоритм використовує детектор. У разі детектора з «жорстким» рішенням атака здійснюється біля кордону, де детектор змінює своє рішення з «присутньою» на «відсутньою». Приклад атаки на детектор із жорстким рішенням:

1 на основі наявного зображення, що містить стегоповідомлення, створюється тестове зображення. Тестове зображення може бути створене різними шляхами, модифікуючи вихідне зображення до того часу, поки детектор покаже відсутності ЦВЗ. Наприклад, можна поступово зменшувати контрастність зображення, або піксел за пікселем замінювати дійсні значення

якимись іншими;

2 атакуючий збільшує або зменшує значення будь-якого пікселя, доки детектор не виявить ЦВЗ знову. Таким чином з'ясовується, збільшив або зменшив значення цього пікселу ЦВЗ;

3 крок 2 повторюється для кожного пікселя у зображенні;

4 знаючи, наскільки чутливим є детектор до модифікації кожного пікселя, атакуючий визначає пікселі, модифікація яких не призведе до суттєвого погіршення зображення, але порушить роботу детектора;

5 ці пікселі віднімаються від вихідного зображення.

Чи можлива побудова стегоалгоритму, стійкого проти подібної атаки, поки що невідомо.

Відомий різновид вищенаведеної атаки для ймовірнісного детектора. Також, як і раніше, атака починається з побудови тестового зображення на межі прийняття рішення детектором. Потім вибирається випадкова двійкова послідовність, та її елементи додаються до пікселів тестового зображення. Якщо детектор виносить рішення про наявність, ця послідовність вважається ЦВЗ. Інакше – ЦВЗ вважається протилежною до цієї послідовності. Далі виконується випадкова перестановка елементів у послідовності, і процес повторюється. Повторивши цю процедуру кілька разів і підсумувавши всі проміжні результати, отримаємо досить хорошу оцінку ЦВЗ.

1.2.4 Атаки проти використовуваного протоколу

Багато стегосистем ЦВЗ чутливі до так званої інверсної атаки. Ця атака полягає у наступному. Порушник заявляє, що в захищеному зображенні частина даних має його водяний знак. Після цього він створює помилковий оригінал, віднімаючи цю частину даних. У хибному оригіналі присутній справжній ЦВЗ. З іншого боку, в захищеному зображенні присутній проголошений порушником помилковий ЦВЗ. Настає нерозв'язна ситуація. Звичайно, якщо детектор має вихідне зображення, то власник може бути

виявлений.

У ряді випадків набагато простіше не видаляти ЦВЗ, а завадити його використанню за призначенням. Наприклад, можливе використання додаткових ЦВЗ отже стає незрозуміло, який їх ідентифікує справжнього власника контенту.

Іншою відомою атакою на протокол використання ЦВЗ є атака копіювання. Ця атака полягає в оцінюванні ЦВЗ у захищеному зображенні та впровадженні оціненого ЦВЗ в інші зображення. Метою може бути, наприклад, протидія системі імітозахисту або аутентифікації.

Одна із слабкостей стегосистеми, що застосовується для захисту від копіювання, є те, що детектор здатний виявити ЦВЗ, тільки коли відеосигнал візуально прийнятний. Однак можна піддати сигнал скремблювання, отримати шумоподібний сигнал, потім без перешкод незаконно скопіювати його. У відеоплеєр у цьому випадку вбудовується дескремблер, який відновлює незаконно зроблену копію. Апаратна реалізація скремблер і дескремблера дуже проста і іноді використовується для захисту, наприклад, програм кабельного телебачення. Можливим захистом проти такого підходу є дозволу копіювання лише певного формату даних.

1.3 Методи протидії атакам на системи ЦВЗ

У найпростіших стегосистемах ЦВЗ при вбудовуванні використовується псевдовипадкова послідовність, що є реалізацією білого шуму гауса і не враховує властивості контейнера. Такі системи практично нестійкі до більшості розглянутих вище атак. Для підвищення робастності стегосистем можна запропонувати низку поліпшень.

У робастной стегосистемі необхідний правильний вибір параметрів псевдовипадкової послідовності. Відомо, що при цьому системи з розширенням спектра можуть бути дуже робастними по відношенню до атак типу шуму додавання, стиснення і т.п. Так вважається, що ЦВЗ повинен

виявлятися за досить сильної низькочастотної фільтрації (7x7 фільтр із прямокутною характеристикою). Отже, база сигналу має бути великою, що знижує пропускну спроможність стегоканалу. Крім того, використовується як ключ ПСП повинна бути криптографічно безпечною.

Причиною нестійкості систем ЦВЗ з розширенням спектра до подібних атак пояснюється тим, що послідовність, що використовується для вкладення, зазвичай має нульове середнє. Після усереднення за досить велику кількість реалізацій ЦВЗ видаляється. Відомий спеціальний метод побудови водяного знака, спрямований проти такої атаки. При цьому коди розробляються таким чином, щоб за будь-якого усереднення завжди залишалася не рівна нулю частина послідовності (статична компонента). Понад те, у ній можливе відновлення решти послідовності (динамічна компонента). Недоліком запропонованих кодів є те, що їх довжина збільшується експоненційно зі зростанням кількості захищених копій, що розповсюджуються. Можливим виходом із цього положення є застосування ієрархічного кодування, тобто призначення кодів для групи користувачів. Деякі аналогії тут є із системами стільникового зв'язку з кодовим поділом користувачів (CDMA).

Різні методи протидії пропонувалися на вирішення проблеми прав власності. Перший спосіб полягає у побудові незворотного алгоритму ЦВЗ. ЦВЗ повинен бути адаптивним до сигналу та вбудовуватися за допомогою односпрямованої функції, наприклад, хеш-функції.

Другий спосіб вирішення проблеми прав власності полягає у вбудовуванні в ЦВЗ деякої тимчасової позначки, що надається третьою, довіреною стороною. У разі виникнення конфлікту особа, яка має на зображенні більш ранню відмітку, вважається справжнім власником.

Один із принципів побудови робастного ЦВЗ полягає в адаптації його спектра. У ряді робіт показано, що загальна спектра ідеального ЦВЗ повинна повторювати загальна спектра контейнера. Спектральна щільність потужності ЦВЗ, звичайно, набагато менше. При такій огинальній спектру

вінерівський фільтр дає найгіршу оцінку ЦВЗ з можливих: дисперсія значень помилки досягає дисперсії значень заповненого контейнера. Насправді адаптація спектра ЦВЗ можлива шляхом локального оцінювання спектра контейнера. З іншого боку, методи вбудовування ЦВЗ у сфері перетворення досягають цієї мети з допомогою адаптації у сфері трансформанти.

Для захисту від атак типу афінного перетворення можна використовувати додатковий (опорний) ЦВЗ. Цей ЦВЗ несе у собі інформації, але використовується для «реєстрації» виконуваних порушником перетворень. У детекторі ЦВЗ є схема попередження, що виконує зворотне перетворення. Тут є аналогія з тестовими послідовностями, що використовуються у зв'язку. Однак у цьому випадку атака може бути спрямована саме проти опорного ЦВЗ. Інший альтернативою є вкладення ЦВЗ у візуально значущі області зображення, які можуть бути видалені з нього без істотної деградації. Нарешті, можна розмістити стего в інваріантних до перетворення коефіцієнтів. Наприклад, амплітуда перетворення Фур'є інваріантна до зсуву зображення (при цьому змінюється лише фаза).

Іншим методом захисту від таких атак є блоковий детектор. Модифіковане зображення розбивається на блоки розміром 12x12 або 16x16 пікселів і для кожного блоку аналізуються всі можливі спотворення. Тобто пікселі в блоці зазнають поворотів, перестановок тощо. Для кожної зміни визначається коефіцієнт кореляції ЦВЗ. Перетворення, після якого коефіцієнт кореляції виявився максимальним, вважається реально виконаним порушником. Таким чином, з'являється можливість повернути внесені порушником спотворення [3].

1.4 Постановка проблеми

Проект являє собою програмний засіб, що містить в собі імплементацію метода згладжування меж областей нанесення цифрового

водяного знаку на великих зображеннях.

На основі аналізу алгоритму та виявлення значущих недоліків існуючих рішень, були сформовані вимоги до методу використаного у розробляємому застосунку.

Основна задача програми – згладжування меж області нанесення цифрового водяного знаку на наданих зображеннях, роблячи його більш стійким до атак.

2 АНАЛІЗ МЕТОДІВ ЗГЛАДЖУВАННЯ КОНТУРІВ ЗОБРАЖЕННЯ

На сьогоднішній день існує велика кількість методів згладжування, але вони ґрунтуються на одному принципі. Вони малюють кілька пікселів одного вихідного пікселя у фінальному зображенні.

Фактично способи розрізняються лише двома пунктами.

1 Пункт. Як вони визначають пікселі, які можуть бути накладені один на одного?

2 Пункт. Як вони змішують кілька відмальованих пікселів для отримання необхідного нам кінцевого пікселя.

Крім цього, дані алгоритми використовують різну кількість пікселів для отримання фінального пікселя. У відеоіграх дана кількість представлена досить просто за допомогою використання числа 2 будь-якої міри, тобто 2x, 4x, 8x і т.д.

Існує кілька термінів, які асоціюються зі згладжуванням, більшість із них виходить від стандартної формули згладжування.

Крім цього слід зазначити, що деякі методи згладжування можуть використовувати відеокарти як Nvidia, так і Radeon, інші - тільки Nvidia або тільки Radeon.

2.1 Традиційні методи

Результат точніший і чистіший, ніж методи постобробки.

