

ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

Метод нанесення цифрового водяного знаку на текстурі тривимірних об'єктів

Автор:
Смирнов В.О.
ст. гр. СПМ-20-2

Керівник:
Мартовицький В.О.
доц. каф. ЕОМ, к.т.н.

Мета дослідження

- Проаналізувати існуючі методи будови водяних знаків текстури.
 - Створити та порівняти властивості систем на основі нейронної мережі та певного детермінованого алгоритму.
 - Порівняти системи за точністю зчитування водяних знаків.
 - Проаналізувати вплив атак на точність зчитування водяного знаку з атакваної текстури.
-

Типи й характеристики систем водяних знаків

Типи систем водяних знаків:

- Сліпі. Не потребують ніяких додаткових даних.
- Напівсліпі. Використовують певні дані, отримані з оригінальної текстури.
- Несліпі. Потребують оригінальну текстуру.

Характеристики:

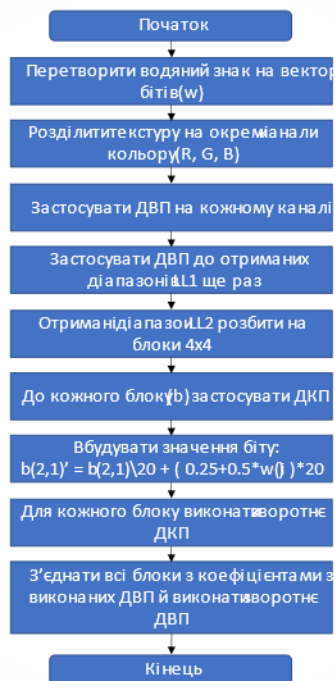
- Ємність. Обсяг вбудованих даних.
 - Надійність. Стабільність зчитування ЦВЗ, стійкість до атак.
 - Непомітність. Візуальна ідентичність вхідної текстури й текстуриконтейнера.
-

Баланс між характеристиками

- Умови непомітності, ємності та надійності суперечать один одному та накладають обмеження.
 - Можна підвищити надійність водяного знаку, але це призводить до більшої помітності ЦВЗ.
 - За умови непомітності водяний знак повинен бути створений з максимально можливим розділенням по оригінальним даних, щоб уникнути ситуації, коли невелике пошкодження текстури призведе до великого обсягу помилок.
 - Аналогічно, можна збільшити корисне навантаження даних, але це врівноважується втратою надійності.
 - Для будь-якої схеми водяних знаків неможливо виконати ці три вимоги одночасно, між ними треба знаходити баланс.
-

Система на основі детермінованих алгоритмів

- Базується на поєднанні дискретного вейвлетного та дискретного косинусного перетворень (ДВП-ДКП).
- Ці алгоритми частотної області обробки зображень часто використовуються в системах ЦВЗ, бо за їх допомогою можна сховати дані з мінімальними змінами зовнішнього вигляду.
- ДВП розкладає текстуру на піддіапазони, змінюючи які можна вбудувати водяний знак, змінюючи лише певну частину вхідної текстури.
- ДКП використовується для більшої стійкості атакам.
- Ця система може обробляти текстури розміром від 256x256 пікселів.
- У якості водяного знаку використовуються зображення розміром 18x18 пікселів, що складається з відтінків сірого.

