УДК 01.05.02; 05.13.06; 05.13.21

А. М. Ковальчук, К. С. Попадинець
Національний університет "Львівська політехніка" ,
кафедра інформаційних технологій видавничої справи

БІНАРНІ ПЕРЕТВОРЕННЯ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA У ЗАХИСТІ ЗОБРАЖЕНЬ ЗА ДОДАТКОВОГО ЗАШУМЛЕННЯ

Запропоновано елементи алгоритму RSA, який може бути використаний стосовно будь-якого зображення, але найбільші переваги досягаються у випадку використання зображень, що містять чітко виокремлені контури.

Ключові слова: матриця зображення, алгоритм, стійкість, шифрування–дешифрування.

Application of the elements of the algorithm RSA, which can be used in respect of any image, but the greatest benefits are achieved when using images containing clearly singled out the contours.

Key words: matrix image, algorithm, stability, encryption–decryption.

Вступ

Зображення є одними із найвживаніших видів інформації в сучасному інформаційному суспільстві. Відповідно актуальним завданням є захист зображень від несанкціонованого доступу та використання [1].

Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Але зображення є специфічним сигналом, який володіє, крім типової інформативності (інформативності даних), ще й візуальною інформативністю [2, 3].

Така інформативність з використанням сучасних методів обробки зображень уможливлює організацію несанкціонованого доступу. Реалізація атаки на зашифроване зображення можлива у двох варіантах: через традиційний злам методів шифрування або через методи візуальної обробки зображень (методи фільтрації, виділення контурів тощо). У зв'язку з цим у разі використання методів шифрування стосовно зображень ставиться ще одне завдання – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів попередньої візуальної обробки зображень.

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

Як відомо [6], теоретична стійкість визначається за умови, що не існує тимчасових обмежень на несанкціоноване дешифрування, і, отже, це є відповіддю на питання, чи криптосистема не може бути розколота в принципі. Їх можна побудувати за допомогою випадкового рівноймовірного ключа шифрування, довжина якого не менша від 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 актуальним завданням є розроблення такого використання алгоритму RSA, щоб:

- зберегти криптографічну стійкість, надану алгоритмом RSA;
- забезпечити повну зашумленість зображення.

Одним зі способів розв'язання цієї задачі є використання елементів алгоритму RSA в деяких афінних перетвореннях, зокрема, в бінарних лінійних перетвореннях.

Характеристики зображення

Нехай задано рисунок ***P*** 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* – кількість точок по ширині *l* та висоті [4, 5]. У загальному випадку *n* і *m* залежні від *l* та *h*, а тому коректнішим є запис

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

Матриці (1) у відповідність ставиться матриця інтенсивностей пікселів

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

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

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

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

Важливою характеристикою зображення є наявність у ньому 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, вони стають світлими, тоді як інші частини зображення залишаються темними [2].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виокремленняя контура означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2, 4]. Це є однією з причин, через яку контури залишаються в зображенні у разі шифрування у системі RSA, оскільки шифрування ґрунтується на піднесенні до степеня за модулем деякого натурального числа. На контурі й на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Опис використання елементів алгоритму RSA у бінарних перетвореннях

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 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 два числа $x = P*c_{ij} + Q*c_{ij+1} + f(P,Q)$, $y = e*c_{ij} + d*c_{ij+1} + f(P,Q)$, де $f(P,Q)$ – деяка функція додаткового зашумлення.

3. Зашифрованими значеннями інтенсивностей ***j***-го і ***j*** +1-го піксела в і-му рядку матриці, $j = 1, 2, \dots , m$, ***m*** – кількість елементів у рядку, вибирають числа $X = P*x + Q*y + g(j)$, $Y = e*x + d* y + g(j)$, де $g(j)$ – деяка функція додаткового зашумлення.

Дешифрування проводиться у послідовності, протилежній до шифрування, після отримання чисел ***X***, ***Y*** виконанням операцій, протилежних до змісту пунктів *3*, *2*.

Результати наведено на рис. 1.

