ГРИЦИШИН В. О.,
МАЙДАНЮК В. П.,
Вінницький національний технічний університет

ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ ДЛЯ ЗАХИСТУ РЕНТГЕНІВСЬКИХ ЗНІМКІВ

Анотація: Розглянуто особливості захисту рентгенівських 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.

Ключові слова: криптографія, стеганографія, зображення.

Abstract: The peculiarities of protecting X-ray images from unauthorized access due to the use of cryptographic and steganographic methods are considered. It is shown that when hiding X-ray images in containers of this type, the number of least significant bits used for hiding in each pixel of the container image can be increased to 4 for each color component.

Keywords: cryptography, steganography, image.

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. 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. Однак, приховування в частотній області вимагає значно більше обчислень, що є неприйнятним для застосувань, де вимагається середній ступінь захисту [1-2].

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 і 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:

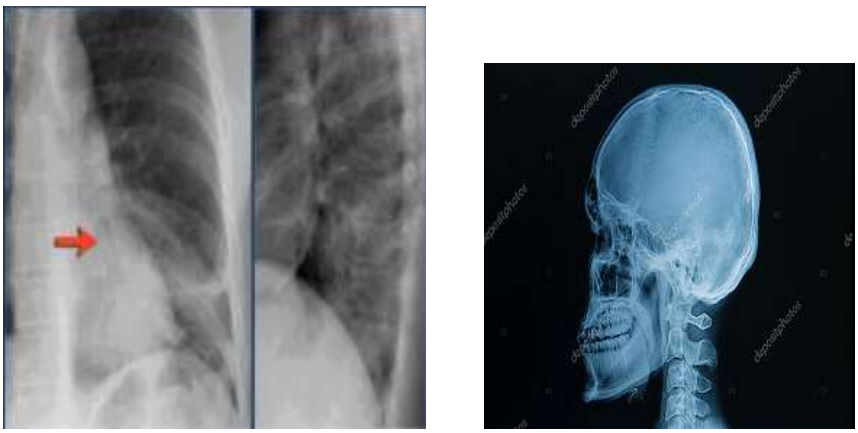
1. Розсіювання бітів зображення, що захищається в площині зображення контейнера з використанням конгруентного генератора псевдовипадкових чисел (ПВЧ) та їх гамування. Для кожної складової кольору (RGB) використовується свій генератор ПВЧ. Він формує послідовності псевдовипадкових чисел T(i) у відповідності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

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

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.
4.

ГУБІНА С.І.,
Вінницьккий державний педагогічний університет
імені Михайла Коцюбинського

ФОРМУВАННЯ ЕМОЦІЙНОГО ІНТЕЛЕКТУ МАЙБУТНІХ УЧИТЕЛІВ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Анотація. У статті аналізуються структура емоційного інтелекту, особливості формування емоційного інтелекту майбутніх учителів в умовах дистанційного навчання. На прикладі використання програми Kahoot!, яка надає можливість вчителям самостійно та професійно створювати навчальні ігри, заохочуючи і мотивуючи учнів до командної співпраці, досягнення своїх навчальних цілей, підвищення рівня цифрової грамотності, зацікавленості в освоєнні наданого матеріалу та його спільному обговоренні показано формування емоційного інтелекту, оскільки ігрові методики завжди мають сильний вплив на емоційну сферу всіх учасників освітнього процесу.

Ключові слова: емоційний інтелект, емоційна сфера, майбутні учитпелі, формування, дистанційне навчання, програма Kahoot!, навчальні ігри, ігрові методики, цифрова грамотність.

Актуальність статті. Сучасні реалії висувають нові вимоги до системи підготовки майбутніх педагогів. які мають зробити країну конкурентоспроможною, вивести її на більш високий соціально-економічний рівень. Наразі суспільство потребує компетентних фахівців у галузі освіти, які вирізняються емоційною стабільністю.