**УДК 01.05.02; 05.13.06; 05.13.21**

**А. Ковальчук, Д. Пелешко, *Ю. Борзов**
Національний університет “Львівська політехніка”**,**
кафедра ІТВС,
*Львівський державний університет безпеки життєдіяльності,

# ВИКОРИСТАННЯ ПОБІТОВИХ ОПЕРАЦІЙ І ДОДАТКОВОГО ЗАШУМЛЕННЯ В АЛГОРИТМІ RSA ПРИ ШИФРУВАННІ–ДЕШИФРУВАННІ ЗОБРАЖЕНЬ



## Вступ

Алгоритм RSA є одним із найуживаніших промислових стандартів шифрування сигналів. Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [4, 5].

Проблема несанкціонованого використання зображень на найнижчому рівні вирішується положеннями про авторське право, а на найвищому – методами криптографії і стеганографії, поліграфічними сітками тощо.

Оскільки зображення є одними із найвживаніших видів інформації в сучасному інформаційному суспільстві, то актуальним завданням є захист зображень від несанкціонованого доступу та використання.

Зображення є сигналом, який володіє не лише типовою інформативністю даних, а й візуальною інформативністю. А остання привносить в питання захисту нові задачі.

Така інформативність з розвинутими сучасними методами обробки зображень дає можливість для організації несанкціонованого доступу. Фактично організація атаки на зашифроване зображення можлива у двох варіантах: традиційним зламом методів шифрування або за допомогою методів візуальної обробки зображень (методи фільтрації, виділення контурів тощо). У зв’язку з цим до методів шифрування у випадку їх використання стосовно зображень висувається ще одне завдання – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуальної обробки зображень.

## Мета роботи

Стосовно зображень актуальною задачею є розроблення модифікації методу RSA для забезпечення повної зашумленості зображення з метою унеможливлення використання методів візуальної обробки зображень і збереження криптографічної стійкості.

Одним із шляхів розв’язання цієї задачі є використання побітових операцій в алгоритмі RSA з додатковим зашумленням в програмній реалізації .

## Характеристики зображення

Цифрове зображення – масив даних, отриманий шляхом дискретизації (аналого-цифрового перетворення) оригіналу. Будучи закодованим за допомогою особливого алгоритму і записаним на носій, цей масив даних стає файлом.

У сучасному процесі поліграфічного виробництва всі ілюстрації й елементи оформлення представлені цифровими зображеннями різних типів. Цифрові зображення за способом дискретизації оригіналу поділяються на растрові, векторні та змішаного типу.

До растрових зображень належать двовимірні масиви даних (матриці пікселів), кожен елемент яких представляє ділянку оригіналу з усередненим колірним показником.

Найменшими елементами векторного зображення є вектор і крива Безьє. Вектор у комп'ютерній графіці – це відрізок, що з'єднує дві точки з заданими координатами. Основним керівним елементом кривої Безьє є вузол (node), також званий контрольною точкою (CP, control point) або контрольної вершиною (CV, control vertex). Ступінь кривизни лінії визначається координатами вузла і двох керівних точок.

Цифрові зображення змішаного типу являють собою масиви даних, що містять інформацію як у вигляді матриці пікселів, так і у вигляді опису векторів, кривих Безьє, примітивів і текстових блоків.

Нехай задано рисунок $\boldsymbol{P}$ з ширини $l$ і висоти $h$. Його можна розглядати як матрицю інтенсивностей пікселів

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

розмірності

$$n = n(l) \text{ і } m = m(h), \quad (2)$$

де $c_{ij}$ – значення інтенсивності у напівтонових зображень пікселя $dtp_{ij}$. Тобто існує відповідність [1]

$$P = \mathbf{P}_{l,h} = \left[ pxl_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)} \rightarrow \mathbf{C}=\left[ c_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)}. \quad (3)$$

Під градацію яскравості зазвичай надається 1 байт, причому 0 – чорний колір, а 255 – білий (максимальна інтенсивність).

