УДК 004.056.5

Ю. Є. Яремчук

М. В. Усач

Удосконалення методу виявлення прихованої інформації у цифрових зображеннях на основі штучного інтелекту

Вінницький національний технічний університет

Анотація *У роботі проаналізовано сучасні підходи до стеганографії та стеганоаналізу, визначено їхні переваги й обмеження. Запропоновано метод, що використовує згорткову нейронну мережу (CNN) для автоматичного розпізнавання ознак стеганографічного вбудовування. Розроблено програмну модель, яка здійснює попередню обробку зображень, аналіз та класифікацію за наявністю прихованих даних. Проведено тестування та верифікацію ефективності моделі за основними метриками точності та достовірності.*

Результати дослідження можуть бути використані в системах кіберзахисту для автоматичного виявлення несанкціонованих інформаційних впливів.

Ключові слова: *стеганографія, стеганоаналіз, згорткова нейронна мережа, цифрове зображення, штучний інтелект, виявлення інформації, кібербезпека.*

Abstract. *The study analyzes modern approaches to steganography and steganalysis, identifying their advantages and limitations. A method based on a convolutional neural network (CNN) is proposed for automatic recognition of steganographic embedding features. A software model has been developed that performs image preprocessing, analysis, and classification to detect the presence of hidden data. Testing and verification of the model's effectiveness were carried out using key accuracy and reliability metrics.*

The research results can be applied in cybersecurity systems for automatic detection of unauthorized information manipulation.

Keywords*: steganography, steganalysis, convolutional neural network, digital image, artificial intelligence, information detection, cybersecurity..*

Вступ

Сучасна епоха характеризується інтенсивним розвитком інформаційних технологій і повсюдним поширенням цифрових систем, що істотно впливають на всі сфери суспільного життя. Цифрові комунікації та зростання обсягів мультимедійного контенту призвели до істотного ускладнення завдань, пов'язаних із забезпеченням кібербезпеки. У сучасному інформаційному середовищі питання захисту даних виходять далеко за межі класичних методів шифрування чи контролю доступу. Одним із найменш помітних, але потенційно небезпечних напрямів є приховане передавання інформації за допомогою стеганографії, коли відомості вбудовуються у звичайні цифрові об'єкти, зокрема у зображення, аудіо- або відеофайли.

Результати дослідження

У межах даного дослідження метод стеганографічного вбудовування LSB (Least Significant Bit) використовується як модельний приклад формування стеганографічних змін у цифрових зображеннях. Його застосування обумовлене простотою реалізації, широким поширенням та можливістю керованого формування навчальної вибірки. Метод LSB у роботі не розглядається як інструмент захисту інформації, а використовується виключно як джерело контрольованих спотворень, що дозволяють дослідити ефективність алгоритмів виявлення.

Основним інструментом виявлення прихованої інформації у даній роботі обрано згорткові нейронні мережі (Convolutional Neural Networks, CNN). Такий вибір зумовлений здатністю CNN автоматично виділяти просторові ознаки у зображеннях та виявляти слабкі, малопомітні зміни структури пікселів, які виникають унаслідок стеганографічного впливу. На відміну від класичних статистичних (RS-аналіз, χ^2-тест), які ґрунтуються на ручному підборі ознак, нейронна мережа формує власні ознаки в процесі навчання.

Для підвищення чутливості до локальних аномалій у роботі використовується удосконалена архітектура CNN з подвійним потоком обробки. Перший потік аналізує вихідне зображення, зберігаючи його глобальну структуру, тоді як другий працює з високочастотною картою, отриманою шляхом застосування спеціального фільтра попередньої обробки. Такий підхід дозволяє одночасно враховувати як загальні, так і дрібномасштабні спотворення.

На відміну від одношарових та класичних CNN-архітектур, запропонована модель здійснює

об’єднання ознак з двох паралельних гілок за допомогою механізму feature fusion, що підвищує інформативність вектору ознак. Додатково використовується регуляризація DropConnect, яка зменшує ризик перенавчання та підвищує стійкість моделі до шуму та втрат якості, зокрема при JPEG-стисненні.

Запропонована архітектура орієнтована на виявлення ознак, характерних не лише для LSB-вбудовування, а й для більш складних стеганографічних методів (DCT, WOW, HUGO), що забезпечує її універсальність. Таким чином, використання CNN як основи удосконаленого методу дозволяє підвищити точність виявлення, зменшити кількість хибних рішень та забезпечити адаптивність системи до різних форматів цифрових зображень.

Обґрунтування вибору згорткової нейронної мережі ґрунтується на її доведеній ефективності у задачах аналізу зображень, автоматичного вилучення просторових ознак та здатності до узагальнення, що робить її доцільною основою для створення сучасних стеганоаналітичних систем.

Удосконалення методу виявлення прихованої інформації

Після аналізу теоретичних підходів і сучасних досліджень у галузі стеганоаналізу стає очевидним, що одним з найефективніших напрямів є використання CNN-моделей — згорткових нейронних структур, що використовуються для обробки та класифікації зображень. Такі мережі дають змогу самостійно виокремлювати закономірності у структурі пікселів і визначати, чи містить зображення ознаки стеганографічного вбудовування.

Розроблення власної моделі CNN у межах даного дослідження має на меті створити демонстраційний прототип, здатний обробляти цифрові зображення, аналізувати їхній зміст і робити висновок про наявність прихованої інформації. Ця модель не призначена для комерційного застосування, однак демонструє принципову можливість використання штучного інтелекту для автоматизованого виявлення стеганографії у середовищах кіберзахисту.

Висновки

У цьому розділі розроблено удосконалений алгоритм методу стеганоаналізу цифрових зображень на основі згорткових нейронних мереж. На основі порівняльного аналізу сучасних архітектур (Xu-Net, Ye-Net, SRNet, EfficientNet) обґрунтовано вибір SRNet як базової моделі завдяки її здатності ефективно виявляти слабкі статистичні спотворення, характерні для стеганографічних вбудовувань.

Запропоновано структурне удосконалення методу шляхом введення подвійного потоку обробки (оригінальне зображення та високочастотно фільтрована карта), а також додавання блоку уваги (Attention), що дає змогу моделі акцентуватися на малопомітних локальних змінах. Описано математичну модель функціонування модифікованої мережі та логіку проходження даних між її компонентами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Усач Микола Васильович – студент групи 2КІТС-24м, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: usachamykola@gmail.com

Науковий керівник: Яремчук Юрій Євгенович – доктор технічних наук, професор, директор Центру інформаційних технологій і захисту інформації, голова секції «Управління інформаційною безпекою» та професор кафедри менеджменту та безпеки інформаційних систем, науковий керівник науково-дослідної лабораторії технічного захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: yurevyar@vntu.edu.ua

Usach Mykola Vasylovych – student of group 2KITS-24m, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: usachamykola@gmail.com

Scientific : Yaremchuk Yurii Yevhenovych – Doctor of Technical Sciences, Professor, Director of the Center for Information Technologies and Information Protection, Head of the “Information Security Management” section, and Professor of the Department of Management and Information Systems Security, Scientific Supervisor of the Research Laboratory of Technical Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: yurevyar@vntu.edu.ua