Форсування даних методів не гарантує, що вони працюватимуть у іграх з відкладеним відмальовуванням. Дане обмеження можна обійти за допомогою зниженої дискретизації, але цей спосіб сильно впливатиме на продуктивність.

Дані методи здебільшого досить затратні за використовуваними ресурсами. Методи постобробки можуть використовуватися як альтернатива

для зниження впливу згладжування на продуктивність.

Традиційні методи не конфліктують із більшістю типів тимчасового згладжування.

2.1.1 Надмірна вибірка згладжування

Цей метод також відомий як повноекранне згладжування Full Scene Anti-Aliasing (FSAA) від AMD і часто замінюється терміном зниження масштабування.

Технічно при коректному використанні зниження масштабування різниця з SSAA/MSAA буде полягати в тому, що зниження масштабування застосовується як до 2D, так і до 3D об'єктів, тоді як SSAA/MSAA лише до 3D об'єктів. У деяких реалізаціях це може призвести до меншого зниження продуктивності та кращої сумісності.

Спотворення зображення з'являються тому, що на відміну від реальних об'єктів, які мають безперервні плавні криві та лінії, монітор відображає людині велику кількість маленьких квадратів. Всі ці пікселі мають однаковий розмір і кожен має свій колір. Лінія відображається тільки як набір пікселів і тому виглядає нерівною, якщо вона не знаходиться ідеально горизонтально або вертикально. Зразки кольору беруться з кількох вибірок усередині пікселя (а не лише в його центрі) і обчислюється середнє значення кольору. За допомогою відображення у вищій роздільній здатності, ніж відображуване, а потім стисненням до необхідного розміру з використанням додаткових пікселів для розрахунку отримує субдискретизоване зображення з більш плавними переходами від одного рядка пікселів до іншого по краях об'єктів.

Дані методи використовують загальну формулу згладжування до повноекранних зображень, зменшуючи ефект сходів. У порівнянні з відображеним зображенням, яке пройшло через MSAA, зображення SSAA/FSAA виглядатиме гладкішим. На 2D текст також можуть вплинути

більшість із реалізації зниження масштабування, у той час як SSAA/MSAA не повинні впливати на текст за їх правильної реалізації.

Реалізована на системах Nvidia Надмірна вибірка згладжування з впорядкованими ґратами – Ordered Grid Supersample Anti-Aliasing (OGSSAA). Може бути включена за допомогою використання Nvidia Profile Inspector у наступних режимах: 2x1, 1x2, 2x2, 3x3, 4x4.

В даний час даний метод був замінений менш ресурсомісткими методами через величезне навантаження на графічний процесор, але внаслідок отримання найкращого результату деякі ігри все ще використовують його як один з варіантів згладжування в налаштуваннях.

2.1.2 Множинна вибірка згладжування

MSAA за своєю суттю – це «бюджетна» версія SSAA.

Для зменшення навантаження, яке створюється SSAA/FSAA на системи, множинна вибірка оптимізує процес, оцінюючи кожен піксель лише один раз, при цьому справжня надлишкова вибірка відбувається тільки на краях обмальованого об'єкта і до значень глибини. Це призводить до аналогічного (але менш радикального) поліпшення якості зображення при одночасному зниженні навантаження на систему при малюванні та зниженні масштабування у високих роздільностях зображення.

Насамперед цей метод прибирає спотворення геометрії, тобто тимчасове спотворення та спотворення шейдерних ефектів, текстур та прозоростей не будуть порушені.

Цей метод також має як плюси, так і мінуси. Він вирішує проблеми із субпікселями, а також не спотворює основний об'єкт великою кількістю вибірок. Однак споживання пам'яті збільшується лінійно зі зростанням кількості вибірок, час малювання залежить від кількості вибірок, а також існують проблеми комплексної інтеграції під час роботи з відкладеним відображенням.

2.2 Методи постобробки

Дані методи використовують менше ресурсів проти традиційними методами.

Ці методи використовуються після відображення зображення, на відміну від традиційних методів. Це означає, що вони сумісні практично з кожною грою, відео чи навіть фотографіями.

При використанні даних методів зображення (зокрема текстури) іноді можуть ставати розмитими, так що загальна якість може стати навіть гіршою за оригінал, якщо метод реалізований неякісно. Розмиття певною мірою можна зменшити із застосуванням технологій підвищення різкості.
Дані методи повинні застосовуватися перед відображенням елементів інтерфейсу у грі для виключення впливу на них.

2.2.1 Швидке приблизне згладжування

Метод не потребує великих обчислювальних потужностей. Це досягається за рахунок згладжування нерівних країв (нерівностей) виходячи з того, як вони зображуються на екрані у вигляді пікселів, замість того, щоб аналізувати самі 3D - моделі, як при звичайному згладжуванні. Крім цього, метод досить швидкий, він виконується за 1,3 мілісекунди на 1 кадр.

Однак поліпшення якості зображення, яке досягається даним методом якості трохи гірше, ніж традиційні методи згладжування, такі як MSAA. Даний метод може бути застосований двічі з використанням двох окремих інструментів (наприклад, внутрішньоігрові налаштування і панеллю управління відеодрайвера і т. д.) або поверх SMAA або TAA для подальшого видалення нерівностей, але з великою ймовірністю даний метод погіршить розмиття нарівні зі збільшенням продуктивності .

FXAA приймає на вхід нелінійні дані RGB, які він перетворює на

скалярну оцінку яскравості для шейдерної логіки. FXAA перевіряє локальний контраст, щоб не обробляти краї зображення. Виявлені краї відмічені червоним, зі змішуванням у бік жовтого для представлення виявленого накладення субпікселів. Пікселі, які пройшли тест на локальний контраст, потім класифікуються як горизонтальні (золоті) або вертикальні (сині). При заданій орієнтації краю контрастна пара пікселів, яка розташована під кутом 90 градусів до вибраного краю (синє і зелене). Алгоритм шукає кінець ребра як і негативному, і у позитивному аспекті (червоне і синє), у бік довгого краю. Після цього відбувається перевірка на істотну зміну середньої яскравості пари висококонтрастних пікселів по краю зображення. Враховуючи кінці країв, положення пікселя на краях перетворюються на субпіксельний зсув на 90 градусів перпендикулярно краю для зменшення спотворення (червоний та синій для негативного та позитивного горизонтального зсуву та золотий та небесний для негативного та позитивного вертикального зсуву). Для вхідної текстури проводиться повторна вибірка з урахуванням даного субпіксельного зміщення. Зрештою додається низькочастотний фільтр залежно від кількості виявлених субпіксельних спотворень.

2.2.2 Морфологічне згладжування

Доступно на картах AMD на Windows і може бути примусово запущено для всіх ігор через панель керування драйвером відеокарти незалежно від графічного API, а також для ігор OpenGL під Linux з драйверами Mesa.

Даний метод більше впливає на продуктивність, ніж FXAA, хоча дозволяє отримати більш чітке зображення.

MLAA призначений для зменшення артефактів спотворення у зображенні без використання додаткових променів або спектрів.

2.2.3 Тимчасове приблизне згладжування

Метод призначений для відеокарт серії Nvidia GeForce GTX 600 та вище.

Техніка в стилі кіно призначена для зменшення тимчасового спотворення (повзання та мерехтіння, що спостерігаються в русі під час гри).

Метод поєднує грубу потужність MSAA зі складними фільтрами, аналогічними тим, які використовуються у фільмах з використанням комп'ютерної графіки для отримання гладкого зображення.

Тимчасове спотворення викликане тим, що частота дискретизації (число кадрів за секунду) сцени занадто мала порівняно зі швидкістю перетворення об'єктів усередині сцени. Через це об'єкти здаються стрибають або з'являються в якомусь місці замість того, щоб створювати враження плавного руху до них. Щоб уникнути артефактів спотворення частота дискретизації сцени повинна бути як мінімум вдвічі вищою, ніж у об'єкта, що швидко рухається. Поведінка затвора у випробувальній вибірці (зазвичай камери) сильно впливає на накладення, оскільки загальна форма експозиції з часом визначає систему з обмеженою смугою перед дискретизацією, що є важливим фактором при згладжуванні. Типовий приклад тимчасового згладжування в кіно – це поява коліс транспортного засобу, що рухаються назад, так званий ефект вагонних коліс [4].

3 АНАЛІЗ МЕТОДІВ НАНЕСЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

3.1 Модель стеганографічної системи

Стеганографія – це спосіб організації зв'язку, який приховує саме наявність зв'язку. На відміну від криптографії, де ворог точно може визначити, чи є повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в невинні послання так, щоб неможливо було запідозрити існування вбудованого таємного послання.

Слово «стеганографія» у перекладі з грецької буквально означає «тайнопис» (steganos - секрет, таємниця; graphy - запис). До неї відноситься безліч секретних засобів зв'язку, таких як невидимі чорнила, мікрофотознімки, умовне розташування знаків, таємні канали і засоби зв'язку на плаваючих частотах і т. д.

Стеганографія займає свою нішу у забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує можливість виявлення самого факту передачі повідомлення. А якщо це повідомлення ще й зашифроване, воно має ще один, додатковий, рівень захисту.

В даний час у зв'язку з бурхливим розвитком обчислювальної техніки та нових каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості представлення інформації в комп'ютерних файлах, обчислювальних мережах тощо. Це дає нам можливість говорити про становлення нового напряму – комп'ютерної стеганографії .

Незважаючи на те що стеганографія як спосіб приховування секретних даних відома вже протягом тисячоліть, комп'ютерна стеганографія - молодий напрямок, що розвивається.