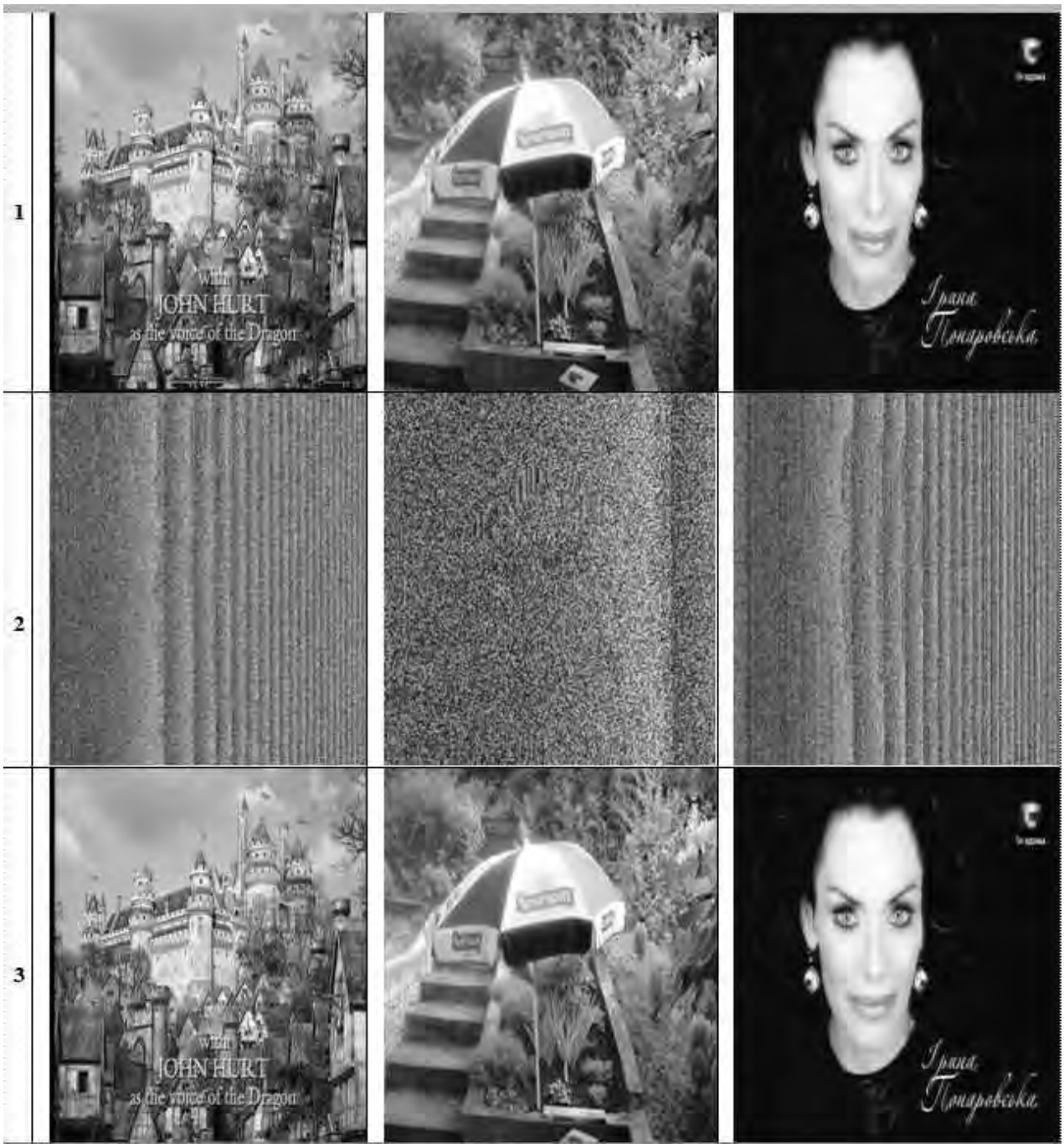

Рис. 1. Зображення: 1 – початкові; 2 – зашифровані; 3 – дешифровані

Шифрування і дешифрування за двома рядками матриці з додатковим зашумленням

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

4. Випадково вибирають натуральне число $e < \varphi(N)$ і знаходять таке натуральне d, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.

5. Будують два числа $x = P*c_{i,j} + Q*c_{i+1,j} + f(P,Q)$, $y = e* c_{i,j} + d* c_{i+1,j} + f(P,Q)$, де $f(P,Q)$ – деяка функція додаткового зашумлення.

6. Зашифрованими значеннями інтенсивностей j-го піксела, $j = 1, 2, \ldots, m$, m – кількість елементів у рядку і-го та i +1-го рядків матриці, вибирають числа $X = P*x + Q*y + h(i)$, $Y = e*x + d* y + h(i))$, де $h(i)$ – деяка функція додаткового зашумлення.

Дешифрування проводиться у послідовності, протилежній до шифрування, після отримання чисел ***X***, ***Y*** виконанням протилежних операцій до змісту пунктів *3*, *2*.

Результати наведено на рис. 2.

