УДК 01.05.02; 05.13.06; 05.13.21

А. Ковальчук, В. Цепак, А. Шевчук
Національний університет “Львівська політехніка”,
кафедра інформаційних технологій видавничої справи

МОДИФІКАЦІЯ АЛГОРИТМУ RSA З ВИКОРИСТАННЯМ ПОБІТОВИХ ОПЕРАЦІЙ У ШИФРУВАННІ-ДЕШИФРУВАННІ КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Описано поєднання елементів алгоритму RSA і побітових операцій для сумісного використання під час шифрування – дешифруванняі зображень. Шифрування – дешифрування проводиться без додаткового зашумлення.

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

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

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

Вступ

Алгоритм RSA (розшифровується як Rivest, Shamir and Aldeman – творці алгоритму) – це криптографічна система з відкритим ключем. RSA став першим алгоритмом, придатним і для шифрування, і для цифрового підпису. Цей алгоритм використовують у великій кількості криптографічних застосунків.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі: відкритий (public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари ключів (keypair). Схема цього алгоритму належить до асиметричного кодування, тобто обчислити процедуру дешифрування є неможливо, знаючи процес шифрування. Для того, щоб обчислити процедуру дешифрування, необхідна велика кількість часу; це неможливо реалізувати на сучасних комп’ютерах, а також на комп’ютерах майбутнього.

Зображення – це відтворення предметів і явищ об’єктивної дійсності в індивідуальному, своєрідному, конкретному художньому образі. Процес отримання фотографічного зображення передбачає отримання реального зображення за допомогою оптичної системи на час експозиції та фіксації цього зображення за допомогою світлочутливої системи у вигляді електронного файла або на фотоплівці. Під час отримання електронної фотографії зображення від оптичної системи оцифровується.

Цифрове зображення – масив даних, отриманий дискретизацією (аналого-цифровим перетворенням) оригіналу. Будучи закодованим за допомогою особливого алгоритму і записаним на носій, цей масив даних стає файлом.

Одією із найбільших форм надання інформації є зображення. Тому захист зображення є актуально задачею. Для шифрування використовують різні класичні методи шифрування. Але зображення несе не тільки типову інформативність, але і візуальну.

Розшифрувати зображення можна за допомогою або злому методу шифрування, або візуальної обробки даних. Тому в процесі шифрування зображення вимагається повна зашумленість. Це унеможливить доступ до інформації за допомогою обробки зображення.

Тому однією з важливих характеристик зображення є наявність в зображенні контурів. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін, тобто контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [2]. Математично ідеальний контур – це розрив просторової функ-

ції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [4]. Це є однією з причин, через 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 контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Мета роботи

Використовуючи алгоритм RSA, необхідно:

- криптографічна стійкість алгоритму не повинна зменшитись;
- зображення повинне бути повністю зашумлене [6];
- контури повинні бути непомітними у результаті шифрування зображення.

Характеристики зображення

Нехай задано зображення P завширшки l і заввишки h. Його можна розглядати як матрицю інтенсивностей пікселів

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

де w_{ij} – значення інтенсивності піксела [1].

Виокремлення контура означає пошук найрізкіших змін, контури – це області, які під впливом певних змін стають світлими, а інші частини зображення залишаються темними [2]. Задача виокремлення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості. Шифрування в системі RSA ґрунтується на піднесенні до степеня за модулем деякого натурального числа, тому контури залишаються в зображенні під час шифрування.

Опис алгоритму шифрування.

Шифрування за трьома послідовними елементами рядка матриці зображення

Нехай P, Q – пара довільних простих чисел і $N = P * Q$, $j(N) = (P - 1)(Q - 1)$ – функція Ейлера.

Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення W:

1. За алгоритмом RSA вибирають такі числа $e < j(N)$, $d < j(N)$, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ j(N))$.
2. Для j-го елемента i-го рядка матриці вибирають число $jj \equiv (P*j^2+Q*i^2+e) \pmod{32}$ і будуються числа $A \equiv jj^e \pmod{N}$, $X = j*A*P$, $1 \le j \le l$, $1 \le i \le h$.
3. Для $j+1$-го елемента вибирають число $jj \equiv (P*(i+1)^2+Q*(j+1)^2+e) \pmod{32}$ і будують числа $B \equiv jj^d \pmod{N}$, $Y = (j+1)*B*P$, $1 \le j \le l$, $1 \le i \le h$.
4. Для $j+2$-го елемента вибирають число $jj \equiv (P*(j+2)^2+Q*(j+2)^2+e) \pmod{32}$ і будують числа $B \equiv jj^d \pmod{N}$, $Z = (j+2)*B*P$, $1 \le j \le l$, $1 \le i \le h$.
5. З використанням бінарної операції ^ – порозрядного виключеного “АБО” – будують числа $a = z_{i,j} \wedge X$, $b = z_{i,j+1} \wedge Y$, $c = z_{i,j+2} \wedge Z$.
6. Виокремлюють кожний розряд a_n числа 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”.