Як і будь-який новий напрямок, комп'ютерна стеганографія, незважаючи на велику кількість відкритих публікацій та щорічні

конференції, тривалий час не мала жодної термінології.

Донедавна для опису моделі стеганографічної системи використовувалася запропонована 1983 Сіммонсом так звана "проблема ув'язнених". Вона полягає в тому, що два індивідууми (Аліса та Боб) хочуть обмінюватися секретними повідомленнями без втручання охоронця (Віллі), який контролює комунікаційний канал. При цьому є ряд припущень, які роблять цю проблему більш менш вирішуваною. Перше припущення полегшує вирішення проблеми і у тому, що учасники інформаційного обміну можуть розділяти секретне повідомлення (наприклад, використовуючи кодову клавішу) перед укладанням. Інше припущення, навпаки, ускладнює вирішення проблеми, оскільки охоронець має право не тільки читати повідомлення, а й модифікувати їх.

Пізніше, на конференції Information Hiding: First Information Workshop у 1996 році було запропоновано використовувати єдину термінологію та обговорено основні терміни.

Стеганографічна система або стегосистема - сукупність засобів та методів, що використовуються для формування прихованого каналу передачі інформації.

При побудові стегосистеми повинні враховуватися наступні положення:

- супротивник має повне уявлення про стеганографічну систему та деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному противнику, є ключ, за допомогою якого тільки його власник може встановити факт присутності та зміст прихованого повідомлення;

- якщо противник якимось чином дізнається про факт існування прихованого повідомлення, це не дозволить йому витягти подібні повідомлення в інших даних доти, доки ключ зберігається в таємниці;

- потенційний противник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні чи розкритті змісту таємних повідомлень.

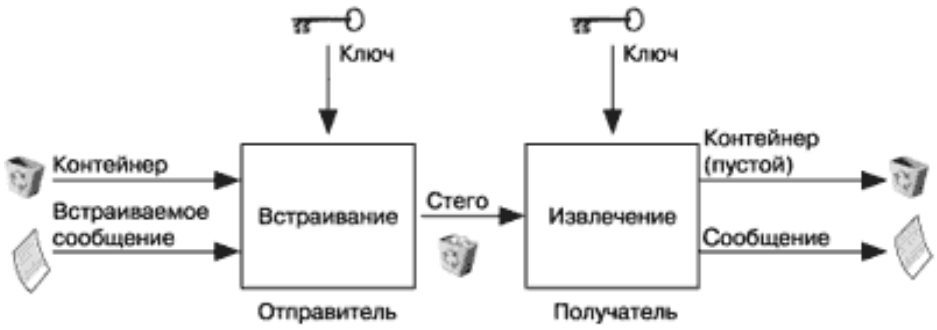

Рисунок 3.1 – Узагальнена модель стегосистеми

Як дані може використовуватися будь-яка інформація: текст, повідомлення, зображення тощо.

У загальному випадку доцільно використовувати слово «повідомлення», оскільки повідомленням може бути як текст або зображення, так і, наприклад, аудіодані. Далі для позначення прихованої інформації будемо використовувати саме термін повідомлення.

Контейнер – будь-яка інформація, призначена для приховування таємних повідомлень.

Порожній контейнер – контейнер без вбудованого повідомлення.

Заповнений контейнер або стего – контейнер, що містить вбудовану інформацію.

Вбудоване (приховане) повідомлення – повідомлення, що вбудовується у контейнер.

Стеганографічний канал або просто стегоканал – канал передачі стего.

Стегоключ або просто ключ - секретний ключ, необхідний приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) у стегосистемі може бути один або кілька стегоключів.

За аналогією з криптографією, за типом стегоключа стегосистеми можна підрозділити на два типи:

- із секретним ключем;
- із відкритим ключем.

У стегосистемі із секретним ключем використовується один ключ, який має бути визначений або до початку обміну секретними повідомленнями, або переданий захищеним каналом.

У стегосистемі з відкритим ключем для вбудовування та вилучення повідомлень використовуються різні ключі, які різняться таким чином, що за допомогою обчислень неможливо вивести один ключ з іншого. Тому один ключ (відкритий) може передаватися вільно незахищеним каналом зв'язку. Крім того, дана схема добре працює і при взаємній недовірі відправника та одержувача.

3.1.1 Вимоги

Будь-яка стегосистема повинна відповідати таким вимогам:

- властивості контейнера повинні бути модифіковані, щоб зміну неможливо було виявити під час візуального контролю. Ця вимога визначає якість приховування повідомлення, що впроваджується: для забезпечення безперешкодного проходження стегоповідомлення по каналу зв'язку воно жодним чином не повинно привернути увагу атакуючого;
- стегоповідомлення має бути стійким до спотворень, у тому числі й зловмисних. У процесі передачі зображення (звук або інший контейнер) може зазнавати різних трансформацій: зменшуватися або збільшуватися, перетворюватися на інший формат і т. д. Крім того, воно може бути стиснуте, в тому числі з використанням алгоритмів стиснення з втратою даних;
- для збереження цілісності повідомлення, що вбудовується, необхідно використання коду з виправленням помилки;
- для підвищення надійності вбудовуване повідомлення має бути дублювання.

В даний час можна виділити три тісно пов'язані між собою і мають одні

корені напрямки програми стеганографії: приховування даних (повідомлень), цифрові водяні знаки та заголовки.

Приховування даних, що впроваджуються, які в більшості випадків мають великий обсяг, пред'являє серйозні вимоги до контейнера: розмір контейнера в кілька разів повинен перевищувати розмір вбудованих даних.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії чи інші оцифровані витвори мистецтва. Основними вимогами, які пред'являються до таких вбудованих даних, є надійність та стійкість до спотворень.

Цифрові водяні знаки мають невеликий обсяг, однак, з урахуванням зазначених вище вимог, для їх вбудовування використовуються складніші методи, ніж для вбудовування повідомлень або заголовків.

Третій додаток, заголовки, використовується в основному для маркування зображень у великих електронних сховищах (бібліотеках) цифрових зображень, аудіо та відеофайлів.

У такому разі стеганографічні методи застосовуються не тільки для застосування ідентифікуючого заголовка, а й інших індивідуальних ознак файла.

Впроваджувані заголовки мають невеликий обсяг, а вимоги, що пред'являються до них, мінімальні: заголовки повинні вносити незначні спотворення і бути стійкими до основних геометричних перетворень.

Рисунок 3.2 – Додатки стеганографії

3.1.2 Обмеження

Кожний з перелічених вище додатків вимагає певного співвідношення між стійкістю вбудованого повідомлення до зовнішніх впливів (зокрема і стегоанализу) і розміром самого вбудованого повідомлення.

Для більшості сучасних методів, що використовуються для приховування повідомлення в цифрових контейнерах, має місце наступна залежність надійності системи від обсягу даних, що вбудовуються (рисунок 3.3).

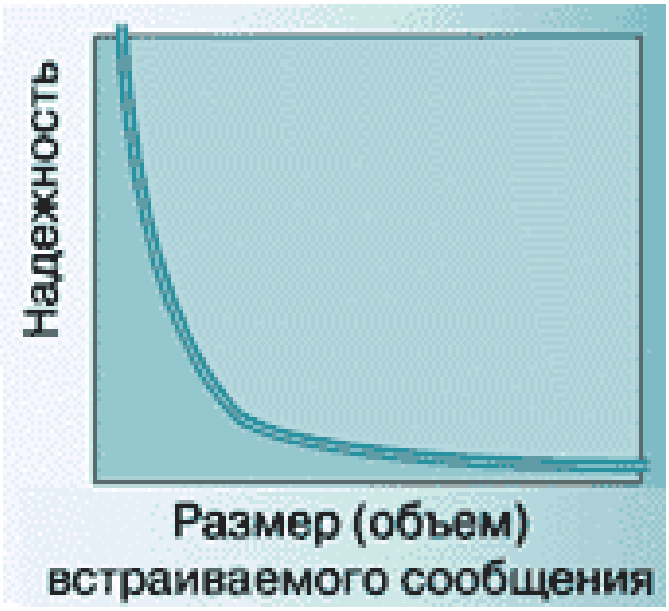

Рисунок 3.3 – Залежність надійності системи від обсягу даних, що вбудовуються

Ця залежність показує, що зі збільшенням обсягу вбудованих даних знижується надійність системи (при незмінності розміру контейнера). Таким чином, контейнер, що використовується в стегосистемі, накладає обмеження на розмір вбудовуваних даних.

3.1.3 Контейнери

Істотний вплив на надійність стегосистеми та можливість виявлення факту передачі прихованого повідомлення робить вибір контейнера.

Наприклад, досвідчене око цензора з художньою освітою легко виявить зміну колірної гами при введенні повідомлення в репродукцію "Мадонни" Рафаеля або "Чорного квадрата" Малевича.

По протяжності контейнери можна поділити на два типи: безперервні (струмові) та обмеженої (фіксованої) довжини. Особливістю потокового контейнера і те, що неможливо визначити його початок чи кінець. Більше того, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти, що призводить до необхідності включати біти, що приховують повідомлення, в потік в реальному масштабі часу, а самі приховують біти вибираються за допомогою спеціального генератора, що задає відстань між послідовними бітами в потоці.

У безперервному потоці даних найбільша вага для одержувача - визначити, коли починається приховане повідомлення. За наявності потокового контейнера сигналів синхронізації або меж пакета, приховане повідомлення починається відразу після одного з них. У свою чергу, для відправника можливі проблеми, якщо він не впевнений, що потік контейнера буде досить довгим для розміщення цілого таємного повідомлення.

