*УДК 01.05.02:05.13.[06+21]*
*Ст. викл. Ю.О. Борзов[1]; доц. А.М. Ковальчук[2]; доц. Д.Д. Пелешко[2], д-р техн. наук*

# МОДИФІКАЦІЯ АЛГОРИТМУ RSA: ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ЗА ОДНИМ РЯДКОМ МАТРИЦІ ЗОБРАЖЕННЯ

Запропоновано модифікації, які може бути використано стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дають змогу чітко виділяти контури.

***Ключові слова:*** матриця зображення шифрування, операція, стійкість дешифрування.

**Вступ**. Зображення є одними із найбільш вживаних видів інформації в сучасному інформаційному суспільстві. Відповідно, актуальним завданням є захист зображень від несанкціонованого доступу та використання. Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Але зображення є специфічним сигналом, який володіє, окрім типової інформативності (інформативності даних), ще й візуальною інформативністю.

Така інформативність з використанням сучасних методів оброблення зображень дає змогу для організації несанкціонованого доступу. Реалізація атаки на зашифроване зображення можлива у двох варіантах: через традиційний злом методів шифрування, або через методи візуального оброблення зображень (методи фільтрації, виділення контурів тощо). З огляду на це, шифрування у випадку їх використання стосовно зображень висувається ще одну вимогу – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів попереднього візуального оброблення зображень.

Алгоритм RSA є одним із найбільш уживаних промислових стандартів шифрування сигналів. Щодо зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [4, 5]. Зазначимо, що існує два підходи до побудови практично стійких шифрів. У першому випадку будують криптосистему, і потім показують, що її розкол є складним завданням. У другому випадку вибирається певна складна математична задача, і потім будується відповідна криптосистема, розкол якої еквівалентний її рішенню.

Теоретичну стійкість визначають за умови, що не існує тимчасових обмежень на несанкціоноване дешифрування, і, отже, це є відповіддю на питання, що криптосистема не може бути розколена в принципі. Їх можна побудувати за допомогою випадкового рівноймовірного ключа шифрування, довжина якого не менша ніж довжина відкритого тексту. Зовсім стійкі системи надзвичайно дорогі в реалізації. Тому на практиці використовують системи, які можна розколоти, але за неприйнятний час.

**Мета роботи**. Стосовно зображень актуальним завданням є розроблення такої модифікації алгоритму RSA, щоб: зберегти криптографічну стійкість; забезпечити повну зашумленість зображення. Одним із шляхів вирішення цієї задачі є поєднання властивостей алгоритму RSA з використанням деяких випадково вибраних натуральних чисел у програмній реалізації.

[1] Львівський ДУ безпеки життєдіяльності;
[2] НУ "Львівська політехніка"

**Характеристики зображення**. Нехай задано рисунок ***P*** з ширини $l$ і висоти $h$. Його можна розглядати як матрицю пікселів

$$<dtp_{ij}>_{1\le i\le n,\ 1\le j\le m}, \tag{1}$$

де: $dtp_{ij}$ – піксел з координатами $i$ та $j$, $n$ і $m$ – число точок по ширині $l$ та висоті. У загальному випадку $n$ і $m$ є залежними від $l$ та $h$, а тому більш коректним є запис

$$n = n(l) \text{ і } m = m(h). \tag{2}$$

Матриці (1) у відповідність ставиться матриця інтенсивностей пікселів

$$C=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \tag{3}$$

де $c_{ij}$ – значення інтенсивності у напівтонових зображень піксела $dtp_{ij}$. Тобто має місце відповідність **[1]**

$$P = \mathrm{P}_{l,h} = \left[ pxl_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)} \to C=\left[ c_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)}. \tag{4}$$

