УДК 004.056.5

# АЛГОРИТМ ШИФРУВАННЯ ЗОБРАЖЕНЬ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ З ВИКОРИСТАННЯМ ДВОКАНАЛЬНОЇ ПЕРЕДАЧІ КЛЮЧІВ

**Віта Каштан**
*Національний технічний університет «Дніпровська політехніка», kashtan.v.yu@nmu.one*

Зображення дистанційного зондування Землі (ДЗЗ) можуть містити військову таємницю, профілі території та інші конфіденційні дані, які забезпечують надійну технічну гарантію сталого розвитку національної економіки кожної країни. Використання зображень ДЗЗ пов'язане з ризиком втрати, крадіжки та перехоплення, особливо якщо зображення зберігаються в хмарному середовищі або передаються через загальнодоступні канали. Тому, шифрування зображень є важливим технічним засобом для запобігання витоку конфіденційної інформації.

Останнім часом розроблено багато ефективних алгоритмів для захисту даних від несанкціонованого доступу, але забезпечення якісного та швидкого шифрування залишається актуальним питанням. Хаотичні системи стали типовим методом шифрування зображень, так як мають складну структуру та високу чутливість до параметрів початкових значень. Передові технології шифрування, які базуються на хаотичній системі, включають такі методи, як кодування DNA, заміну S-box, зигзагоподібне скремблювання, схему підйому, математичні моделі та компресійне зондування. Всі вищевказані алгоритми використовують однакову операцію для шифрування кожного каналу (багатоканального) зображення. Це означає, що коли зловмисник зламує зображення у градаціях сірого (панхромне зображення), то всі інші частини зображення можуть бути легко перехоплені.

*Метою даної роботи* є розробка алгоритму шифрування зображень дистанційного зондування Землі з використанням двоканальної передачі ключів.

Модель двоканальної передачі ключів (Dual-Channel Key Transmission Model) – це метод передачі ключа шифрування, який використовує два незалежні канали передачі для підвищення надійності та безпеки передачі даних. Структурна схема алгоритму шифрування представлена на рисунку 1. Запропонована модель використовує два незалежних канали: головний канал і канал підтвердження. Головний канал використовується для передачі основного потоку даних на основі симетричного ключа, тоді як канал підтвердження використовує прихований ключ на рівні бітів (це дозволяє додати ключ у зашифроване зображення). Процес передачі ключа в моделі Dual-Channel Key Transmission складається з наступних етапів: 1) Ключ генерується відправником та поділяється на дві частини. Одна частина передається по головному каналу, а інша – по каналу підтвердження. 2) Одержувач отримує дві частини ключа та перевіряє їх цілісність. 3) Якщо ключі виявляються неповними або пошкодженими, вони не обробляються та процес передачі повторюється. Якщо обидві частини ключа були успішно отримані, вони об'єднуються для створення повного ключа шифрування.

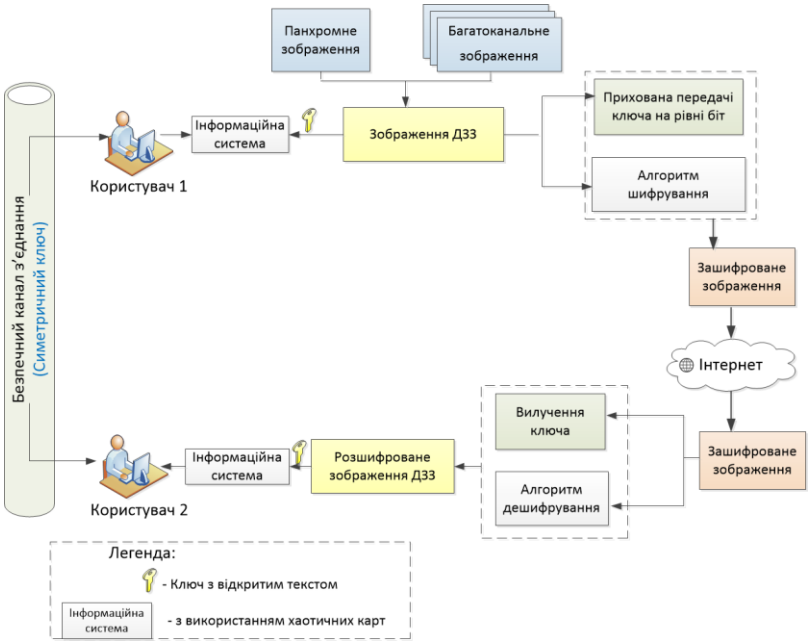


Рис.1. Схема шифрування ДЗЗ зображень

Коли дешифратор отримує зображення з прихованим ключем на рівні біт, він спочатку використовує хаотичну послідовність потоку ключів, щоб визначити приховане положення ключа. Після цього піксельне значення зображення перетворюється на 8-розрядні двійкові числа, останні біти об'єднуються для отримання 32-розрядної двійкової послідовності. Для розшифрування ключа використовується операція XOR порозрядно. Таким чином, два типи ключів взаємодіють у хаотичній системі як ключі шифрування, що ускладнює зловмиснику правильно відновити (дешифрувати) оригінальне зображення, навіть якщо він перехопить один з ключів.

Запропонований в роботі алгоритм шифрування зображень дистанційного зондування Землі з використанням двоканальної передачі ключів через загальнодоступні канали зв'язку, наприклад через Інтернет, пошту або інші канали дозволяє захистити дані від несанкціонованого доступу. Такий підхід дозволяє підвищити безпеку передачі багатоканальних (багатоспектральних) зображення дистанційного зондування Землі через супутникові або військові канали зв'язку.