При використанні контейнерів фіксованої довжини відправник заздалегідь знає розмір файлу і може вибрати біти в придатній псевдовипадковій послідовності. З іншого боку, контейнери фіксованої довжини, як це вже зазначалося вище, мають обмежений об'єм і іноді повідомлення, що вбудовується, може не помістится у файл-контейнер.

Інший недолік полягає в тому, що відстані між бітами, що приховують, рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, в той час як істинний випадковий шум буде мати експоненціальний розподіл довжин інтервалу. Звичайно, можна породити

псевдовипадкові експонентно розподілені числа, але цей шлях зазвичай занадто трудомісткий. Однак на практиці найчастіше використовуються саме контейнери фіксованої довжини як найбільш поширені і доступні.

Можливі наступні варіанти контейнерів.

1 Контейнер генерується самою стегосистемою. Прикладом може бути програма MandelSteg, у якій як контейнер для вбудовування повідомлення генерується фрактал Мандельброта. Такий підхід можна назвати конструюючою стеганографією.

2 Контейнер вибирається з деякої кількості контейнерів. У цьому випадку генерується велика кількість альтернативних контейнерів, щоб потім вибрати найбільш підходящий для приховування повідомлення. Такий підхід можна назвати селектуючою стеганографією. В даному випадку при виборі оптимального контейнера з множини згенерованих найважливішою вимогою є природність контейнера. Єдиною проблемою залишається те, що навіть оптимально організований контейнер дозволяє сховати незначну кількість даних при дуже великому обсязі самого контейнера.

3 Контейнер надходить ззовні. В даному випадку відсутня можливість вибору контейнера і для приховування повідомлення береться перший контейнер, який не завжди підходить до вбудовуваного повідомлення. Назвемо це безальтернативною стеганографією [5].

3.2 Методи нанесення ЦВЗ на зображення

Методи нанесення цифрових водяних знаків на зображення можна класифікувати на основі робочої області, видів документів, природи алгоритму, людського сприйняття та типу застосування, як показано на рисунку 3.4.

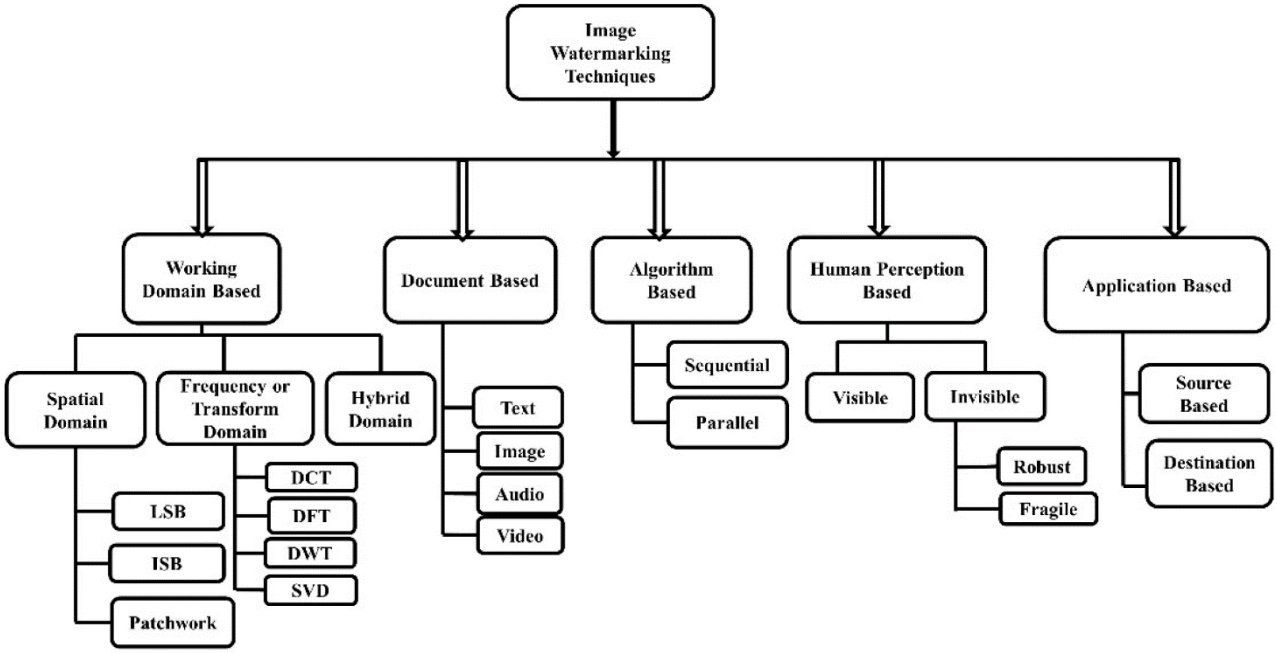

Рисунок 3.4 – Класифікація методів нанесення ЦВЗ на зображення

У даній роботі розглядається техніка нанесення водяних знаків у просторовій області.

Вказана техніка вставляє інформацію водяного знака в зображення хоста, як визначено власником у просторовій або часовій області, за допомогою різних методів, включаючи алгоритми модифікації найменших значущих бітів (LSB), проміжні значущі біти (ISB) або алгоритми клаптевого шиття, а також розширений спектр і кореляцію. -базовані алгоритми. Ці методи працюють безпосередньо на вихідних пікселях зображення. Водяний знак можна вставити шляхом маніпулювання значеннями пікселів на основі логотипу або інформації про підпис, наданої автором. У найбільш часто використовуваних дизайнах інтенсивності пікселів у відомих точках простору представляють зображення, де перевертається найнижчий біт певних пікселів у кольоровому або сірому зображенні. Залежно від інтенсивності пікселя отриманий водяний знак може бути видимим або невидимим. У даному розділі розглядаються різні підходи щодо технік просторової області, які привернули увагу дослідників завдяки

оптимальному балансу між непомітністю, надійністю та ємністю, які є найважливішими вимогами будь-якої техніки водяних знаків. Ці методи мають низьку складність, підвищену ефективність і швидше виконання. Крім того, якість зображення водяного знака можна контролювати. Однак ці методи працюють добре, лише якщо зображення не піддається жодному шуму чи модифікації людиною. Обрізання зображень можна використовувати для виключення водяного знака, який є основною слабкістю водяних знаків просторової області. Ці методи вбудовують великий обсяг даних з точки зору місткості, але вставлені дані можуть бути легко виявлені різними атаками. Крім того, невеликий предмет можна вставити кілька разів. Таким чином, єдиний збережений водяний знак буде вважатися досягненням, незважаючи на втрату більшої частини зображення через кілька атак.

3.2.1 Найменший значущий біт (LSB)

Модифікація найменшого розряду є найбільш часто використовуваним алгоритмом для водяного знака просторової області. Тут найменший значущий біт (LSB) випадково вибраних пікселів може бути змінений, щоб приховати старший біт (MSB) іншого. Він генерує випадковий сигнал за допомогою певного ключа. Водяний знак вставляється в найменші значущі біти основного зображення і може бути вилучений таким же чином. Декілька методів можуть обробляти зображення хоста. Цей тип алгоритму простий і простий у реалізації. Найменші значущі біти несуть менш відповідну інформацію, і, таким чином, якість зображення хоста не впливає. Він забезпечує високу прозорість сприйняття з незначним впливом на зображення хоста. Однак на цей алгоритм можуть вплинути небажані шуми, обрізання, стиснення з втратами тощо, і він може бути атакований хакером, встановивши всі біти LSB в «1», легко змінюючи вбудований водяний знак без будь-яких труднощів. Техніку LSB можна легко зрозуміти на прикладі, зображеному на малюнку 8. Припустимо, що два значення пікселя в

зображенні хоста становлять 130 (10 000 010) і 150 (10 010 110). Тоді, використовуючи техніку LSB, якщо вбудований водяний знак дорівнює 10, то значення пікселя водяного знака будуть 131 (10 000 011) і 150 (10 010 110) відповідно.

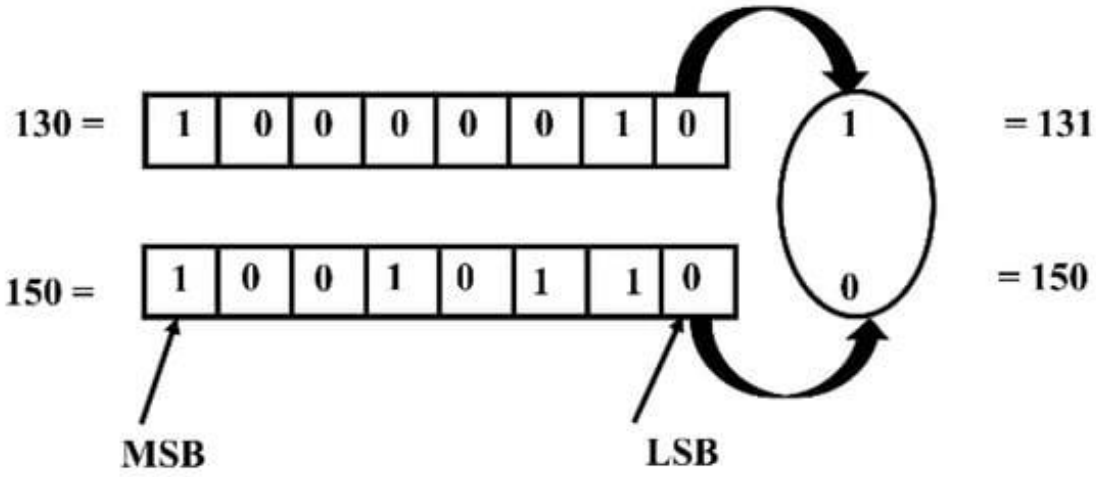

Рисунок 3.5 – Приклад методу найменшого значного розряду (LSB)

