МОДЕЛЮВАННЯ ПРОЦЕСІВ І СИСТЕМ

УДК 01.05.02; 05.13.06; 05.13.21

А. Ковальчук [1], Д.Пелешко [1], Ю.Борзов [2]
[1] Національний університет "Львівська політехніка",
кафедра інформаційних технологій видавничої справи,
[2] Львівський державний університет безпеки життєдіяльності

БІНАРНІ ОПЕРАЦІЇ ТА ЕЛЕМЕНТИ АЛГОРИТМУ RSA ПРИ ШИФРУВАННІ-ДЕШИФРУВАННІ КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Описано поєднання елементів алгоритму RSA і бінарних операцій для сумісного використання при шифруванні–дешифруванні зображень. Шифрування–дешифрування проводиться без додаткового зашумлення.

Ключові слова: шифрування, дешифрування, алгоритм RSA, бінарна операція.

Described combination of elements of the RSA algorithm and binary operations for the joint use for encryption–interpretation of images. Encryption–decryption is performed without additional noise.

Key words: encryption, decryption, the RSA algorithm, binary operation.

Вступ

Алгоритм RSA є одним із найуживаніших промислових стандартів шифрування сигналів. На відміну від симетричного кодування, за якого процедура розшифрування легко відновлюється за процедурою шифрування і зворотно, у схемі кодування з відкритим ключем неможливо обчислити процедуру дешифрування, знаючи процедуру шифрування. Точніше, час роботи алгоритму, що обчислює процедуру дешифрування, настільки великий, що його не можна реалізувати на будь-яких сучасних комп'ютерах, так само як і на будь-яких комп'ютерах майбутнього. Такі схеми кодування називають асиметричними.

Зображе́ння предме́та – відтворення вигляду, форми і кольору предмета світловими променями, що пройшли оптичну систему з центрованих сферичних поверхонь, які мають одну загальну оптичну вісь. Повноцінні растрові зображення надходять з фотокамер та сканерів. Зокрема, за їх допомогою відбувається масове "оцифрування" набутків культури – книжок і фотоплівок.

Зображення як стохастичний сигнал є одним із найширше використовуваних видів інформації. Відповідно актуальним завданням є захист такого зображення від несанкціонованого доступу та використання. Це спричиняє використання відомих класичних методів шифрування у випадку шифрування зображень. Але зображення є сигналом, який володіє, крім типової інформативності, ще й візуальною інформативністю.

Така інформативність із сучасними методами обробки зображень уможливлює організацію несанкціонованого доступу. Фактично організація атаки на зашифроване зображення можлива у двох варіантах: через традиційний злом 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 ставиться ще одна вимога – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуальної обробки зображень.

Існують певні проблеми щодо шифрування зображення, а саме частково зберігаються контури на різко флуктуаційних зображеннях [4, 5]. Виокремлення контурів у зображенні виконується на етапі створення опису його вмісту, і, отже, час виділення контурів впливає на загальний час виконання пошуку. З іншого боку, на час пошуку впливають часові витрати на порівняння описів вмісту зображень. Отже, алгоритм виділення контурів має відрізнятися якомога вищою швидкодією і при цьому створювати компактний опис контуру, придатний для подальшого порівняння.

Мета роботи

Щодо зображення актуальним завданням є таке модифіковане використання алгоритму RSA, щоб:

– не зменшити криптографічну стійкість алгоритму RSA;

– забезпечити повну зашумленість зображення, щоб унеможливити використання методів візуальної обробки зображень.

Одним зі способів створення такої модифікації є поєднання елементів алгоритму RSA і бінарних операцій у програмній реалізації.

Характеристики зображення

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

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

де c_{ij} – значення інтенсивності піксела. Тобто відзначається відповідність [1]

$$P = P_{l,h} = \left[pxl_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)} \to C=\left[c_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)}. \quad (2)$$

Під градацію яскравості звичайно виділяється 1 байт, причому 0 – чорний колір.