Для градації яскравості звичайно беруть 1 байт, причому 0 – чорний колір, а 255 – білий (максимальна інтенсивність). Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура потребує використання операцій над сусідніми елементами, які є чутливими до змін і пригашають 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 у площині зображення. Тому виділення контура означає пошук найбільш разючих змін, тобто максимумів модуля вектора градієнта **[2]**. Це є однією з причин, через що контури залишаються в зображенні під час шифрування в системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю певного натурального числа. При цьому, на контурі і на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

**Опис модифікацій алгоритму RSA**

**Шифрування і дешифрування по одному рядку матриці зображення.** Нехай $P$, $Q$ – пара довільних простих чисел і $N = P\cdot Q$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення $C$:

1. Випадково вибирають натуральне число $e < \varphi(N)$ і знаходять таке натуральне $d$, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. Будують число $A = c_{ij} + Q + P + i + j - d$.
3. Зашифрованим значенням інтенсивності $i$-го піксела, $i$ = 1, 2, …, $m$, $m$ – кількість елементів у рядку, вибирають число $B \equiv A^{\mathrm{e}} (\mathrm{mod}\ N)$.

Дешифрування проводять в порядку, протилежному до шифрування після отримання числа $B^{\mathrm{d}} \equiv (A^{\mathrm{e}})^{\mathrm{d}} (\mathrm{mod}\ N)$, виконанням протилежних операції до змісту пунктів 3), 2), 1). Результати наведено на рис. 1.

