УДК 01.05.02; 05.13.06; 05.13.21

[1)]Ю.О. Борзов, [2)]А.М. Ковальчук, [2)]Д.Д. Пелешко,

[1)] Львівський Державний університет безпеки життєдіяльності

[2)]НУ «Львівська політехніка» **,**

кафедра інформаційних технолгій видавничої справи,

МОДИФІКАЦІЯ АЛГОРИТМУ RSA: ШИФРУВАННЯ-ДЕШИФРУВАННЯ ПО ОДНОМУ РЯДКУ МАТРИЦІ ЗОБРАЖЕННЯ

Запропоновано модифікації, які можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дозволяють чітко виділяти контури.

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

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.

MODIFICATION OF ALGORITHM RSA: ШИФРУВАННЯ-ДЕШИФРУВАННЯ ON ONE LINE OF MATRIX OF ZOBRAZHENNYA

A modification that can be used on any type of image, but the greatest benefits are achieved in the case of images that can clearly mark the contours.

Keywords: matrix image, encryption, operation, resistance decryption

Вступ

Зображення є одними із найбільш вживаних видів інформації в сучасному інформаційному суспільстві. Відповідно актуальною задачею 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, в додаток до типової інформативності (інформативності даних), ще й візуальною інформативністю

Така інформативність з використанням сучасних методів обробки зображень дає можливість для організації несанкціонованого доступу. Реалізація атаки на зашифроване зображення можлива у двох варіантах: через традиційний взлом методів шифрування, або через методи візуальної обробки зображень (методи фільтрації, виділення контурів, тощо). В 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 попередньої візуальної обробки зображень.

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

Слід зазначити, що існує два підходи до побудови практично стійких шифрів. У першому випадку будується криптосистема, і потім показується, що її розкол є складною задачею. У другому випадку вибирається деяка складна математична задача, і потім будується відповідна криптосистема, якої розкол еквівалентний рішенню цієї задачі.

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

Мета роботи

Стосовно зображень актуальною задачею є розробка 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 в програмній реалізації .

Характеристики зображення

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

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

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

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

Матриці (1) у відповідність ставиться матриця інтенсивностей пікселів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \qquad (3)$$

де c_{ij} – значення інтенсивності у напівтонових зображень піксела dtp_{ij}. Тобто

має місце відповідність [1]

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

Під градацію яскравості звичайно приділяється 1 байт, причому 0 - чорний колір, а 255 - білий (максимальна інтенсивність).

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура вимагає 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].

