

АНАЛІЗ МЕТОДІВ ЗАХИСТУ БІОМЕДИЧНИХ ЗОБРАЖЕНЬ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз сучасних методів захисту біомедичних зображень від несанкціонованого доступу. Обґрунтовано доцільність застосування стеганографічних підходів для забезпечення конфіденційності медичних даних. Запропоновано метод приховування рентгенівського зображення в іншому рентгенівському зображенні як контейнері. Розглянуто можливості реалізації методу з використанням спектральних перетворень, зокрема перетворення Фур'є, перетворення Уолша–Адамара та дискретного косинусного перетворення.

Ключові слова: несанкціонований доступ, шифрування, стеганографія, перетворення Фур'є, перетворення Уолша–Адамара, дискретне косинусне перетворення.

Abstract

The paper analyzes modern methods for protecting biomedical images against unauthorized access. The feasibility of applying steganographic approaches to ensure the confidentiality of medical data is substantiated. A method for concealing an X-ray image within another X-ray image used as a container is proposed. The possibilities of implementing the method using spectral transforms are considered, in particular the Fourier transform, the Walsh–Hadamard transform, and the discrete cosine transform.

Keywords: unauthorized access, encryption, steganography, Fourier transform, Walsh–Hadamard transform, discrete cosine transform.

Вступ

Віддалена радіологія стала невід'ємною частиною сучасної медичної практики, забезпечуючи швидкий доступ до діагностичних зображень та висновків, незалежно від географічного положення пацієнта або лікаря. Однак, разом із розвитком технологій з'являються нові виклики, пов'язані з безпекою та конфіденційністю медичної інформації [1].

Дані медичних обстежень, особливо радіологічні зображення, можуть містити чутливу інформацію про стан здоров'я пацієнта, що робить їх цінною мішенню для кіберзлочинців. Несанкціонований доступ до таких даних може призвести до їх неправомірного використання, наприклад, для шантажу, незаконного продажу або зміни діагнозу.

Огляд методів захисту біомедичних зображень

Всі методи захисту біомедичних зображень від несанкціонованого доступу можна розділити на дві групи [1]:

- традиційні методи захисту файлів;
- методи що враховують специфіку зображень.

До методів захисту першої групи можна віднести такі [1]:

1. Шифрування даних: Шифрування біомедичних зображень перед їх зберіганням або передачею є одним з найефективніших способів захисту. Використання алгоритмів шифрування, таких як AES (Advanced Encryption Standard), забезпечує високий рівень безпеки.

2. Контроль доступу: Впровадження систем контролю доступу, які обмежують доступ до біомедичних зображень лише авторизованим користувачам. Це може включати використання паролів, біометричної аутентифікації або багатофакторної аутентифікації.

3. Аудит та моніторинг: Регулярний аудит та моніторинг доступу до біомедичних зображень допомагає виявляти та запобігати несанкціонованому доступу. Це включає ведення журналів доступу та аналіз підозрілої активності [1].

4. Використання VPN: Віртуальні приватні мережі (VPN) забезпечують безпечний канал для передачі даних через Інтернет, що допомагає захистити біомедичні зображення від перехоплення під час передачі.

5. Захист хмарних сховищ: Якщо біомедичні зображення зберігаються в хмарі, важливо використовувати хмарні сервіси з вбудованими функціями шифрування та контролю доступу.

Існують специфічні методи захисту біомедичних зображень, які враховують особливості цих даних. Деякі з них такі [2]:

1. Водяні знаки: Вбудовування водяних знаків у біомедичні зображення допомагає ідентифікувати джерело зображення та виявляти несанкціоноване копіювання або модифікацію.

2. Стиснення з шифруванням: Використання методів стиснення даних разом із шифруванням дозволяє зменшити обсяг даних для зберігання та передачі, одночасно забезпечуючи їх захист.

3. Анонімізація даних: Видалення або маскування особистої інформації з біомедичних зображень перед їх обробкою або передачею допомагає захистити конфіденційність пацієнтів.

4. Блокчейн: Використання блокчейн-технологій для зберігання та передачі біомедичних зображень забезпечує високий рівень безпеки та прозорості, оскільки кожна транзакція записується у незмінний реєстр.

