

ВИРІШЕННЯ ПРОБЛЕМИ ЗАХИСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ.

Іванішина Д.О.

Науковий керівник – доц., к.т.н. Яремчук Ю. Є.

У зв'язку з широким розповсюдженням мережових технологій велика кількість зображення та відео з приватною та діловою інформацією поширюється у мережі. На сьогодні інформаційна безпека цифрового зображення важлива у багатьох областях, таких як відеосервіс за запитом, відеоконференції, безпека зв'язку, захист інтелектуальної власності та авторського права. Скремблювання зображення – хороший спосіб захистити зображення шляхом його перетворення у незрозумілу засекречену форму для неавторизованих користувачів.

Відомі на сьогодні методи скремблювання цифрових зображень мають ряд недоліків: процес кодування і декодування складний, що призводить до дуже високих обчислювальних витрат; результат скремблювання не дуже ефективний, оскільки інформація даного зображення перерозподілена за певною закономірністю по зображенню, яку можна передбачити і, таким чином, дізнатися істинну форму або значення цього зображення, методи не забезпечують достатнього рівня стійкості при атаках на зображення, як ущільнення, шум і втрата пакетів даних.

Результати аналізу показали, що методи скремблювання зображення на основі Р-чисел Фібоначчі усувають дані недоліки. Зокрема, метод скремблювання цифрового зображення у просторовій області змінює позиції пікселів шляхом використання 2-D Р-Фібоначчі перетворення. Метод, який працює у частотній області (включаючи формат JPEG): порушує знаки коефіцієнтів ДКП, використовуючи 2-D Р-Фібоначчі перетворення. Відмінною рисою методів є використання захисних ключів, які доступні тільки для авторизованих користувачів. У якості ключа слугує параметр p , який має безліч можливих варіантів, що гарантує високу захищеність зашифрованого зображення.

Скремблювання цифрового зображення на основі Р-чисел Фібоначчі реалізуються для чорно-білого і кольорового зображення. Методи мають хороші показники в поширених атаках на зображення таких як втрата даних, ущільнення, шум.

Дані методи можуть бути застосовані для повного і часткового шифрування зображення, шифрування аудіо сигналу, телевізійного відео сигналу шляхом скремблювання кожного рядка або кадру відео передачі; для кодування ущільненого бітового потоку, а також шифрування ключів.