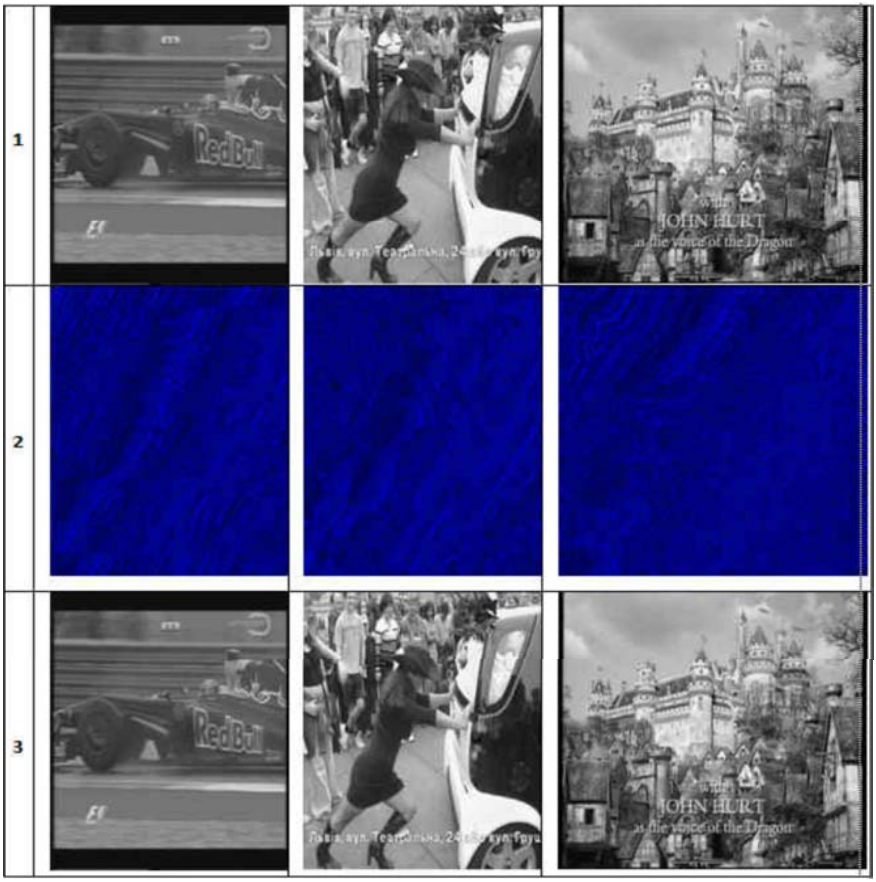


***Рис. 1. 1) початкові зображення; 2) зашифровані зображення; 3) дешифровані зображення***

**Шифрування і дешифрування по одному рядку матриці з додатковим зашумленням**

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

1. Випадково вибирають натуральне число $e < \varphi(N)$ і знаходять таке натуральне $d$, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. Будують число $A = c_{ij} + Q + P + i + j - d$.
3. Зашифрованим значенням інтенсивності $i$-го піксела, $i = 1, 2, \ldots, m$, $m$ – кількість елементів у рядку, вибирають число $C \equiv A^{\mathrm{e}} (\mathrm{mod}\ N) + f(i, j)$.

Дешифрування проводять в порядку, протилежному до шифрування після отримання числа $(C - f(i,j))^{\mathrm{d}} \equiv (A^{\mathrm{e}})^{\mathrm{d}} (\mathrm{mod}\ N)$, виконанням протилежних операції до змісту пунктів 3), 2), 1). Результати наведено на рис. 2. Для шифрування вибирали такі функції: $f(i,j) = i^2, f(i,j) = i \cdot j, f(i,j) = j^2$.

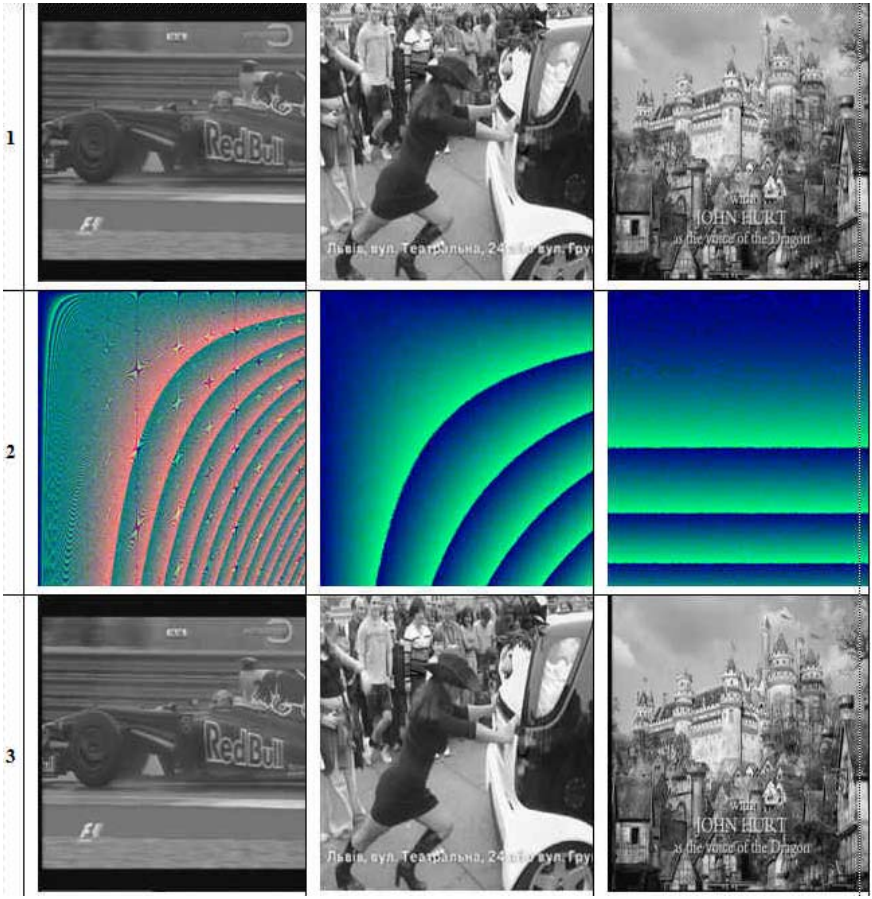


***Рис. 2. 1) початкові зображення; 2) зашифровані зображення; 3) дешифровані зображення***

З порівняння рис. 1, 2) і рис. 2, 2) видно, що шифрування з додатковим зашумленням відрізняється від шифрування без додаткового зашумлення. Контури в обох зашифрованих зображеннях відсутні. Початкові і дешифровані зображення тільки незначно відрізняються рівнем яскравості. Функції додаткової зашумленості $f(i, j)$ можуть бути довільними цілозначними функціями і додатково, до створюваної алгоритмом RSA зашумленості, підвищують криптографічну стійкість вказаних модифікацій.