Декілька дослідників вивчали модифікації техніки LSB, які зазвичай пов’язані з просторовою областю. Методи LSB були розроблені на основі бітової площини цифрових дискретних сигналів (наприклад, аудіо або зображення). Бітова площина, яка представляє сигнал, — це набір бітів, що мають однакову позицію біта в кожному з двійкових чисел. Більшість методів використовує лише одну бітову площину для вбудовування. Ця техніка працює з найменшим бітовим бітом (тобто восьмими бітовими площинами), але інші використовують три бітові площини (тобто шоста-восьма бітові площини) або навіть чотири бітові площини (тобто п'ята-восьма біт-площини) для вбудовування з прийнятною якістю зображення. Чотири найменші значущі біти (тобто п’ятий–восьмий біти зображення обкладинки) можна замінити вибраним бітом секретного зображення, просто використовуючи операцію АБО певним чином. Цей метод спочатку перетворює зображення хоста в потік двійкових бітів, виводить нуль у

вбудованому біті, а потім зміщує секретне зображення вправо на 4 біти. Потім над цими хостом і секретним зображення виконується операція АБО, щоб отримати об’єднане зображення. Ця операція проілюстрована на рисунку 3.6.

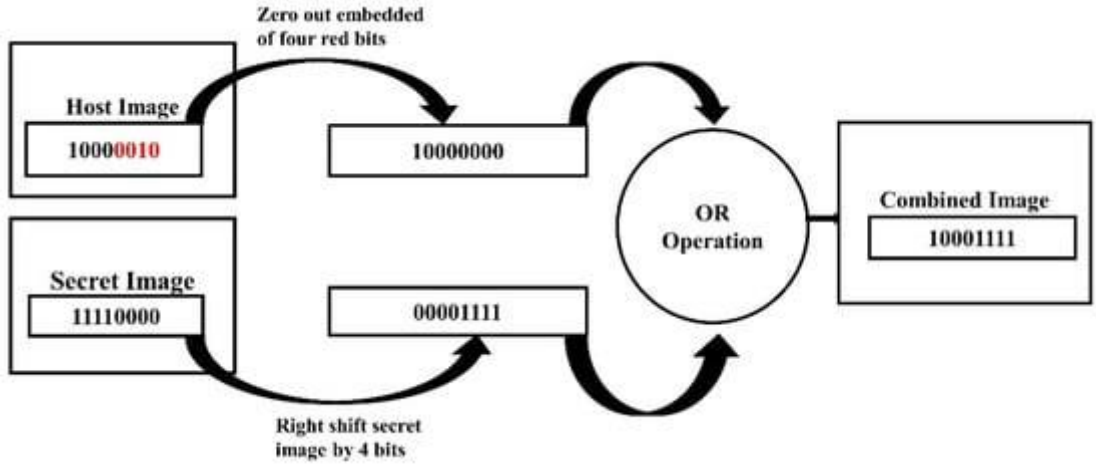

Рисунок 3.6 – Структурна схема методу LSB (чотири бітові площини)

Наведений вище малюнок найкраще охарактеризує приклад. Нехай значення пікселя зображення обкладинки (або зображення хоста) становить 130 (10 000 010), а двійкове представлення секретного зображення — 11 110 000. Після вбудовування нуля значення зображення обкладинки становить 128 (10 000 000). Після зсуву вправо на чотири біти значення секретного зображення становить 15 (00,001,111). Потім виконується операція виключне АБО, щоб отримати комбінований піксель зображення, який має десяткове значення 143 (10 001 111). Тому цей метод показує найгірший сценарій, коли зображення хоста і секретне зображення здаються однаковими. Іншими словами, різниця між основним і секретним зображенням становить (2k-1), де k — кількість різних бітових площин. Для отримання випадкових сигналів алгоритм LSB може використовувати певний ключ (разом із генератором m-послідовності). Таким чином, використовуючи метод Хаффмана, двовимірний сигнал водяного знака може бути вставлений у хост-зображення

з відповідним значенням пікселя. Метод Фунга та Годоя змінює пікселі зображення хоста — в середньому лише половину бітів (найменш 1–4 біти) — на кількість бітів вбудованого секретного повідомлення.

Зоровий апарат людини не може розпізнати це через незначні зміни інтенсивності кольорів. Тим не менш, підпорядкований зловмисник може легко виявити змінені біти завдяки прості операції. Манджула і Данті запропонували метод вставки 2-3-3 LSB, який використовує секретні дані, що містять вісім бітів. Ці дані вставляються в LSB в порядку 2-3-3, таким чином, що два (02) біти вставляються в канал R, три (03) біти вставляються в канал G, а решта три (03) біти вставляються в канал B. Цей метод покращує значення MSE та PSNR порівняно з методом 3-3-2 на основі хешування. У методі на основі блоків зображення обкладинки може бути оброблено шляхом розбиття його на блоки за допомогою певних методів, таким чином, що секретне зображення ніколи не може бути вилучено. Потім вбудований водяний знак кодується шляхом зміни відносин між сусідніми блоками.

Звичайна техніка водяного знака просторової області має найвищу ймовірність створення ефекту солі та перцю. Таким чином, Abraham and Paul запропонували метод для нанесення водяних знаків на кольорове зображення в просторовій області без істотного погіршення якості зображення та зміни кольору сприйняття порівняно зі звичайним водяним знаком просторового домену. Щоб зробити автентифікацію та/або відновлення можливими, водяний знак вбудований у всі блоки зображень, щоб забезпечити вищу якість зображення та високу стійкість до атак. M1 і M2 гарантують, що вбудовані біти менше руйнують зорову систему людини, де M1 — це маска вбудовування, а M2 — маска компенсації. Змінені пікселі не помітні, порівняно з сусідніми пікселями. Експериментальні результати показали, що запропонований ними алгоритм відновлював дані водяного знака навіть після того, як найменші значущі біти були спотворені, і що алгоритм забезпечував хороше значення PSNR. Хоча техніку LSB можна легко змінити, зрозуміти, як буде змінено цифрове зображення, щодо цілісності та безпеки, є складним

завданням. Алгоритм хешування LSB аутентифікує цифрове зображення за допомогою схеми хешування, яка приховує хеш-функцію. В одному дослідженні використовувався вбудований хеш-код LSB для захисту оригінального файлу та вилучення вбудованого хеш-коду, щоб створити вихідний файл, який здавалося б таким же, як і вихідний файл. У цьому випадку вбудований водяний знак, який використовується для вилучення даних, невидимий. Проте методи LSB можуть бути легко реалізовані, і, таким чином, пов’язана з цим складність обчислень може бути зменшена.

3.2.2 Проміжний значущий біт (ISB)

Методи LSB є найпоширенішими та простими передовими методами водяних знаків у просторовій області, але вони не забезпечують надійність проти атак. З цієї причини альтернативні методи, такі як методи проміжних значущих розрядів (ISB), були розроблені для підвищення надійності та збереження якості системи водяних знаків. У кількох дослідженнях розроблено методи ISB з використанням різних алгоритмів. Один із цих методів замінює класичну техніку LSB на ISB шляхом знаходження найкращого значення пікселя між серединою і краєм діапазону. У цьому методі зображення водяного знака захищається від різних атак, а зміна зображення водяного знака зводиться до мінімуму. Інше дослідження зосередилося на моделі подвійного проміжного значущого біта (DISB), в якій два біти вбудовуються в кожен піксель основного зображення, а решта шість (06) бітів змінюються, щоб налаштувати вихідний піксель. Зображення водяного знака можна вибрати, вибравши найближче значення пікселя до оригіналу, якщо існує різниця між оригіналом і вбудованим. Запропонована модель створює зображення водяного знака більш високої якості, ніж метод LSB. Таким чином, метод DISB забезпечує високу стійкість до атак і покращує якість зображень із водяними знаками. Надійність і якість є двома найважливішими вимогами до будь-якої системи водяних знаків, які можна

проаналізувати за допомогою справедливих нормалізованих значень взаємної кореляції (NCC).

Для нанесення водяних знаків зображення в просторовій області використовувалися методи ISB. Ця техніка замінює оригінальні пікселі зображення пікселями водяного знака, зберігаючи пікселі водяного знака близько до заповненої або порожньої області в пікселях вихідного зображення. Значення пікселя водяного знака перевіряється відповідно до діапазону кожної бітової площини, а потім вихідний піксель файлу зображення розміщується за межами будь-якого з країв діапазону. У зображеннях у відтінках сірого є вісім (08) бітових площин, де перша бітова площина містить MSB, а восьма містить LSB, а решта (друга–сьома) бітові площини використовуються як ISB. Якщо значення пікселя зображення у відтінках сірого дорівнює 133 (10 000 101), то проміжні значущі біти представлені на рисунку 3.7.