Важливою характеристикою зображення є наявність у зображенні контурів [1]. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і затемнюють області постійних рівнів яскравості, тобто контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [2].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виокремлення контуру означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин того, що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут ґрунтується на піднесенні до степеня за модулем деякого натурального числа. При цьому на контурі і на сусідніх до контуру пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

## Опис модифікації

**Шифрування і дешифрування за одним рядком матриці зображення**

Нехай $\boldsymbol{P}$, $\boldsymbol{Q}$ – пара довільних простих чисел і $\boldsymbol{N = P * Q}$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення $\boldsymbol{C}$:

1. Випадково вибирається натуральне число $\boldsymbol{e < \varphi(N)}$ і знаходиться таке натуральне $\boldsymbol{d}$, що виконується конгруенція $\boldsymbol{ed \equiv 1 (\mathrm{mod}\ \varphi(N))}$.
2. Будується число $\boldsymbol{A = (e << k) + (d << l) + (e << l) + (d << k)}$ , де $\boldsymbol{k < 16}$ , $\boldsymbol{l < 16}$ – натуральні числа, $\boldsymbol{k \neq l}$, **<< –** операція логічного зсуву ліворуч**.**
3. У кожному рядку виконується логічний зсув ліворуч значення інтенсивності $\boldsymbol{i}$-го пікселя, $\boldsymbol{i = 1, 2, \dots , m}$, $\boldsymbol{m}$ –число елементів у рядку за таким правилом: виконується логічний зсув ліворуч значення інтенсивності пікселя на величину $\boldsymbol{i \bmod n}$ , $\boldsymbol{n < 16}$.
4. Будується число $\boldsymbol{B}$ відніманням від отриманого значення інтенсивності пікселя числа $\boldsymbol{(A + e)}$.
5. Зашифрованим значенням інтенсивності $\boldsymbol{i}$-го пікселя, $\boldsymbol{i = 1, 2, \dots , m}$, $\boldsymbol{m}$ –число елементів у рядку, вибирається число $\boldsymbol{C \equiv B^e \ (\mathrm{mod}\ N) + f(i^2)}$ .

Дешифрування проводиться в порядку, протилежному до шифрування після отримання числа $\boldsymbol{(C - f(i^2))^d \equiv (B^e)^d \ (\mathrm{mod}\ N)}$, виконанням протилежних до змісту пунктів 4, 1 операцій.

Результати наведені на рис. 1–3.

*Рис. 1. Початкове зображення*

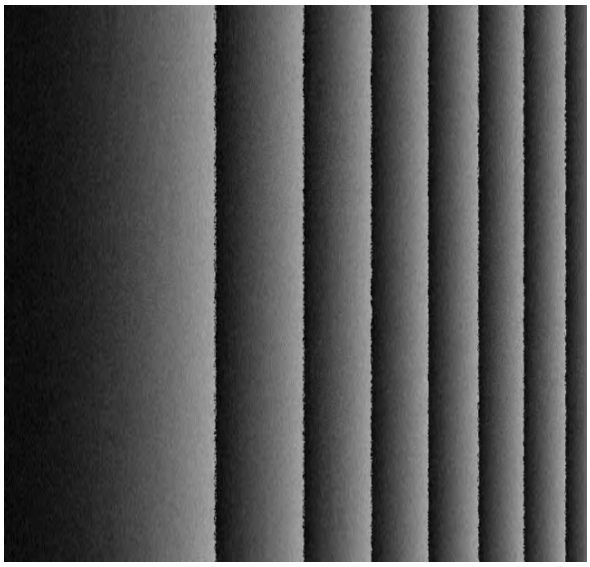

*Рис. 2. Зашифроване зображення*

*Рис. 3. Дешифроване зображення*

**Шифрування за двома рядками матриці**

Шифрування відбувається з використанням елементів двох рядків за алгоритмом, який описано вище, для шифрування елементів одного рядка інтенсивнстей, за винятком п.5, причому кожний рядок з вибраних двох рядків шифрується незалежно за своїм алгоритмом, для нього модифікованим п.5.