**Висновки**:

1. Запропоновані модифікації шифрування призначені для шифрування зображень в градаціях сірого кольору і ґрунтуються на використанні ідей базового алгоритму RSA.
2. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги досягаються 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 величина шифрованого зображення.
4. Стійкість до несанкціонованого дешифрування, запропонованими потоковою модифікацією, забезпечується алгоритмом RSA.
5. Модифіковані методи шифрування побудовані так, що за малих значень ключа також можна досягти якісного шифрування, але за умови вірного підбору параметрів шифрування. При цьому досягається висока швидкість роботи алгоритму.
6. Реалізація стійкості модифікованих криптографічних алгоритмів з одночасним забезпеченням якості зображення не потребує значних обчислювальних ресурсів.

## Література

1. Павлидис Т. Алгоритмы машиной графики и обработки изображений / Т. Павлидис. – М. : Изд-во "Радио и связь", 1986. – 399 с.

2. Яне Б. Цифровая обработка изображений / Б. Яне. – М. : Изд-во "Техносфера", 2007. – 583 с.

3. Шнайер Брюс. Прикладная криптография / Брюс Шнайер. – М. : Изд-во "Триумф", 2003. – 815 с.

4. Рашкевич Ю.М. Модифікація алгоритму RSA для деяких класів зображень / Ю.М. Рашкевич, Д.Д. Пелешко А.М. Ковальчук, М.З. Пелешко // Технічні вісті. – 2008. – Вип. 1(27), 2(28). – С. 59-62.

5. Ковальчук А. Поєднання алгоритму RSA і побітових операцій при шифруванні – дешифруванні зображень / А. Ковальчук, Д. Пелешко, М. Хомин, Ю. Борзов // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні науки та інформаційні технології. – Львів : Вид-во НУ "Львівська політехніка". – 2011. – № 694. – С. 309-313.

***Борзов Ю.О., Ковальчук А.М., Пелешко Д.Д.*** **Модификация алгоритма RSA: шифрование-дешифрование по одной строке матрицы изображения**

Предложены модификации, которые могут быть использованы относительно любого типа изображений, но наибольшие преимущества достигаются в случае использования изображений, которые позволяют четко выделять контуры.

***Ключевые слова:*** матрица изображения шифровки, операция, стойкость дешифрации.

***Borzov Yu.O., Koval'chuk A.M., Peleshko D.D.*** **Modification of algorithm of RSA: enciphering and decoding after one line of image matrix**

Modifications which it can be utillized in relation to any as images are offered, but most advantages are arrived at in the case of the use of images which enable expressly to select contours.

***Keywords:*** matrix image, encryption, operation, resistance decryption.

***УДК 339.92***

***Доц. И.В. Шкрабак, канд. гос. управления – Донецкий государственный университет управления***

# СТРУКТУРНАЯ УСТОЙЧИВОСТЬ ЭКОНОМИКИ РЕГИОНА С ПОЗИЦИЙ СИНЕРГЕТИЧЕСКОЙ ТЕОРИИ ИНФОРМАЦИИ

Рассмотрены теоретические вопросы анализа структурной устойчивости экономики на мезоуровне с позиций синергетической теории информации и направления их практического использования в государственном управлении экономическим развитием территорий.

***Ключевые слова:*** синергетическая теория информации, системно-конгломератные объекты, структурная устойчивость, хаос, порядок, экономическое развитие территории.