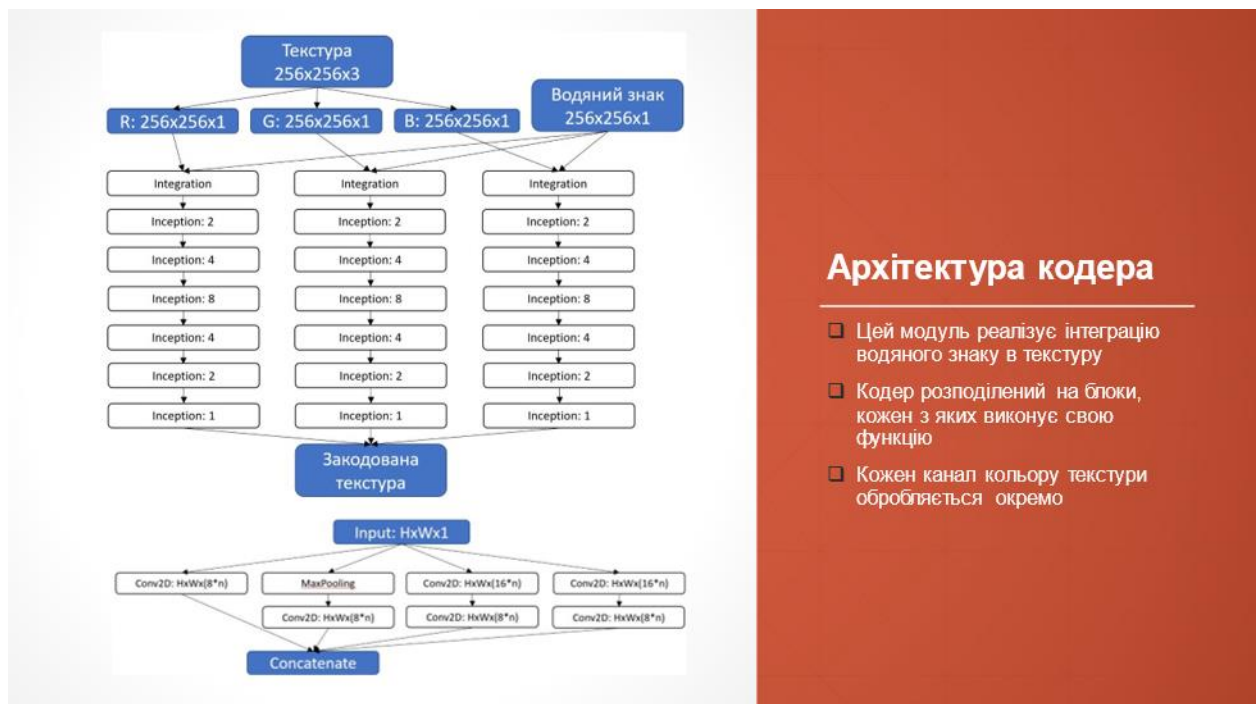


Алгоритм роботи системи заснованої на ДВП-ДКП

- ❑ Кожен канал кольору текстури обробляється окремо
- ❑ Виконується вейвлетне перетворення другого рівня
- ❑ ДКП виконується після ДВП
- ❑ Вбудова водяного знаку проводиться блочно

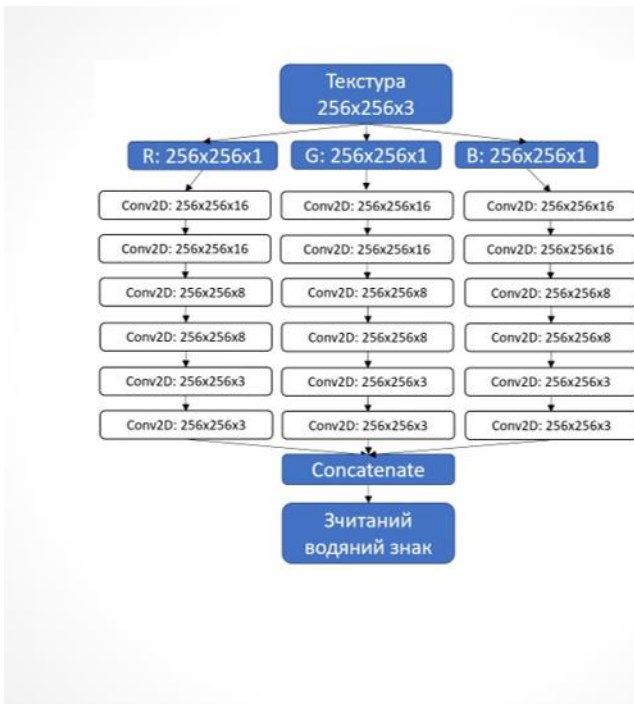
Система на основі нейронної мережі

- При створенні використалися сучасні підходи до побудови мереж.
- Основною операцією, що виконується нейронною мережею є згортка.
- Ця система може обробляти лише текстури розміром 256x256 пікселів, що мають 3 канали кольору.
- У якості водяного знаку використовуються зображення розміром 256x256 пікселів, що складається з відтінків сірого.



