

## Підхід до вбудовування цифрових водяних знаків у медичні зображення DICOM із застосуванням згорткової нейронної мережі CNN

Вінницький національний технічний університет

### *Анотація*

*Запропонований підхід стеганографічного вбудовування цифрових водяних знаків у медичні зображення DICOM із застосуванням згорткової нейронної мережі CNN. Модель передбачає попереднє оброблення зображень та навчання CNN виявляти оптимальні ділянки для вбудовування ЦВЗ без втрати діагностичної цінності. Забезпечується висока непомітність вбудованих даних при збереженні якості зображень.*

**Ключові слова:** стеганографія, цифрові водяні знаки, DICOM, нейронні мережі.

### **An approach to embedding persistent digital watermarks in DICOM medical images using convolutional neural network CNN**

### *Abstract*

*The paper proposes an approach to steganographic embedding of digital watermarks in DICOM medical images using a convolutional neural network CNN. The model involves image preprocessing and training of CNNs to identify optimal areas for embedding DWMs without losing diagnostic value. It ensures high invisibility of embedded data while maintaining image quality.*

**Keywords:** steganography, digital watermarks, DICOM, neural networks.

### **Вступ**

Захист важливих медичних даних у цифрову епоху набуває особливої актуальності. Стеганографічне вкладення цифрових водяних знаків (ЦВЗ) у медичні зображення DICOM забезпечує автентичність та цілісність інформації. Однак традиційні методи можуть призводити до втрати якості зображень [1-3]. Тому пропонується удосконалений підхід із залученням згорткових нейронних мереж (CNN) для оптимізації вкладення ЦВЗ без суттєвого впливу на діагностичну цінність зображень.

### **Результати дослідження**

Опрацьовано значний теоретичний доробок в галузі стеганографічного захисту інформації, зокрема, варто відзначити таких закордонних та вітчизняних науковців: Блум Д., Весельська О., Денисюк В., Зюбіна Р., Калкер Т., Карпинець В., Кашук В., Кейр Ф., Кокс І., Кошкіна Н., Мельник С., Мілер М., Фрідріх Д., Хорошко В., Юдін О., Яремчук Ю. Незважаючи на наявність теоретичних напрацювань у галузі стеганографічного захисту даних, питання застосування сучасних методів глибокого машинного навчання, зокрема згорткових нейронних мереж CNN, для непомітного та стійкого вкладення цифрових водяних знаків у медичні зображення DICOM залишається недостатньо висвітленим і потребує додаткових досліджень.

У даній роботі пропонується підхід до стеганографічного вкладення ЦВЗ у медичні зображення DICOM, що ґрунтується на використанні згорткової нейронної мережі CNN. Запропонована структурна модель передбачає попереднє оброблення зображень, включно з фільтрацією, бінаризацією та виявленням зсувів і потоків за допомогою вейвлет-перетворень.

Ключовим етапом є навчання CNN на наборі медичних зображень та відповідних ЦВЗ із застосуванням методів регуляризації для покращення узагальнення. Навчена модель CNN стає здатною автоматично виявляти найменш зашумлені та найбільш стійкі ділянки кожного окремого зображення для безпосереднього вкладення ЦВЗ шляхом модифікації значень пікселів у цих регіонах.

CNN навчається на великому наборі прикладів медичних зображень DICOM для визначення оптимальних ділянок вкладення з мінімальним впливом на якість візуалізації. Це досягається шляхом оптимізації мережі за допомогою функції втрат, що поєднує візуальну подібність та надійність

вилучення ЦВЗ.

Запропонований підхід передбачає попереднє оброблення зображень, включно з фільтрацією, бінаризацією та виявленням зсувів і потоків за допомогою вейвлет-перетворень. Ключовим етапом є навчання CNN на наборі медичних зображень та відповідних ЦВЗ із застосуванням методів регуляризації для покращення узагальнення. Навчена модель CNN стає здатною автоматично виявляти найменш зашумлені та найбільш стійкі ділянки кожного окремого зображення для безпосереднього вкладення ЦВЗ шляхом модифікації значень пікселів у цих регіонах [4].