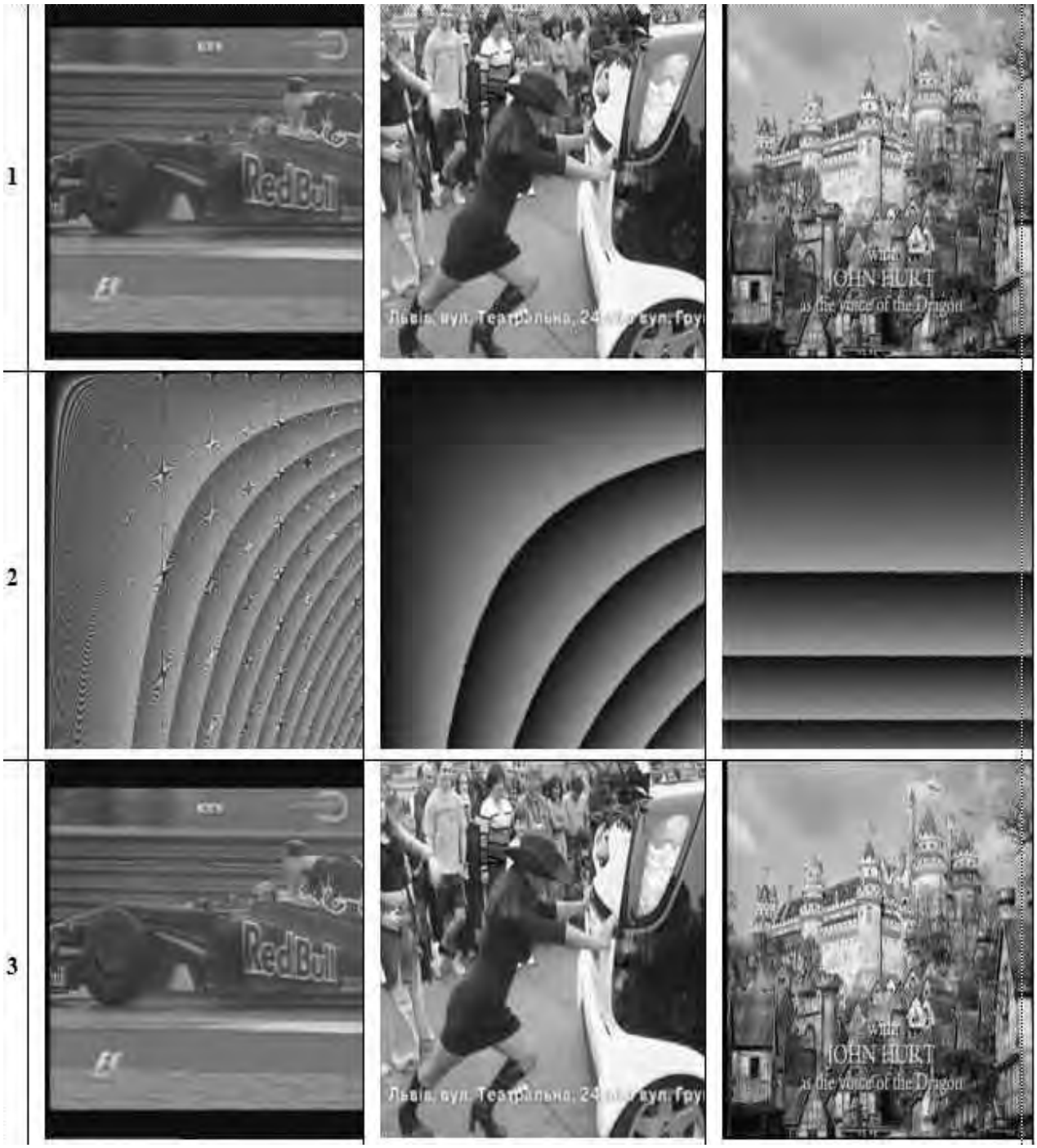

Рис. 2. Зображення: 1 – початкові; 2 – зашифровані; 3 – дешифровані

З порівняння рис. 1 і 2 видно, що шифрування за одним рядком матриці відрізняється від шифрування за двома рядками матриці. Контури в обох зашифрованих зображеннях відсутні. Початкові й дешифровані зображення тільки незначно відрізняються рівнем яскравості. Функції додаткової зашумленості ***f*(*P*,*Q*)**, ***h*(*i*)** та ***g*(*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 у градаціях сірого і ґрунтуються на використанні ідей базового алгоритму RSA.

2. Запропоновані алгоритми можна використовувати стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дають змогу чітко виділяти контури.

3. Обидві модифікації без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення зростає розмір шифрованого зображення.

4. Стійкість до несанкціонованого дешифрування запропонованими модифікаціями забезпечується алгоритмом RSA з додатковою стійкістю, яка визначається бінарним перетворенням.

5. Модифіковані методи шифрування побудовані так, що за малих значень ключа також можна досягти якісного шифрування, але за умови правильного підбору параметрів шифрування. При цьому досягається висока швидкість роботи алгоритму.

1. Прэтт У. Цифровая обработка изображений: пер. с англ. – М.: Мир, Кн. 2., 1982. – 480 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 4. Модифікація алгоритму RSA для деяких класів зображень / Рашкевич Ю. М., Пелешко Д. Д., Ковальчук А. М., Пелешко М. З. // Технічні вісті. – 2008/1(27), 2(28). – С. 59–62. 5. Ковальчук А., Пелешко Д., Хомин М., Борзов Ю. Поєднання алгоритму RSA і побітових операцій при шифруванні – дешифруванні зображень // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – 2011. – № 694. – С. 309–313. 6. Нетравали А. Н., Лимб Д. О. Кодирование изображений: обзор. – ТИИЭР. – 1980. – Т. 68, № 3. – С. 76–117.