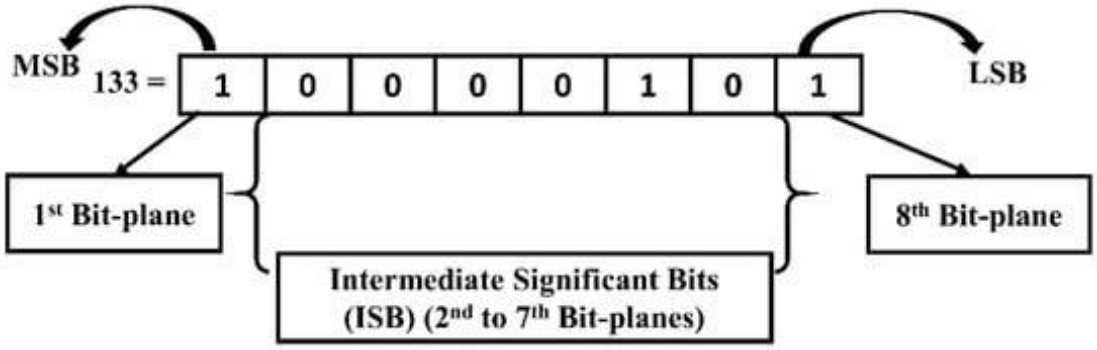

Рисунок 3.7 – Розрядна площина цифрового зображення

PSNR і NCC є найбільш часто використовуваними показниками якості для зображень із водяними знаками, де PSNR визначає інтенсивність і слабкість методів водяних знаків, тоді як останній підтверджує силу використаного алгоритму, застосованого до зображення з водяним знаком після атак. Розглядаючи це питання, у роботі виявлено сильні та слабкі сторони техніки водяних знаків цифрового зображення, визначивши порогові

значення PSNR та NCC. Обговорювана техніка водяних знаків вбудовувала чотири водяні знаки в ISB з шести файлів зображень у відтінках сірого один за одним шляхом заміни вихідних пікселів зображення новими пікселями та одночасного збереження їх близько до вихідних значень пікселів. Запропонований ними алгоритм продемонстрував кращу стійкість до деяких поширених операцій обробки зображень, таких як фільтрація, стиснення, шум і розмиття, на основі значень PSNR і NCC. Надійність не зменшується проти атак геометричних перетворень, таких як масштабування та поворот, при яких на інтенсивність пікселів не впливає їхнє змінене розташування. Таким чином, щоб підвищити надійність повідомлень проти різних атак і протистояти геометричним перетворенням (наприклад, масштабування, обрізання та фільтрації), можна використовувати методи ISB замість методів LSB, коли секретне повідомлення може бути вбудовано в бітову площину. (або розрядні площини).

3.2.3 Мозаїчний алгоритм

Мозаїчний алгоритм (patchwork) — це псевдовипадковий статистичний процес, який невидимо вбудовується в оригінальне зображення за допомогою надлишкового кодування шаблону за допомогою розподілу Гаусса. Два патчі A і B вибираються псевдовипадковим чином, і дані зображення першого патча (A) бліднуть, а ті, що в B, затемнені. Методи печворку демонструють кращу стійкість проти максимальних негеометричних модифікацій зображення, а процес не залежить від вмісту вихідного зображення. У цьому випадку надійність може бути підвищена за рахунок більш афінного кодування, розпізнавання функцій або обох, а код може бути втрачений шляхом масштабування, трансляції або обертання перед декодуванням. Хоча печворк неупереджено стійкий до обрізання, він погіршує його точність. Псевдовипадковий бітовий потік генерується шляхом вибору пар пікселів із вихідного зображення. Біт інформації кодується в пару, де d означає різницю

між двома пікселями; кодування дорівнює 0 для d < 0, а пікселі міняються місцями для d > 0. Наступна пара може бути просунута, якщо d дорівнює 0 або більше, ніж попередньо визначений поріг. Отже, яскравість може бути збільшена на одну одиницю в одній точці і зменшена, відповідно, в іншій точці. Цей метод підходить для великих ділянок випадкової текстури, але не для текстових зображень. Ділянка випадкового текстурного візерунка на зображенні копіюється в область зображення з подібною текстурою. Кожна область текстури відновлюється за допомогою автокореляції. У дослідженні було запропоновано узагальнений алгоритм печворку, що складається з адитивного та мультиплікативного печворку. Цей метод використовує статистичні дані для вбудовування та виявлення водяного знака. Для виявлення даних водяного знака цей метод використовує схему зсуву розташування та схему зсуву масштабу. Було показано, що запропонований ними метод стійкий до атак стиснення. Проте стійкість до різних атак дуже висока у методі печворку; невелика кількість даних може бути прихована. Водяний знак можна вставити за допомогою надлишкового кодування шаблону в зображення, а водяний знак можна витягти за допомогою секретного ключа, що стосується алгоритму декодування [6].

4 РОЗРОБКА МЕТОДУ ЗГЛАДЖУВАННЯ КОНТУРІВ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ПРИ ВБУДОВІ У ЗОБРАЖЕННЯ

4.1 Теорія

Фільтр анізотропної дифузії Перона і Маліка – це фільтр, що згладжує цифрові зображення, ключова особливість якого полягає в тому, що при згладжуванні він зберігає і «підсилює» межі областей на зображенні.

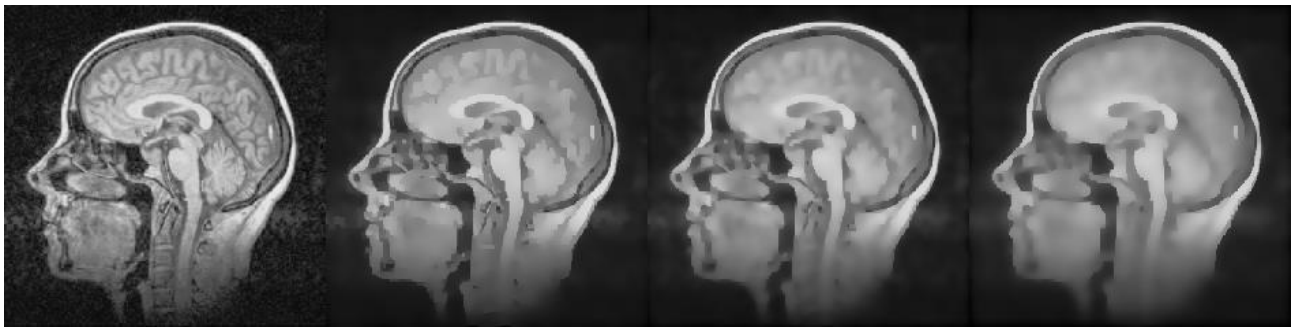

Рисунок 4.1 – Крайнє ліве зображення – оригінальне, праворуч від оригінального – фільтровані з різними параметрами

У фільтрі анізотропної дифузії згладжене зображення є деяким членом сімейства зображень, отриманих рішенням наступного рівняння математичної фізики:

$$I_t(x, y, t) = div(c(x, y, t)\nabla I(x, y, t)), \quad (4.1)$$

З початковою умовою:

$$I(x, y, 0) = I_0(x, y), \quad (4.2)$$

де $I(x, y, t)$ – однопараметричне сімейство зображень; чим більше t,

тим більше ступінь розмиття вихідного зображення;

$I_o(x, y)$ – початкове зображення;

I_t – похідна за t;

div – оператор дивіргенції;

∇ – градієнт.

З погляду теорії, зображення – це деяка безперервна функція двох змінних, а сама картинка (матриця пікселів) – дискретизація цієї функції. Причому 0 відповідає нульовій яскравості точки зображення, тобто чорний колір.

За своєю суттю фільтр анізотропної дифузії є модифікацією фільтра Гаусса.

Якщо підставити замість функції $c(x, y, t)$ одиницю, тобто $(x, y, t) \equiv 1$, то виходить рівняння ізотропної дифузії:

$$I_t(x, y, t) = div\big(\nabla I(x, y, t)\big) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2}, \tag{4.3}$$

Математики Коендерінк і Гумел показали, що таке сімейство розмитих зображень за параметром t, можна еквівалентно отримати як рішення рівняння згортки функції зображення з ядром Гауса (це і є фільтр Гауса):

$$I(x, y, t) = I_0(x, y) * G(x, y; t), \tag{4.4}$$

де $*$ – оператор звертки;

$G(x, y; t) = \frac{1}{2\pi t^2} e^{-\frac{x^2+y^2}{2t^2}}$ – функція ядра Гауса з нульовим математичним очікуванням і t середньоквадратичним відхиленням.

Функція $(x, y; t)$ грає роль деякого «регулювальника» згладжування.

Виходячи з рівняння фільтра (формула 4.1), для збереження початкового значення в точці зображення потрібно, щоб похідна за часом дорівнювала нулю (тобто значення будь-яких шарах розмиття було

константою). Отримано такі умови на функцію c:

$c(x, y, t) = 0$ – на кордонах;

$c(x, y, t) = 1$ – всередині областей, інакше кажучи, всередині областей має відбуватися звичайне гаусове розмиття.

Перона та Малік використовували градієнт функції зображення ∇I як просту для розрахунку та досить точну апроксимацію меж областей. Чим більша норма градієнта, тим чіткіша межа. Виходячи з цього отримуємо:

$$c(x, y, t) = g(||\nabla I(x, y, t)||), \tag{4.5}$$

де $g(.)$ – деяка функція із областю значень на відрізку [0;1].

Через нечітке визначення меж через норму градієнта, вимагають також, щоб функція g була монотонною спадною.

Перона та Малік запропонували два варіанти функції g:

$$g(x) = e^{-(\frac{x}{k})^2}, \tag{4.6}$$

$$g(x) = \frac{1}{1+(\frac{x}{k})^2}, \tag{4.7}$$

де k – параметр, який визначається або дослідним шляхом, або деяким «вимірювачем» зашумленості.