Завдання виділення контура вимагає використання операцій над сусідніми елементами, які чутливі 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. Тому виділення контура означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через які контури залишаються в зображенні у разі шифрування в системі RSA, оскільки шифрування тут ґрунтується на піднесенні до степеня за модулем деякого натурального числа. При цьому на контурі і на сусідніх з ним пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Опис алгоритму шифрування

Шифрування за одним рядком матриці зображення

Нехай $\boldsymbol{P, Q}$ – пара довільних простих чисел і $\boldsymbol{N = P * Q}$, $\boldsymbol{j(N) = (P - 1)(Q - 1).}$ Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення $\boldsymbol{C}$:

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

2. Якщо $\boldsymbol{i \equiv 0\ (\mathrm{mod}\ 2),\ 1 \le i \le l}$, то випадково вибирають число $\boldsymbol{m \equiv (i + P)\ (\mathrm{mod}\ 31)+1,}$ і будують числа $\boldsymbol{B \equiv m^e\ (\mathrm{mod}\ N), X = i*B*P.}$

3. Якщо $\boldsymbol{i \equiv 1\ (\mathrm{mod}\ 2),\ 1 \le i \le l}$, то випадково вибирають число $\boldsymbol{m \equiv (i + Q)\ (\mathrm{mod}\ 31)+1,}$ і будують числа $\boldsymbol{B \equiv m^d\ (\mathrm{mod}\ N), X = i*B*Q.}$

4. З використанням бінарної операції ^ - порозрядного виключеного “АБО” – будують число $\boldsymbol{a = c_{i,j} \wedge X.}$

5. Виокремлюється кожний розряд $\boldsymbol{a_i}$ числа $\boldsymbol{a}$ за такою схемою: a_1= a & 01; a_2= a & 02; a_3 = a & 04; a_4= a & 010; a_5 = a & 020; a_6 = a & 040; a_7 = a & 0100; a_8 = a & 0200; a_9 = a & 0400; a_{10} = a & 01000; a_{11} = a & 02000; a_{12} = a & 04000; a_{13} = a & 010000; a_{14} = a & 020000; a_{15} = a & 040000;

a_{16} = a & 0100000; a_{17} = a & 0200000; a_{18} = a & 0400000; a_{19} = a & 01000000; a_{20} = a & 02000000; a_{21} = a & 04000000; a_{22} = a & 010000000; a_{23} = a & 020000000; a_{24} = a & 040000000; a_{25} = a & 0100000000; a_{26} = a & 0200000000; a_{27} = a & 0400000000; a_{28} = a & 01000000000; a_{29} = a & 02000000000; a_{30} = a & 04000000000; a_{31} = a & 010000000000; a_{32} = a & 020000000000, де & - операція арифметичного "І".

6. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою: $k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.

7. Зашифрованим є зображення після 5-го кроку.

8. Всі числа B записуються в таку матрицю

$$V = \begin{pmatrix} b_{1,1} & \dots & b_{1,l} \\ \dots & \dots & \dots \\ b_{h,1} & \dots & b_{h,l} \end{pmatrix}.$$

Дешифрування за одним рядком матриці зображення

Дешифрування проводиться при заданих числах $e < j(N)$ і d, $N = P*Q$, $j(N) = (P - 1)(Q - 1)$.

1. Якщо $i \circ 0 \pmod 2$, $1 \le i \le l$, то будується число $m \equiv B^d \pmod N$ і число $X = i*B*P$.

2. Якщо $i \circ 1 \pmod 2$, $1 \le i \le l$, то будується число $m \equiv B^e \pmod N$ і число $X = i*B*Q$.

3. Виокремлюється кожний розряд a_i числа a за схемою: a_1= a & 01; a_2 = a & 02; a_3 = a & 04; a_4 = a & 010; a_5 = a & 020; a_6 = a & 040; a_7 = a & 0100; a_8 = a & 0200; a_9 = a & 0400; a_{10} = a & 01000; a_{11} = a & 02000; a_{12} = a & 04000; a_{13} = a & 010000; a_{14} = a & 020000; a_{15} = a & 040000; a_{16} = a & 0100000; a_{17} = a & 0200000; a_{18} = a & 0400000; a_{19} = a & 01000000; a_{20} = a & 02000000; a_{21} = a & 04000000; a_{22} = a & 010000000; a_{23} = a & 020000000; a_{24} = a & 040000000; a_{25} = a & 0100000000; a_{26} = a & 0200000000; a_{27} = a & 0400000000; a_{28} = a & 01000000000; a_{29} = a & 02000000000; a_{30} = a & 04000000000; a_{31} = a & 010000000000; a_{32} = a & 020000000000, де & - операція арифметичного "І".

4. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою: $k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.

5. З використанням бінарної операції ^ - порозрядного виключеного "АБО" - будується число $c_{i,j} = a \wedge X$.

6. Дешифрованим є зображення після 5-го кроку.

Результати наведено на рис. 1–3, при $P = 53, Q = 83$.

Рис. 1. Початкове зображення

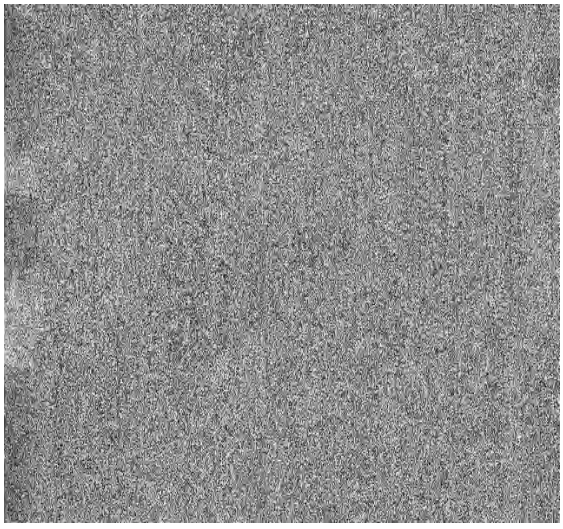

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Результати наведено на рис. 1 – 3 при $P = 127, Q = 53$.

Рис. 4. Початкове зображення

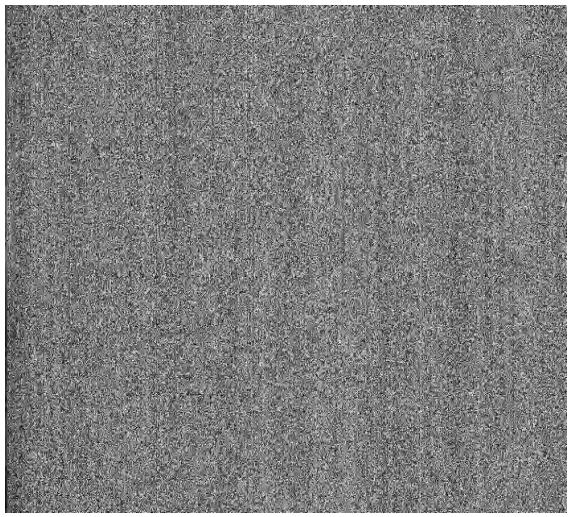

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

З порівняння рис. 2 і рис. 5 видно, що шифрування за різних значень простих чисел ***P*** і ***Q*** істотно не відрізняється. Контури в обох зашифрованих зображеннях відсутні. Початкові та дешифровані зображення тільки незначно відрізняються рівнем яскравості.

Висновки

1. Запропоновані модифікації шифрування призначені для шифрування кольорових зображень і ґрунтуються на використанні ідей базового алгоритму RSA. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення.

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

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

1. Павлидис Т. Алгоритмы машинной графики и обработки изображений. – М.: Радио и связь, 1986. – 399 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Шнайер Брюс. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 4. Модифікація алгоритму RSA для деяких класів зображень / Рашкевич Ю.М., Д.Д. Пелешко А.М. Ковальчук, М.З. Пелешко // Технічні вісті. – 2008/1(27), 2(28). – С. 59–62. 5. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction / Y. Rashkevych, A. Kovalchuk, D. Peleshko, M. Kupchak // Proceedings of the X-th International Conference CADSM 2009. 24–28 February 2009, Lviv-Polyana, Ukraine. – P. 469–473