УДК 004.056

# ЗАХИСТ БІОМЕДИЧНИХ ЗОБРАЖЕНЬ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Майданюк В.П., Грицишин В.О. (maidaniuk2000@gmail.com)
Вінницький національний технічний університет (Україна)

*Розглянуто особливості захисту біомедичних зображень від несанкціонованого доступу за рахунок використання криптографічних та стеганографічних методів. Показано, що при приховуванні рентгенівських знімків в контейнерах того типу кількість молодших біт, що використовуються для приховування в кожному пікселі зображення-контейнера може бути збільшена до 4 по кожній складовій кольору.*

## Вступ

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 [1].

Можна виділити такі напрямки вирішення задачі захисту біомедичних зображень:

- традиційний – шифрування файлів зображень [2];
- врахування специфіки зображення – виконуються будь-які перетворення в площині зображення, які виключають відтворення початкового зображення без спеціальних засобів. Після перетворення зображення зберігається у початковому форматі.

Другий підхід має переваги, оскільки дозволяє реалізувати специфічні алгоритми перетворення простіші в реалізації, а збереження зображення у тому ж форматі приховує факт перетворення – ущільнення, шифрування та інше.

Загальна схема системи захисту наведена на рис. 1.


Рисунок 1 – Загальна схема захисту зображень від несанкціонованого доступу

Тобто вхідними і вихідними даними є файли у форматі зображення. В якості перетворень можуть застосовуватись криптографічні, стеганографічні або інші перетворення в площині зображення, а не з файлами.

## Використання стеганографії для захисту рентгенівських знімків

Стеганографія (пер. з грец, «тайнопис») — це наука про приховану передачу інформації за допомогою збереження в таємниці самого факту передачі. 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.

Рентгенівські знімки це зображення з вузьким динамічним діапазоном, з наявністю ділянок з плавною зміною яскравості, тому слід очікувати, що кількість прихованих біт в кожному пікселі можна збільшити без втрати візуальної якості зображення, а відповідно і ймовірності виявлення факту приховування іншого зображення в зображенні-контейнері.

Для проведення досліджень в якості контейнера використовується зображення типу рентгенівський знімок, приховується зображення того ж типу.

Алгоритм захисту включає такі кроки:

1. Розсіювання бітів зображення, що захищається в площині зображення контейнера з використанням конгруентного генератора псевдовипадкових чисел (ПВЧ) та їх гамування. Для кожної складової кольору (RGB) використовується свій генератор ПВЧ. Він формує послідовності псевдовипадкових чисел T(i) у відповідності з співвідношенням [3]:

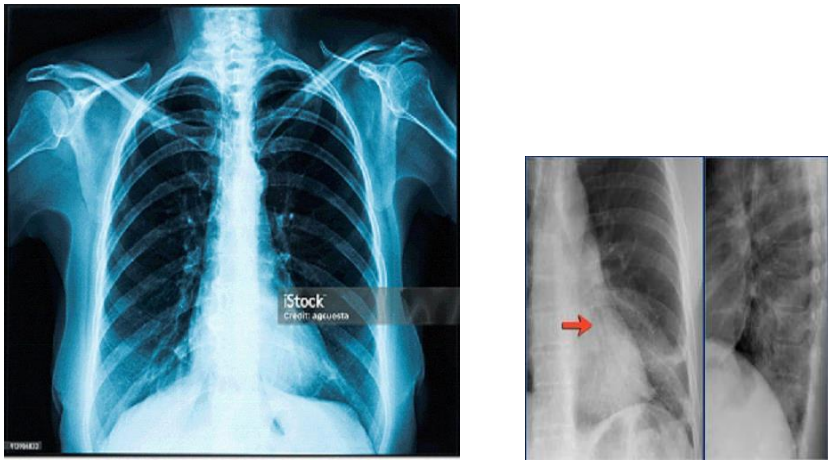
$$T(i+1) = (A*T(i)+C) \bmod M \quad (1)$$

де T(0) – початкова величина, обрана як твірне число;

A і C – константи.

Такий датчик ПВЧ генерує псевдовипадкові числа з визначеним періодом повторення, що залежить від обраних значень A и C. Лінійний конгруентний генератор має максимальну довжину $M=2^n$ тільки тоді, коли C - непарне; A mod 4 = 1. Значення T(0), A, C можуть бути ключем шифру. A в якості значення M вибирається найближче число кратне «2» більше кількості пікселів в зображенні-контейнері, що підвищує криптостійкість шифрування.

2. В кожному пікселі контейнера приховується 12 біт зображення що захищається Для приховування використовуються 4 молодших біти в кожній складовій кольору. Причому дані, що приховуються в поточному пікселі контейнера належать різним пікселям зображення, що захищається.




а) б)

Рисунок 2 – Зображення-контейнер (а) і приховане (б) в ньому зображення

Проведені дослідження показали, що при приховуванні рентгенівських знімків в контейнерах того ж типу кількість молодших біт, що використовуються для приховування в кожному пікселі зображення-контейнера може бути збільшена до 4 по кожній складовій кольору, відмінності від оригінального зображення-контейнера непомітні, середньо-квадратичне відхилення (СКВ) від оригінального складає 4-6 (рис. 2).

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Безпека та конфіденційність у віддаленій радіології. [Електронний ресурс]. https://radiolance.ua/bezpeka-ta-konfidentsijnist-u-viddalenij-radiologiyi/

[2] Олександр Романюк, Володимир Майданюк, Сергій Павлов, Наталія Тітова , Сергій Романюк. Шифрування медичних зображень // Медико-технічна співпраця заради перемоги: Актуальні завдання медичної, біологічної фізики та інформатики. Матеріали доповідей та виступів III всеукраїнської науково-практичної конференції з міжнародною участю 5-6 квітня 2024 року Вінниця. – Вінниця: Едельвейс. – С. 86-89.

[3] Майданюк, В. П. Основи теорії інформації та кодування : електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Майданюк В. П., Романюк О. Н., Тужанський С. Є. – Вінниця : ВНТУ, 2022. – 133 с.