Цей підхід дозволяє адаптувати та вдосконалити процес вбудовування, забезпечуючи високу точність і ефективність за рахунок точного визначення найкращих регіонів на зображенні для безпечного розміщення додаткової інформації при збереженні візуальної цілісності медичних зображень без втрати діагностичної цінності.

Таким чином, структурна модель процесу вбудовування ЦВЗ у медичні зображення DICOM у роботі пропонується такою (рис. 1).

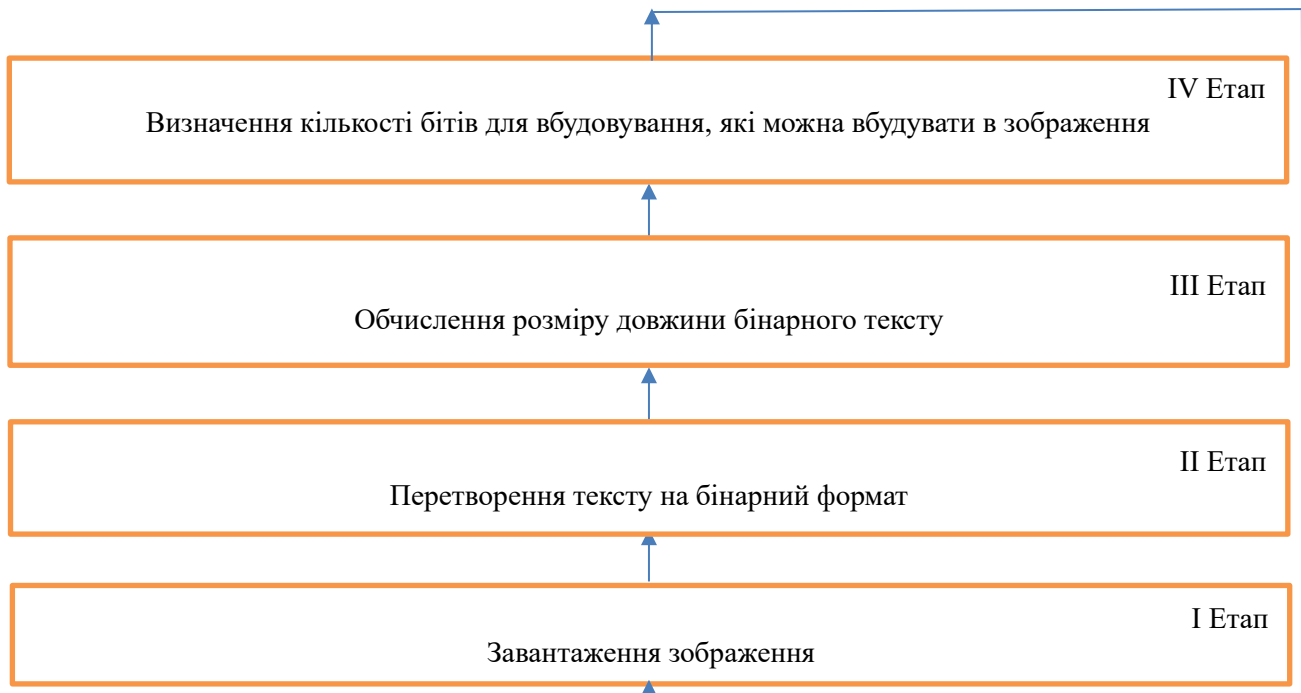


Рисунок 1 Структурна модель процесу вбудовування ЦВЗ у DICOM

Запропонована структурна модель процесу вбудовування цифрових водяних знаків у медичні зображення формату DICOM складається з чотирьох послідовних етапів.

Першим етапом є фільтрація вхідного зображення, що є стандартною процедурою попередньої обробки в задачах комп'ютерного зору. Фільтрація дозволяє виявити внутрішні особливості зображення, необхідні для подальшої обробки.