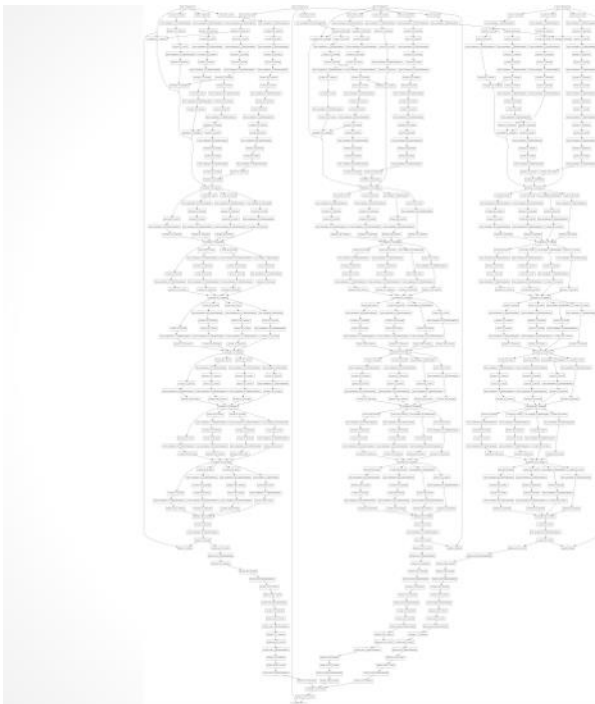
Архітектура кодера

- ❑ Цей модуль реалізує інтеграцію водяного знаку в текстуру
- ❑ Кодер розподілений на блоки, кожен з яких виконує свою функцію
- ❑ Кожен канал кольору текстури обробляється окремо



Архітектура декодера

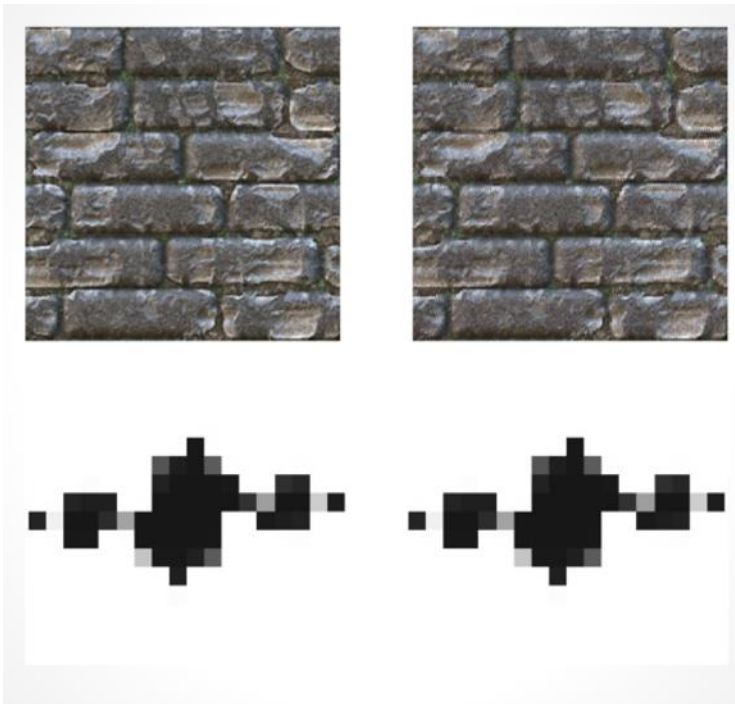
- ❑ Цей модуль відповідає за зчитування водяного знаку з текстури -контейнера
- ❑ Декодер має простішу структуру порівняно з кодером
- ❑ Кожен канал кольору текстури обробляється окремо також