Для того, щоб детальніше розглянути другу функцію (формула 4.7) необхідно побудувати графіки функції g для кількох різних k.

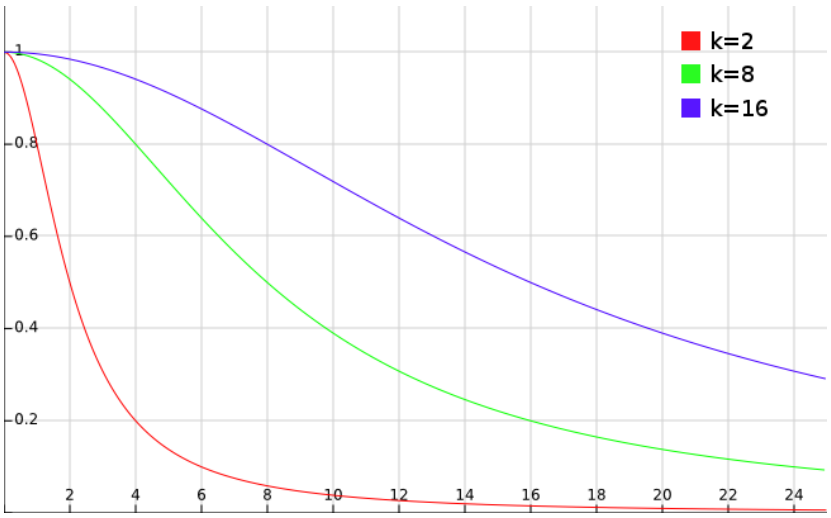

Рисунок 4.2 – Графіки функції g для кількох різних k

Можна побачити, що чим більше k, тим більше значення функції g для будь-якої фіксованої точки.

Наприклад, нехай у певній точці зображення $(\tilde{x}, \tilde{y})$, відомо значення норми градієнта на рівні $\tilde{t}$: $||\nabla I(\tilde{x}, \tilde{y}, \tilde{t})|| = 4$. Тоді $g_{k=2}\left(\left|\left|\nabla I\left(\widetilde{x, \tilde{y}, \tilde{t}}\right)\right|\right|\right) = g_{k=2}(4) = 0.2$, у той час як $g_{k=16}(4) \approx 0.94$. Виходить у першому випадку було слабко «згладжено» значення в точці, оскільки за введеним раніше критерієм вона швидше за все лежить на кордоні, а в другому – значення функції g практично одиниця, відповідно точка не вважається граничною і буде згладжена звичайним розмиттям Гауса.

Таким чином, k виступає в ролі «бар'єру» для шумів, і зі зростанням k зростає «вимога» на те, що точка буде вважатися граничною.

4.2 Дискретизація

Щоб перейти безпосередньо до алгоритму фільтра, необхідно зробити дискретизацію рівняння. Досить простою з погляду математичних викладок і невибагливою до обчислень буде дискретизація рівняння методом кінцевих різниць. Для зручності необхідно переписати основне рівняння:

$$\frac{\partial}{\partial t} I(x,y,t) = \frac{\partial}{\partial x}\left[c(x,y,t)\frac{\partial}{\partial x} I(x,y,t)\right] + \frac{\partial}{\partial y}\left[c(x,y,t)\frac{\partial}{\partial y} I(x,y,t)\right], \quad (4.8)$$

Записати умову стійкості для явної схеми, що вийшла, — нетривіальне завдання через нелінійність рівняння. Але Перона і Малік визначили, що за $\Delta x = \Delta y = 1$ схема буде стійка для всіх $0 \le \Delta t \le \frac{1}{4}$. Враховуючи цей факт і те, що дискретним представленням функції зображення буде матриця значень пікселів, необхідно переписати основну розрахункову схему матричного вигляду:

$$I_{i,j}^{t+1} = I_{i,j}^{t} + \Delta t\left[C_{N_{i,j}^t} \cdot \nabla N I_{i,j}^{t} + C_{S_{i,j}^t} \cdot \nabla S I_{i,j}^{t} + C_{E_{i,j}^t} \cdot \nabla E I_{i,j}^{t} + C_{W_{i,j}^t} \cdot \nabla W I_{i,j}^{t}\right], \quad (4.9)$$

де $\nabla N^{I_{i,j}^t} = I_{i-1,j}^{t} - I_{i,j}^{t}$;

$\nabla S^{I_{i,j}^t} = I_{i+1,j}^{t} - I_{i,j}^{t}$;

$\nabla E^{I_{i,j}^t} = I_{i,j+1}^{t} - I_{i,j}^{t}$;

$\nabla W^{I_{i,j}^t} = I_{i,j-1}^{t} - I_{i,j}^{t}$;

$C_{N_{i,j}^t} = g(||(\nabla I)_{i-1/2,j}^{t}||)$;

$C_{S_{i,j}^t} = g(||(\nabla I)_{i+1/2,j}^{t}||)$;

$C_{E_{i,j}^t} = g(||(\nabla I)_{i,j+1/2}^{t}||)$;

$C_{W_{i,j}^t} = g(||(\nabla I)_{i,j-1/2}^{t}||)$.

Для розрахунку коефіцієнтів C спочатку необхідно обчислити норму градієнта. Найпростіший спосіб апроксимувати норму градієнта - замінити її на довжину проекції градієнта на відповідну вісь різницевої сітки.

Хоча це досить груба заміна, що апроксимує дещо інше рівняння дифузії, вона тим не менш також забезпечує збереження загальної яскравості зображення, а також дає практично ідентичні результати в порівнянні з більш точною апроксимацією норми градієнта, виграючи у останньої швидкості обчислень.

Остаточно розрахункова формула виглядатиме так:

$$I_{i,j}^{t+1} = I_{i,j}^{t} + \Delta t[g(|N|) \cdot N + g(|S|) \cdot S + g(|E|) \cdot E + g(|W|) \cdot W], \quad (4.10)$$

де $N = \nabla N^{I_{i,j}^{t}}$;

$S = \nabla S^{I_{i,j}^{t}}$;

$E = \nabla E^{I_{i,j}^{t}}$;

$W = \nabla W^{I_{i,j}^{t}}$.

Схематично розрахункову схему можна зобразити як на малюнку нижче.

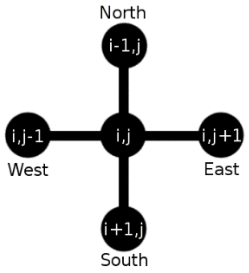

Рисунок 4.3 – Розрахункова схема

Тобто нове значення залежить від поточного значення та значень чотирьох сусідів осередку матриці. Виникає питання – як перераховувати граничні осередки, адже розрахункова схема у такому разі виходитиме за межі матриці.

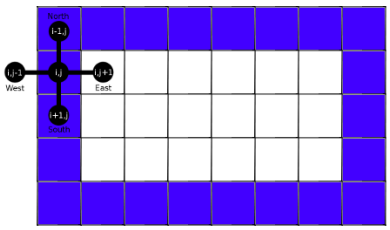

Рисунок 4.4 – Розрахункова схема у.межах матриці

Щоб фільтр змінював значення яскравості в осередках у межах максимуму та мінімуму яскравості вихідного зображення, процес, описаний основним рівнянням, має бути адіабатичним. Звідси отримується гранична умова Діріхле виду: $I(D) = 0$. Тобто межі просто заповнюється нулями [7].

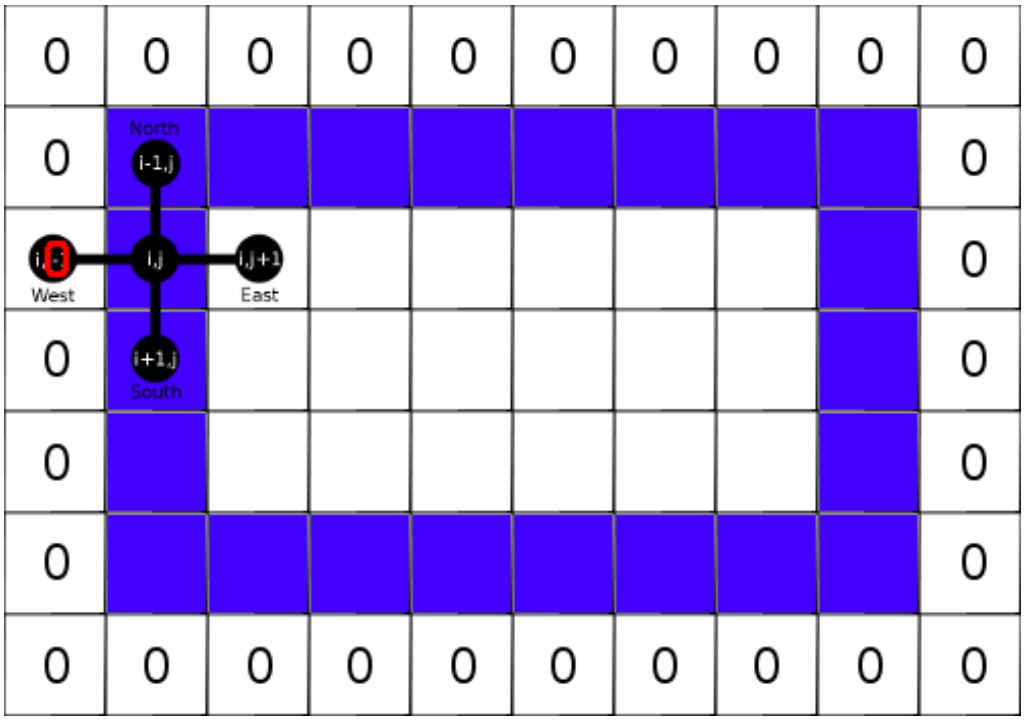

Рисунок 4.5 – Заповнення меж матриці нулями

4.3 Алгоритм

Виходячи з розрахункової формули в пам'яті завжди доведеться тримати як мінімум два двовимірні масиви, перший відповідатиме

оригінальному зображенню, другий — розмитому. Якщо провести аналогію з фільтром Гауса, то для розмиття зображення з радіусом t у фільтрі Перона та Маліка нам потрібно виконати $\frac{t}{\Delta t}$ повторень повного перерахунку зображення, щоразу замінюючи зображення з попереднього шару розмиття на «оригінальне».