Другим етапом є бінаризація зображень шляхом застосування порогового значення для виділення областей гистограми. Під час бінаризації RGB-зображень або зображень у відтінках сірого порогове значення використовується для розподілу пікселів зображення на дві категорії. Для вибору оптимального порогового значення застосовується адаптивний алгоритм, заснований на аналізі піків гистограми. Зазначається, що бінаризація є ефективним способом сегментації кольорів на зображенні при використанні гистограм.

Третім етапом є виявлення зсувів та оптичних потоків (кореляція відеопотоків) за допомогою кореляційних відношень, заснованих на вейвлет-перетвореннях. Ці підходи є важливими інструментами в системах комп'ютерного зору, оскільки дозволяють виявляти зсуви та рухи об'єктів. Прості детектори зсуву реалізуються шляхом обчислення різниць корелятором.

Ключовим і завершальним етапом процесу вбудовування стійких ЦВЗ у медичні зображення DICOM є навчання згорткової нейронної мережі CNN на основі попередніх етапів обробки зображень.

Таким чином, модель поєднує традиційні методи обробки зображень та машинне навчання для вирішення завдання вбудовування ЦВЗ у медичні зображення формату DICOM [5].

Алгоритм вкладки ЦВЗ включає завантаження та передоброблення зображення, розрахунок доступного простору вкладки, перевірку достатності ємності й безпосереднє кодування інформації ЦВЗ у канали кольорів визначених оптимальних пікселів зображення. Координація процесу вкладки відбувається на основі параметрів, отриманих завдяки аналізу CNN. Таким чином, запропонований метод забезпечує високу непомітність вбудованих даних без втрат якості медичного зображення (рис.2).