Сукупна структура нейронної мережі

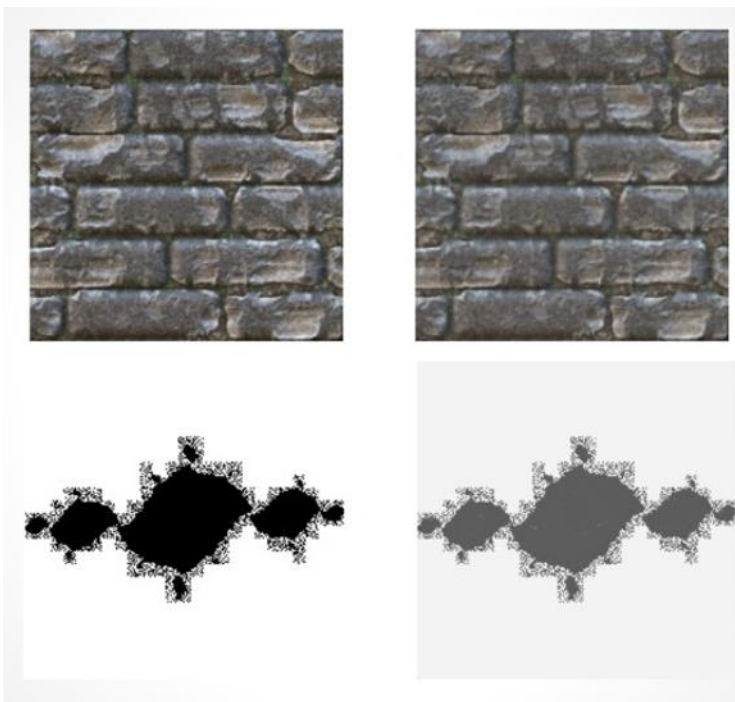
Це сукупна схема, в яку входять:

- Кодер
- Декодер
- Допоміжні шари мережі, необхідні під час навчання



Приклад роботи системи на основі ДВП-ДКП

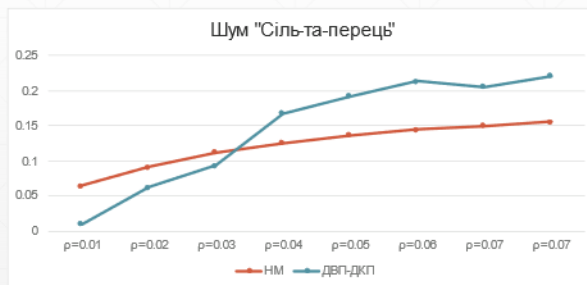
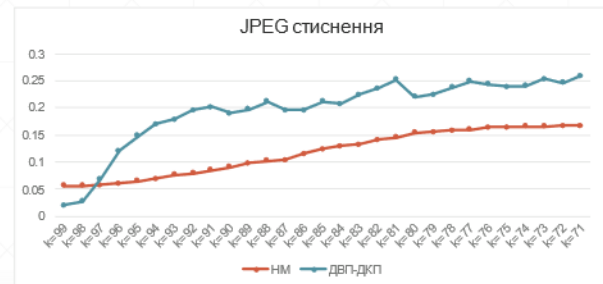
- ❑ Текстура -контейнер має ледве помітні зміни в світлих частинах порівняно з оригіналом
- ❑ Зчитаний водяний знак повністю відповідає тому, що був вбудований



Приклад роботи системи основаної на нейронній мережі

- ❑ Текстура після вбудови водяного знаку стала трохи яскравішою та має певне розмилування в центрі
- ❑ Зчитаний водяний знак навіть без атак не повністю відповідає оригіналу
- ❑ Водяний знак має значно меншу контрастність порівняно з оригіналом, але всі його деталі збережені

Результати перевірки стійкості атак



Висновки

- Обидві системи водяних знаків працюють та виконують поставлену задачу.
- Без зовнішнього впливу детермінований алгоритм зчитує водяний знак взагалі без помилок, на відміну від нейронної мережі.
- Система на основі нейронної мережі є більш стійкою до атак та має можливість вбудовувати значно більший обсяг даних.
- В майбутньому нейронна мережа може бути покращена завдяки:
 - розширенню розмірів текстур, які вона може обробляти;
 - розгляду нових метрик, які використовуються під час навчання мережі.

ДОДАТОК Б

Загальна схема розробленої нейронної мережі