Послідовність дій буде наступна:

1 визначити ширину та висоту зображення (w і h відповідно);

2 виділити пам'ять під двомірний масив розмірністю (w+2)*(h+2) (названий I);

3 виділити пам'ять під двомірний масив розмірністю (w+2)*(h+2) (названий BlurI);

4 заповнити масив нулями I = 0;

5 зчитати зображення та записати дані пікселів у центр масиву I (тобто залишити ліворуч, праворуч, зверху, знизу по одному нульовому стовпцю або рядку);

6 повторити поки що level<t (спочатку level=0);

7 створити та зберегти зображення з даних масиву BlurI. Це розмите зображення;

8 звільнити пам'ять та вийти із програми.

Для кольорових зображень принцип дій зберігається, але перерахунок потрібно виконувати окремо для кожного каналу.

4.4 Програмна реалізація

Найпростішим форматом, який до того ж розуміють і багато графічних редакторів є PGM P5. Це відкритий формат зберігання растрових зображень типу bitmap без стиснення у відтінках сірого. У нього простий заголовок ASCII, а саме зображення є послідовність однобайтних (для відтінків сірого від 0 до 255) цілих чисел без знака.

Процедура оформлена для роботи з PGM у вигляді модуля. Цей модуль

працює тільки із зображеннями з максимальним значенням сірого 255.

Програма починається з підключення модуля для роботи з PGM та оголошення всіх необхідних змінних.

Лістинг 4.1 – Підключення модуля та оголошення змінних

```
program blur
  use pgmio

  implicit none

  double precision, parameter :: t=10.0d0, deltaT=0.2d0,
k=10.0d0
  character*(*), parameter :: input='dif_tomography.pgm',
output='output.pgm'

  double precision, allocatable :: u(:,:), nu(:,:)
  double precision :: north, south, east, west, level
  integer :: w, h, offset, n, i, j

end program blur
```

Параметр t — це рівень розмиття, на якому необхідно припинити роботу алгоритму, deltaT — крок за часом, k — параметр поки що не описаної функції g. Input та output — файл із вихідним зображенням та вихідний файл відповідно.

Тепер треба розрахувати розміри вхідного зображення змінні w і h, виділити пам'ять для масиву зображення і масиву згладженого зображення та зчитати дані з файлу input.

Лістинг 4.2 – Виділення пам'яті

```
call pgmsize(input, w, h, offset)
allocate(u(0:w+1,0:h+1))
u=0
allocate(nu(w,h))
call pgmread(input, offset, w, h, u, 0, 0)
```

Процедура pgmread зчитує w*h байт, пропускаючи offset байт

(займаємих заголовком PGM) масив u. Останні два параметри повідомляють процедуру, що відлік у матриці u починається з нуля по кожному виміру.

Наступним кроком виконується саме згладжування.

Лістинг 4.3 – Виконання згладжування

```
level = 0 !лічильник рівня згладжування
  do while (level<t)
    do j=1,h
        do i=1,w
            north = u(i-1,j)-u(i,j)
            south = u(i+1,j)-u(i,j)
            east = u(i,j+1)-u(i,j)
            west = u(i,j-1)-u(i,j)
            nu(i,j) = u(i,j) +
deltaT*(g(north)*north+g(south)*south+g(east)*east+g(west)*west)
        end do
    end do
    u(1:w,1:h) = nu(1:w,1:h) !заміна оригінального на розмите
    level = level + deltaT
  end do
```

Наприкінці програми необхідно зберегти отримане згладжене зображення та звільнити пам'ять.

Лістинг 4.4 – Збереження отриманого зображення

```
deallocate(u)

  call pgmwriteheader(output, w, h)
  call pgmappendbytes(output, nu, 1, 1)

  deallocate(nu)
```

Процедура pgmwriteheader створює файл output і записує заголовок PGM P5. Процедура pgmappendbytes записує в кінець файлу output послідовність байт з nu, враховуючи, що індекси nu починаються з 1 по обидва виміри. Треба відмітити, що pgmappendbytes записує байти з двовимірного масиву знову ж таки в порядку стовпців, тому, хоча в пам'яті і

знаходилася транспонована версія зображення, при записі зображення транспонується назад.

4.5 Проведення експерименту

Для початку необхідно порівняти розмиття фільтра Перона і Маліка з гаусовим розмиттям при однакових t.

Рисунок 4.6 – Вихідне зображення

Треба виконати згладження цього зображення фільтром Гауса та фільтром анізотропної дифузії.

Рисунок 4.7 – Згладження фільтром Гауса (t=10)

Рисунок 4.8 – Згладження фільтром Пірона і Маліка (t=10)

Відмінно видно, як гаусове розмиття сильно змащує межі областей, у той час як фільтр анізотропної дифузії в цілому зберігає їх.

Тепер необхідно поекспериментувати із параметрами варіюючи k при

однакових t і deltaT (t=10, deltaT=0.2).

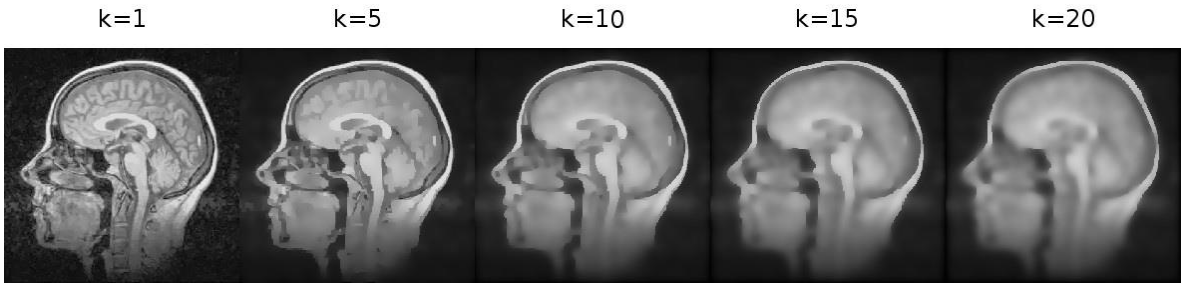

Рисунок 4.9 – Експеримент із параметрами

Можна побачити, що межі великих областей не зміщуються зі збільшенням k. Але дрібніші області поступово починають зливатися. При досить великому k фактично отримаємо гаусове розмиття, тому що умова на кордон не пройде жодна точка.

ВИСНОВКИ

Робота присвячена розробці програмного засобу для згладжування меж цифрових водяних знаків на великих зображеннях. Використання подібних програм дозволяє покращити безопасність зображень з точки зору захищення права власноссті.

Проведений аналіз існуючих рішень, під час якого виявилося, що забезпечення стійкості до атак видалення є більш менш вирішеним завданням, то забезпечення стійкості до геометричних атак і локальних змін зображення все ще мало вивчено, тому на вивчення останнього був зроблений фокус.

Була розглянута одна з можливих апроксимацій фільтра анізотропної дифузії.

Поставлені в роботі задачі виконані в повному обсязі. Подальший розвиток проекту передбачає продовження аналізу і покращення алгоритму згладжування меж ЦВЗ на великих зображеннях та блокування атак на системи ЦВЗ. Також можна провести експерименти з іншими функціями g, ввести функцію аналізу шуму для автоматичного підбору параметра k.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. О методе цифровых водяных знаков на основе особенностей изображения и моментов Цернике / О.Ю. Никитина // Штучний інтелект. — 2008. — № 3. — С. 339-37. — Бібліогр.: 14 назв. — рос.

2. Кайнов П. А. Внедрение цифровых водяных знаков с использованием сегментации изображения [Електронний ресурс] / П. А. Кайнов, Б. Б. Борисенко. – 2013. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/vnedrenie-tsifrovyh-vodyanyh-znakov-s-ispolzovaniem-segmentatsii-izobrazheniya/viewer.

3. Методы и средства сокрытия (маскирования) сообщений в стегоканалах, подвергаемых атакам [Електронний ресурс] // Национальная библиотека им. Н. Э. Баумана. – 2017. – Режим доступу до ресурсу: https://bit.ly/3NjY3ev.

4. Виды сглаживания и их особенности [Електронний ресурс] // i2HARD. – 2021. – Режим доступу до ресурсу: https://i2hard.ru/publications/27401.

5. ОСНОВНЫЕ ПОЛОЖЕНИЯ СТЕГАНОГРАФИИ [Електронний ресурс] // Защита информации. Конфидент. – 2000. – Режим доступу до ресурсу: http://citforum.ru/internet/securities/stegano.shtml.

6. Digital Image Watermarking Techniques [Електронний ресурс] // Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail-1902, Bangladesh. – 2020. – Режим доступу до ресурсу: https://www.mdpi.com/2078-2489/11/2/110/htm.

7. Сглаживание изображений фильтром анизотропной диффузии Перона и Малика [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://bit.ly/3NcYUgh.