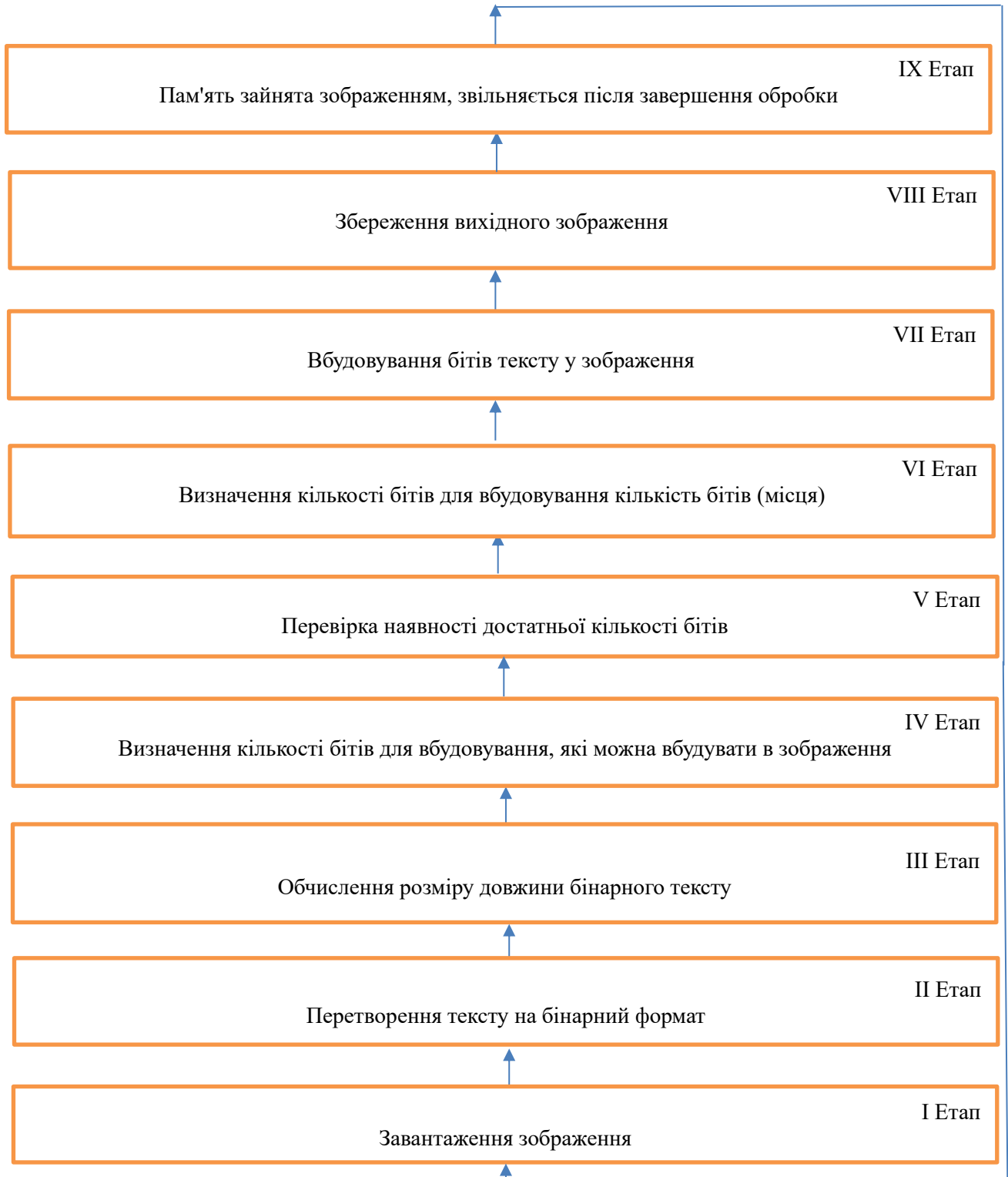


Рисунок 2 Деталізована структурна модель процесу вбудовування ЦВЗ у DICOM

Запропонована деталізована структурна модель складається з 9 етапів, що включають завантаження зображення, кодування тексту ЦВЗ, визначення доступного місця для вбудовування, безпосереднє вкладення біт ЦВЗ у канали кольорів оптимальних пікселів зображення визначених за допомогою CNN, збереження результату та звільнення пам'яті на рис.2.

Етап 1. На початковому етапі відбувається завантаження вихідного зображення у пам'ять. Функція отримує шлях до зображення та виконує його читання та передачу у внутрішнє подання даних.

Етап 2. Вхідний текст, який необхідно вбудувати у зображення, конвертується у бінарне подання для забезпечення сумісності з подальшою обробкою.

Етап 3. Визначається довжина бінарного подання тексту в бітах. Ця інформація є необхідною для наступного етапу - визначення достатності місця у зображенні для вбудовування.

Етап 4. Кількість бітів, які можна вбудувати у зображення, обчислюється як добуток кількості пікселів та параметра сили вкладання. Цей параметр вказує ступінь стійкості вбудованого тексту до можливих спотворень зображення.

Етап 5. На цьому етапі відбувається порівняння довжини бінарного тексту з кількістю доступних бітів у зображенні. Якщо довжина перевищує доступне місце, генерується повідомлення про помилку.

Етап 6. Відбувається безпосереднє вбудовування біт бінарного тексту у зображення. Для кожного пікселя змінюється його колір таким чином, щоб останній значущий біт відповідав чергового біту вбудованого тексту.

Етап 7. Після завершення вбудовування тексту, зображення з вбудованим текстом зберігається у вказаний вихідний файл.

Етап 8. Оскільки під час роботи алгоритму зображення завантажувалось у пам'ять, на цьому етапі відбувається звільнення займаної ним пам'яті для вивільнення системних ресурсів.

Етап 9. Після виконання всіх попередніх кроків робота алгоритму завершується. Вихідним результатом є зображення з вбудованим текстом.

Цей підхід забезпечує високу непомітність вбудованих даних при збереженні якості медичних зображень, що є важливим для їх діагностичної цінності.

Підсумовуючи, запропонований підхід із залученням потужних можливостей CNN для вибору оптимальних регіонів вкладання ЦВЗ є проривом у галузі стеганографічного захисту медичних зображень. Він дозволяє безпечно приховувати велику кількість аутентифікаційних даних без жодного візуально помітного впливу на діагностичну цінність зображень.