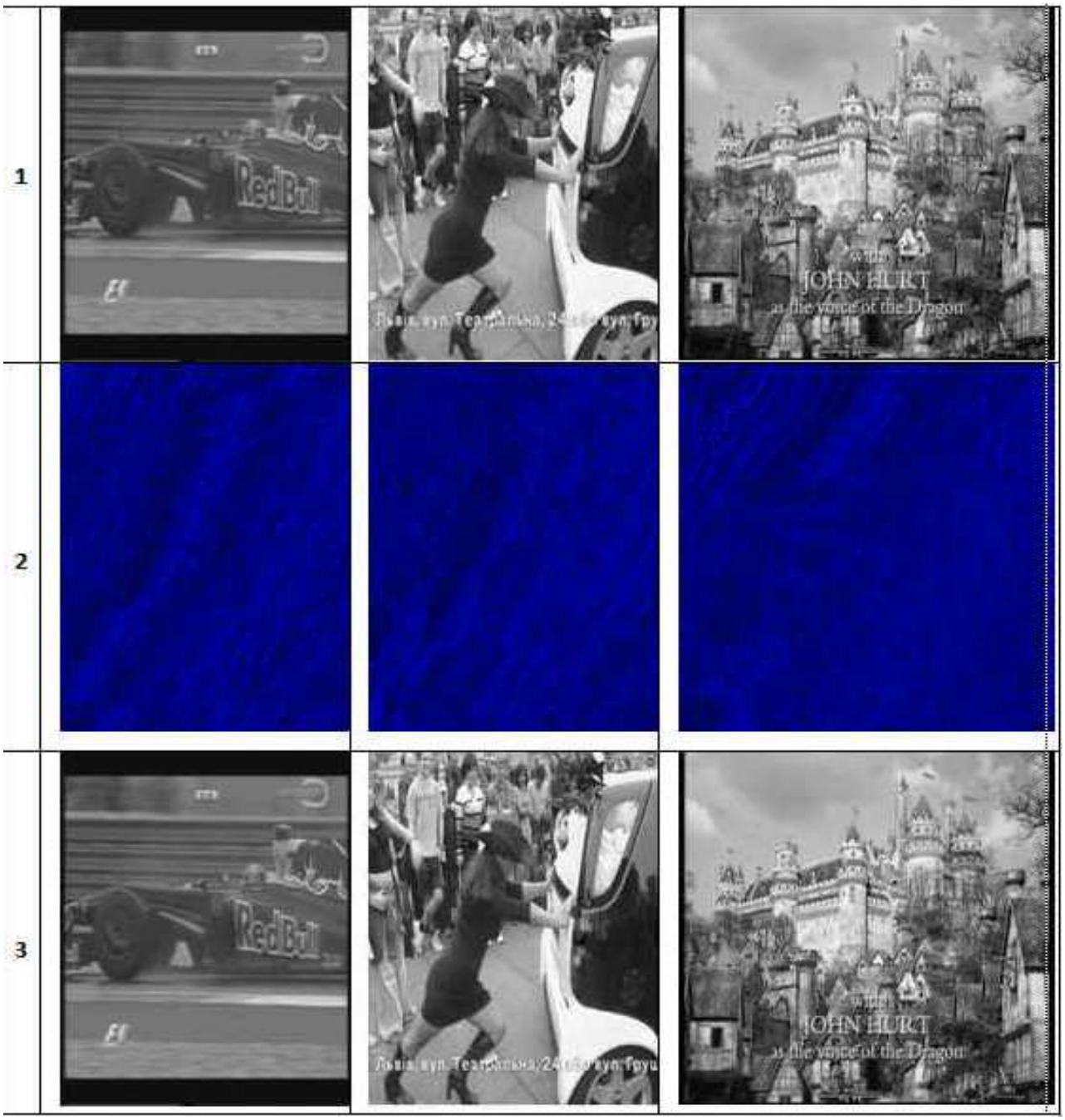

Рис. 1. 1) Початкові зображення 2) Зашифровані зображення 3) Дешифровані зображення

Математично – ідеальний контур це – розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук

найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю деякого 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 $N = P * Q$. Шифрування відбувається

поелементно з використанням наступного перетворення елементів матриці зображення C:

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

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

Результати наведені на рис.1.

Шифрування і дешифрування по одному рядку матриці з додатковим зашумленням

Нехай P, Q – пара довільних простих чисел і $N = P * Q$. Шифрування відбувається

поелементно з використанням наступного перетворення елементів матриці зображення C:

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. Будується число $A = c_{ij} + Q + P + i + j - d$.

Зашифрованим значенням інтенсивності i – ого піксела, $i = 1, 2, \ldots, m$, m – кількість елементів у рядку, вибирається число $C \equiv A^e \ (\mathrm{mod}\ N) + f(i, j)$.

Дешифрування проводиться в порядку, протилежному до шифрування після отримання числа $(C - f(i, j))^d \equiv (A^e)^d \ (\mathrm{mod}\ N)$, виконанням протилежних операції до змісту пунктів 3), 2), 1).

Результати наведені на рис.2. Для шифрування вибиралися такі функції : $f(i, j) = i^2$, $f(i, j) = i * j$, $f(i, j) = j^2$.

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 зашумлності ***f(i , j)*** можуть бути довільними цілозначними функціями і додатково, до створюваної алгоритмом RSA зашумленості, підвищують криптографічну стійкість вказаних модифікацій.