Пункт 5 має вигляд:

5.1. Для першого рядка зашифрованим значенням інтенсивності ***i***-го піксела, $i = 1, 2, \dots, m$, $m$ – число елементів у рядку, вибирається число $C \equiv B^e \pmod N + g(i^2)$.

5.2. Для другого рядка зашифрованим значенням інтенсивності ***i***-го піксела, $i = 1, 2, \dots, m$, $m$ – число елементів у рядку, вибирається число $C \equiv B^e \pmod N - g(i^2)$.

Дешифрування відбувається в протилежному порядку з урахуванням п.п. 5.1, 5.2.

Результати наведено на рис. 4–6.

*Рис. 4. Початкове зображення*

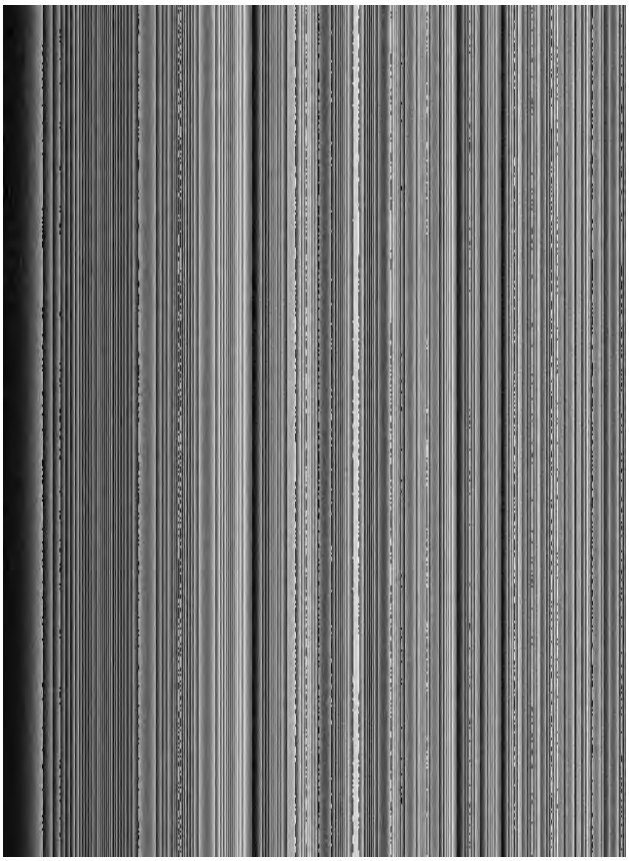

*Рис. 5. Зашифроване зображення*

*Рис. 6. Дешифроване зображення*

Порівнюючи рис. 2 і 5, бачимо, що шифрування за одним рядком матриці (3) істотно не відрізняється від шифрування за двома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Початкові і дешифровані зображення тільки незначно відрізняються за рівнем яскравості

**Висновки**

1. Запропоновані модифікації шифрування призначені для шифрування зображень в градаціях сірого і грунтуються на використанні ідей базового алгоритму RSA.

2. Запропоновані модифікації можна використовувати стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дають змогу чітко виділяти контури.

3. Обидва типи модифікацій без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зрости розмір шифрованого зображення.

4. Стійкість до несанкціонованого дешифрування запропонованою потоковою модифікацією забезпечує алгоритм RSA.

*1. Никулин Е.А. Компьютерная геометрия и алгоритмы машинной графики. – СПб.: БХВ-Петербург, 2005. – 560 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 4. Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З. Модифікація алгоритму RSA для деяких класів зображень // Технічні вісті. – 2008/1(27). – 2(28). – С. 59–62. 5. Rashkevych Y., Kovalchuk A., Peleshko D., Kupchak M. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction // Proceedings of the X-th International Conference CADSM 2009. 24–28 February 2009, Lviv–Polyana, Ukraine. – P. 469–473.*