5. Машинне навчання для виявлення аномалій: Використання алгоритмів машинного навчання для аналізу доступу до біомедичних зображень та виявлення підозрілої активності може допомогти запобігти несанкціонованому доступу.

Однак, поки що недостатня увага приділяється стеганографічним методам захисту біомедичних зображень. Стеганографія - це наука про приховану передачу інформації за допомогою збереження в таємниці самого факту передачі [3]. Якщо криптографічні методи, швидше за все, слід відносити до оборонних інструментів інформаційного протистояння, то стеганографія через свою специфіку може стати в XXI столітті технологією створення нової високоефективної інформаційної зброї.

Для стеганографії важливим є вибір контейнера для приховування повідомлення. Найбільшу місткість забезпечують контейнери у вигляді файлів зображень, у яких можна замінити в кожному пікселі по крайній мірі 1 молодший біт по кожній складовій кольору на біт повідомлення, тобто у пікселі можна приховати мінімум 3 біти інформації. Якщо в якості контейнера для приховування рентгенівського знімка вибрати інший рентгенівський знімок, то кількість прихованих біт в кожному пікселі можна збільшити до 6 без втрати візуальної якості зображення і виявлення факту приховування іншого зображення в зображенні-контейнері, оскільки рентгенівський знімок це зображення з вузьким динамічним діапазоном, з наявністю ділянок з плавною зміною яскравості.

Відомо два методи приховування повідомлень в зображеннях:

- приховування в просторовій області, тобто безпосередньо в пікселях зображення;
- приховування в частотній області, тобто в коефіцієнтах деякого перетворення, які отримують із зображення. Наприклад, перетворення Фур'є, Уолша-Адамара, дискретне косинусне перетворення або інше. Приховування в частотній області вимагає значно більше обчислень, але забезпечує збільшення ємності контейнера [4-6].

Експерименти показали, що якщо в якості контейнера використати ненормалізовані трансформанти перетворення Уолша-Адамара, отримані з рентгенівського зображення, то кількість молодших біт, які використовуються для приховування в кожному пікселі зображення-контейнера можна збільшити до 4 по кожній складовій кольору [5-6].

Висновки

Встановлено, що у разі використання рентгенівського зображення як контейнера для приховування іншого рентгенівського зображення забезпечується можливість збільшення ємності вбудовування даних. Зокрема, при реалізації методу в просторовій області кількість вбудованих бітів у кожен кольоровий складовий піксель може бути збільшена до двох без суттєвого погіршення візуальної

якості контейнера. У випадку застосування методів вбудовування в частотній області цей показник може бути підвищений до чотирьох бітів за умови збереження прийнятних значень об'єктивних метрик якості зображення (зокрема, PSNR).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Безпека та конфіденційність у віддаленій радіології. [Електронний ресурс]. <https://radiolance.ua/bezpeka-ta-konfidentsijnist-u-viddalenij-radiologiyi/>
2. Конспект лекцій з вивчення дисципліни «Обробка біомедичних зображень та реконструкція об'єктів» для студентів спеціальності 163 - Біомедична інженерія освітня програма Інтелектуальні штучні імпланти та медичні апарати в біоінженерії / Уклад. Л.Г. Коваль. – Вінниця : ВНТУ, 2020.
3. Хорошко, В.О. К Комп'ютерна стеганографія: навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінєць. – Вінниця: ВНТУ, 2017. – 155 с.
4. Грицишин В. О., Майданюк В. П. Ущільнення зображень з використанням перетворення Уолша-Адамара. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/view/17603/14625> (дата звернення 21.10.2023). - Назва з екрана.
5. Майданюк В. П., Грицишин В. О. Захист біомедичних зображень від несанкціонованого доступу. / Інформаційні технології і автоматизація – 2024 / Матеріали XVII міжнародної науково-практичної конференції. Одеса, 31 жовтня - 1 листопада 2024 р. - Одеса, Видавництво ОНТУ, 2024 р. – С. 200-201.
6. Грицишин В. О., Майданюк В. П. Використання стеганографії для захисту рентгенівських знімків / Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції 20-21 листопада 2024 р. – Суми/Вінниця: НІКО/ КЗВО «Вінницька академія безперервної освіти», 2024. – 336 с.

Майданюк Володимир Павлович - канд. техн. наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: maidaniuk2000@gmail.com.