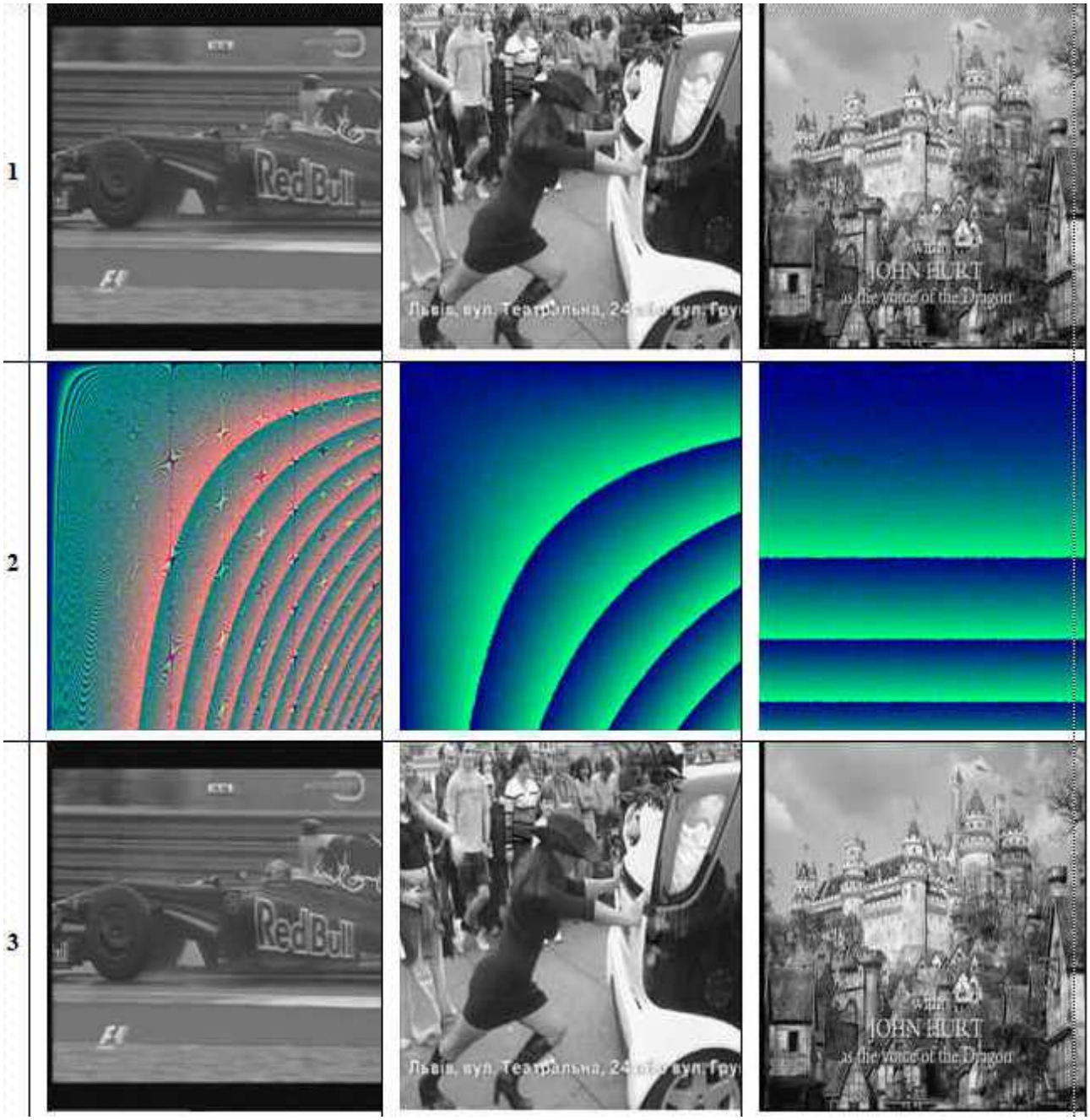

Рис. 2. 1) Початкові зображення 2) Зашифровані зображення 3) Дешифровані зображення

Висновки

1. Запропоновані модифікації шифрування призначені для шифрування зображень в градаціях сірого і грунтуються 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 дозволяють 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 запропонованими потоковою модифікацією забезпечується алгоритмом RSA.

5. Модифіковані методи шифрування побудовані так, що при малих значеннях 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 вимагають значних обчислювальних ресурсів.

Література

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

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

3. Брюс Шнайер. Прикладная криптография / Шнайер Брюс. – М. : 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 2008/1(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 НУ "Львівська політехніка". – Сер.: Комп'ютерні науки та інформаційні технології. – 2011. – № 694. – С. 309-313.