## **Висновки**

У роботі запропоновано удосконалений підхід до вбудовування стійких цифрових водяних знаків у медичні зображення формату DICOM із застосуванням згорткових нейронних мереж. Основні висновки полягають у наступному:

Розроблена структурна модель процесу вбудовування ЦВЗ у медичні зображення DICOM поєднує попереднє оброблення зображень, включно з фільтрацією, бінаризацією та виявленням зсувів і потоків за допомогою вейвлет-перетворень, з навчанням згорткової нейронної мережі на основі цих даних.

Навчена модель CNN стає здатною автоматично виявляти найменш зашумлені та найбільш стійкі ділянки окремих зображень для безпосереднього вбудовування ЦВЗ шляхом модифікації значень пікселів у цих регіонах.

Застосування CNN дозволяє адаптувати й оптимізувати процес вбудовування, забезпечуючи високу точність і ефективність за рахунок точного визначення найкращих регіонів на зображенні для безпечного розміщення додаткової інформації.

Запропонований підхід забезпечує високу непомітність вбудованих даних при збереженні візуальної цілісності медичних зображень без втрати їх діагностичної цінності.

Алгоритм вбудовування ЦВЗ включає завантаження та передоброблення зображення, розрахунок доступного простору вбудовування, перевірку достатності ємності й безпосереднє кодування інформації ЦВЗ у канали кольорів визначених оптимальних пікселів зображення на основі параметрів, отриманих від навченої моделі CNN.

Таким чином, запропонований підхід демонструє перспективність використання методів глибокого навчання, зокрема згорткових нейронних мереж, для удосконалення процесів стеганографічного вбудовування цифрових водяних знаків у медичні зображення DICOM з метою забезпечення автентичності та цілісності важливих медичних даних.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kalker T. Considerations on watermarking security / T. Kalker //IEEE International Workshop on Multimedia Signal Processing. – Cannes (France), 2001. – P. 201–206. (дата звернення: 16.05.2024)
2. ХОРОШКО, В. О.; ЯРЕМЧУК, Ю. Є.; КАРПІНЕЦЬ, В. В. Комп'ютерна стеганографія. 2017. – Вінниця : ВНТУ, 2017. – 155с. (дата звернення: 16.05.2024)
3. Павлов В.Г., Карнацький О.С. Особливості використання стеганографічних методів // Матеріали XI міжнародної науково-технічної конференції «АВІА-2013» - Т.1. – К.:НАУ, 2013, ст.2.41 - 2.44. (дата звернення: 17.05.2024)
4. Krizhevsky A. ImageNet classification with deep convolutional neural networks / A.Krizhevsky, I.Sutskever, E.Geoffrey // Communications of the ACM. – 2017. – Vol. 6, № 60. – P. 84–90. (дата звернення: 18.05.2024)
5. Лебедев В.О. Розпізнавання медичних зображень на основі згорткової нейронної мережі /В.М. Гусятін, В.О. Лебедев // Проблеми інформатизації: Матеріали сьомої міжнародної науково-технічної конференції Черкаси– Харків Баку–Бельско-Бяла., Том 3. 13-15 листопада 2019 р., С.35. (дата звернення: 18.05.2024)

*Азарова Анжеліка Олексіївна* – к.т.н., професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, [azarova.angelika@gmail.com](mailto:azarova.angelika@gmail.com)

*Azarova A. Anzhelika* – Ph.D., Professor, Department of Information Systems Management and Security, Vinnytsia National Technical University, Vinnytsia, e-mail: [azarova.angelika@gmail.com](mailto:azarova.angelika@gmail.com)

*Шевчук Адам Володимирович* — студент групи ІКІТС-206, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: [adam.5s@ukr.net](mailto:adam.5s@ukr.net)

*Shevchuk Adam V.* – student of ICITS-20b group, Faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, e-mail: [adam.5s@ukr.net](mailto:adam.5s@ukr.net)