УДК 004.056

Труханська В. О., здобувачка 3 курсу спеціальності 122 Комп'ютерні науки,
Хмелівський Ю. С., асистент кафедри інформаційних технологій

ОГЛЯД НАПРЯМІВ ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ У ВІДЕОФАЙЛАХ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі, коли все більше інформації передається в цифровому вигляді, проблема захисту інформації від стороннього втручання є доволі поширеною. Електронне підслуховування, шахрайство, комп'ютерні віруси та інші електронні загрози можуть призвести до серйозних наслідків, як-от втрата конфіденційності або фінансові втрати. Дослідження методів цифрової стеганографії – це актуальне завдання, яке сприятиме покращенню захисту інформації в цифровому світі.

Існують два основні напрями розв'язання задачі прихованої передачі даних: криптографія та стеганографія. Метою криптографії є обмеження доступу до інформації шляхом її шифрування. На відміну від криптографії, стеганографія дає змогу приховати сам факт наявності прихованих даних. Бурхливий розвиток інформаційних технологій в останні роки дав суттєвий поштовх для появи і покращення методів комп'ютерної стеганографії. З'явились нові варіанти застосування – приховані повідомлення вбудовують у графічні, аудіо- та відеоматеріали, текстові файли та навіть у файли програм [1]. Комп'ютерна стеганографія базується на двох принципах: файли, що містять зображення чи звукові матеріали, можуть бути певною мірою змінені без втрати функціональності, і органи чуття людини не здатні відрізнити незначні зміни в кольорі або якості звуку. Другий принцип можна успішно використовувати з огляду на надлишковість деяких сучасних аудіо- та графічних форматів: наприклад, зміна найменш значимих бітів 24-бітного зображення, які відповідають за колір конкретного пікселя, не призводить до явних змін у зображенні [2].

Сьогодні через збільшення об'ємів інформації та збільшення пропускної здатності каналів зв'язку все більшу актуальність має питання приховування інформації у відеопослідовностях. Передача цифрового відео в останні роки є типовою подією і не викликає підозр. Наприклад, сервіс YouTube нараховує сотні мільйонів відеофайлів, причому один і той же відеоматеріал зустрічається в різних форматах. Велика кількість відеофайлів розміщується в P2P-мережах. Були розглянуті деякі особливості використання форматів відеофайлів для приховування інформації. Незважаючи на те, що існує велика кількість відеоформатів, на практиці для приховування інформації використовуються формати

MPEG-2 і MPEG-4. Розглянемо три способи вбудовування інформації в файли формату MPEG-2: вбудовування на рівні коефіцієнтів, на рівні бітової площини і завдяки енергетичній різниці між коефіцієнтами [5].

У першому способі біти приховуваної інформації вбудовуються в коефіцієнти дискретного косинусного перетворення (ДКП). Головною проблемою модифікації коефіцієнтів ДКП в стисненому потоці відео є накопичення зміщень та помилок. Спотворення, викликані зміною коефіцієнтів ДКП, можуть поширюватися в часовій і в просторовій областях, тому для компенсації спотворень додають спеціальний сигнал. Через обмеження бітової швидкості, під час додавання даних змінюються лише 10–20 % коефіцієнтів ДКП. Під час використання цього методу приховувана інформація зберігається під час фільтрування, зашумлення адитивним шумом і дискретизації [3].

Другий метод відрізняється високою пропускною здатністю і невеликою обчислювальною складністю. Але є й істотний недолік: інформація вбудована так, що може бути легко видалена. Під час повторного накладенні послідовності біт якість відео погіршиться незначно, а прихована інформація буде знищена.

В основі останнього методу лежить диференціальне вбудовування енергії (ДВЕ). Цей метод може бути застосований не лише до відеоданих MPEG, але і до інших алгоритмів стиснення відео. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП, і це має свої переваги. Алгоритм ДВЕ вносить у відео менше спотворень, ніж метод вбудовування інформації на рівні бітової площини. Для видалення прихованої інформації потрібне проведення більш складних обчислювальних операцій, ніж вбудовування нової довільної бітової послідовності [4].

Стеганографія – перспективний метод захисту даних, що ґрунтується на маскуванні зберігання та передачі інформації у масиві даних контейнера. Для досягнення мети розглянуто низку прийомів, із яких найбільш ефективним є застосування надлишковості медіафайлів. У процесі дослідження було розглянуто особливості приховування інформації у відеофайлах, здійснено порівняння наявних алгоритмів комп'ютерної відеостеганографії.

Список використаних джерел

1. Стеганографія: навч. посіб. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. Харків: Вид. ХНЕУ, 2011. 232 с.

2. Комп'ютерна стеганографія: навч. посіб. / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. Вінниця: ВНТУ, 2017. 155 с.

3. Що таке стеганографія? URL: https://uk.theastrologypage.com/steganography (дата звернення: 24.11.2023).

4. Digital Watermarking and Steganography / I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker. London: Elsevier, 2008. 593 p.

5. Wayner P. Disappearing Cryptography: Information Hiding: Steganography and Watermarking. London: Elsever, 2009. 440 p.

УДК 004.43

Труханська В. О., здобувачка 3 курсу спеціальності 122 Комп'ютерні науки,
Хмелівський Ю. С., асистент кафедри інформаційних технологій

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МОВ ОБРОБКИ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі дані стають все більш важливими. Вони використовуються в різних сферах діяльності, від бізнесу до науки. Для аналізу їх даних використовуються різні методи, зокрема статистичний аналіз та машинне навчання, а для реалізації цих методів – мови програмування. У наш час існує велика кількість мов програмування, які дають змогу систематизувати послідовність операцій, що здійснюються з даними, насамперед у комп'ютері, для отримання нової інформації шляхом обчислень, перегляду і уточнення наявної інформації. Найпопулярнішими мовами є Python та R.

Python – це універсальна високорівнева мова програмування, яка широко використовується в різних галузях, а також орієнтована на підвищення продуктивності розробника і полегшення процесу читання коду. Python має простий та інтуїтивно зрозумілий синтаксис, що робить його відносно легким для вивчення. Водночас стандартна бібліотека має достатній обсяг корисних функцій [1].

Мова R спеціально розроблена для статистичного аналізу та машинного навчання і використовується для аналізу даних та складання прогнозів. R має широкий спектр вбудованих функцій, бібліотек та пакетів для вирішення різних завдань. Для статистики, управління даними та їх візуалізації існують стандартні функції та прогресивні алгоритми машинного навчання. До того ж R має велику спільноту користувачів, які створюють пакети для різних завдань [2].

Отже, спершу необхідно зрозуміти, в яких випадках краще застосовувати R, а в яких Python. R зазвичай застосовується в тих випадках, коли для аналізу даних потрібні виділені обчислювальні потужності або окремі сервери. R добре підходить для дослідницької роботи, зручна та практична за будь-якого варіанта аналізу даних, оскільки в мові R існує безліч пакетів, а також готові тести, які забезпечують потрібний інструментарій для швидкого старту. R навіть може бути корисною під час роботи з великими даними [3].

Python може знадобитись у випадках, коли завдання, які пов'язані з аналізом даних, вмонтовуються в роботу вебдодатків, або якщо статистичний код