ВИКОРИСТАННЯ БІТОВИХ ОПЕРАЦІЙ В МОДИФІКАЦІЇ АЛГОРИТМУ RSA ДЛЯ ШИФРУВАННЯ І ДЕШИФРУВАННЯ КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Навитка М. Л.
Національний університет "Львівська політехніка"

Однією з найбільш використовуваних форм представлення інформації в цифровому вигляді є зображення. Через це - актуальним завданням є захист зображень від несанкційованого доступу та використання. Проблема несанкційованого використання зображень з однієї сторони вирішена положення «Закону про авторське право», а з другої – методами криптографії та стенографії, друкованих сіток та іншими.

Головною підставою для захисту зображення є наступне припущення: зображення – це стохастичний сигнал. Це зумовлює використання класичних методів шифрування сигналів у випадку зображень. Але зображення – це специфічна інформація у вигляді візуального контенту, що вносить нові проблеми по забезпеченню конфіденційності і дає додаткові можливості несанкціонованого доступу. Фактично організація хакерських атак на зашифровані зображення є двох типів: класичний злом за допомогою методів шифрування і з використанням методів візуальної обробки зображень (злом може бути здійснений за лічені години чи хвилини, а часом і режимі реального часу).

Що стосується методів шифрування , в разі їх застосування до зображення, перед ними ставиться ще одна задача - повне шифрування шумів зображення. Це необхідно для запобігання використання візуальних методів відтворення зображень. RSA-алгоритм є одним з найбільш використовуваних стандартів для шифрування. Але по відношенню до зображення існують деякі проблеми з його використанням, наприклад, така як - часткове збереження контурів, присутніх у зображенні.

ОСОБЛИВОСТІ ЗОБРАЖЕННЯ

Маємо зображення P з шириною l і висотою h. Воно може бути представлене у вигляді матриці пікселів

$$<dtpij>1\le i\le n,\ 1\le j\le m, \qquad (1)$$

де dtpij – піксель з координатами (i ,j), n і m - кількість пікселів по ширині і висоті

Матриця (1) у відношенні до матриці інтенсивності кольорових пікселів має вигляд

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix} \qquad (2)$$

де c_{ij} – значення інтенсивності пікселів зображення dtp_{ij} , $1\le i \le n$, $1\le j \le m$ [1].

Модифікований алгоритм RSA

Нехай P,Q - *пара випадкових простих чисел,* тоді

$$N = PQ,\ (N) = (P-1)(Q-1).$$

Натуральному числу d, ставиться у відповідність представлення

$$ed \equiv 1 (\mathrm{mod}\ (N)).$$

де $e < (N)$ - довільно вибране додатне ціле число

Шифрування здійснюється поелементно для кожного рядка за допомогою перетворення елементів зображення матриці С.

АЛГОРИТМ ШИФРУВАННЯ

- Якщо $j \bmod 2 \ 0$, тоді число представляється як:

$jj = \text{random}(j + P) \bmod 31 + 1,$

$a_{i,j} \ jj^e \bmod N, \quad X = j \ a_{i,j} \ P.$

- Якщо $j \bmod 2 \ 1$, тоді число представляється так:

$jj = \text{random}(j + Q) \bmod 31 + 1,$

$a_{i,j} \ jj^d \bmod N, \quad X = j \ a_{i,j} \ Q.$

Будуємо число $K = c_{i,j} \wedge X$.

Зашифроване число отримується за циклічною зміною числа K 31 – jj біта.

Результатом є матриця зашифрованих значень інтенсивності пікселів введеної матриці і матриці ключів.

АЛГОРИТМ ДЕШИФРУВАННЯ

- Якщо $j \bmod 2 \ 0$, то число представляється:

$jj = \text{random}(j + P) \bmod 31 + 1,$

$a_{i,j} \ jj^d \bmod N, \quad X = j \ a_{i,j} \ P.$

- Якщо $j \bmod 2 \ 1$, то число сконструйоване:

$jj = \text{random}(j + Q) \bmod 31 + 1,$

$a_{i,j} \ jj^e \bmod N, \quad X = j \ a_{i,j} \ Q.$

Представлення циклічного введення числа 31 – jj бітового.

Результатом є матриця пікселів зашифрованих значень інтенсивності, (^ - “OR” оператор).

Приклад

Рис.1 Вхідне зображення.

Рис.2 Дешифроване зображення

Рис.3 Зашифроване зображення

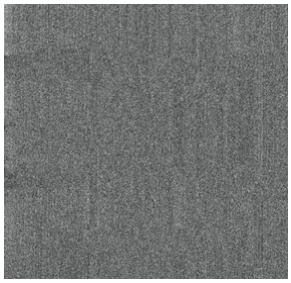
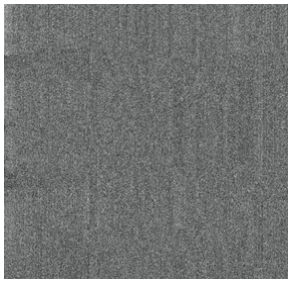


Рис.4 Ключі матриці



Запропоновані модифікації повністю відповідають стійкості до дешифрування алгоритму RSA і забезпечують, при правильному підборі ключа, практично повну зашумленість зашифрованого зображення, що унеможливлює отримання з нього будь-якої інформації без дешифрування.

1. Б.Шнайдер. Прикладная криптография.– М.: Издательство Триумф, 2003.-816с. 2. Юрій Рашкевич, Анатолій Ковальчук , Дмитро Пелешко. Проективні відображення першого порядку в шифруванні і дешифруванні зображень з елементами алгоритму RSA. – Львів: Технічні вісті 2009/№1(29), 2(30). С. 41 – 44.