7. Виконують циклічне заміщення $jj + 1$ розрядів числа a за схемою: $k = a_{jj+1}$, $a_{jj+1} = a_{jj}$, …, $a_2 = a_1$, $a_1 = k$.

8. Виокремлюється кожний розряд b_n числа b за такою схемою: $b_1 = b$ & 01; $b_2 = b$ & 02; $b_3 = b$ & 04; $b_4 = b$ & 010; $b_5 = b$ & 020; $b_6 = b$ & 040; $b_7 = b$ & 0100; $b_8 = b$ & 0200; $b_9 = b$ & 0400; $b_{10} = b$&01000; $b_{11} = b$&02000; $b_{12} = b$ &04000; $b_{13} = b$ &010000; $b_{14} = b$ &020000; $b_{15} = b$ & 040000; $b_{16} = b$ & 0100000; $b_{17} = b$ & 0200000; $b_{18} = b$ & 0400000; $b_{19} = b$ & 01000000; $b_{20} = b$ & 02000000; $b_{21} = b$ & 04000000; $b_{22} = b$ & 010000000; $b_{23} = b$ & 020000000; $b_{24} = b$ & 040000000; $b_{25} = b$ & 0100000000; $b_{26} = b$ & 0200000000; $b_{27} = b$ & 0400000000; $b_{28} = b$ & 01000000000; $b_{29} = b$ & 02000000000; $b_{30} = b$ & 04000000000; $b_{31} = b$ & 010000000000; $b_{32} = b$ & 020000000000, де & – операція арифметичного "І".

9. Виконують циклічне заміщення $jj + 1$ розрядів числа b за схемою: $k = b_{jj+1}$, $b_{jj+1} = b_{jj}$, …, $b_2 = b_1$, $b_1 = k$.

10. Виокремлюють кожний розряд c_n числа c за такою схемою: $c_1 = c$ & 01; $c_2 = c$ & 02; $c_3 = c$ & 04; $c_4 = c$ & 010; $c_5 = c$ & 020; $c_6 = c$ & 040; $c_7 = c$ & 0100; $c_8 = c$ & 0200; $c_9 = c$ & 0400; $c_{10} = c$&01000; $c_{11} = c$&02000; $c_{12} = c$ &04000; $c_{13} = c$ &010000; $c_{14} = c$ &020000; $c_{15} = c$ & 040000; $c_{16} = c$ & 0100000; $c_{17} = c$ & 0200000; $c_{18} = c$ & 0400000; $c_{19} = c$ & 01000000; $c_{20} = c$ & 02000000; $c_{21} = c$ & 04000000; $c_{22} = c$ & 010000000; $c_{23} = c$ & 020000000; $c_{24} = c$ & 040000000; $c_{25} = c$ & 0100000000; $c_{26} = c$ & 0200000000; $c_{27} = c$ & 0400000000; $c_{28} = c$ & 01000000000; $c_{29} = c$ & 02000000000; $c_{30} = c$ & 04000000000; $c_{31} = c$ & 010000000000; $c_{32} = c$ & 020000000000, де & – операція арифметичного "І".

11. Виконують циклічне заміщення $jj + 1$ розрядів числа c за схемою: $k = c_{jj+1}$, $c_{jj+1} = c_{jj}$, …, $c_2 = c_1$, $c_1 = k$.

12. Зашифрованим є зображення після кроків 5 – 11.

Дешифрування за трьома послідовними елементами рядка матриці зображення

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

1. Для j-го елемента i-го рядка матриці вибирають число $jj \equiv (P*j^2+Q*i^2+e) \pmod{32}$ і будують числа $A \circ jj^e \pmod{N}$, $X = j*A*P$, $1 \le j \le l$, $1 \le i \le h$.

2. Для $j+1$-го елемента вибирають число $jj \equiv (P*(i+1)^2+Q*(j+1)^2+e) \pmod{32}$ і будують числа $B \circ jj^d \pmod{N}$, $Y = (j+1)*B*P$, $1 \le j \le l$, $1 \le i \le h$.

3. Для $j+2$-го елемента вибирають число $jj \equiv (P*(j+2)^2+Q*(j+2)^2+e) \pmod{32}$ і будують числа $B \circ jj^d \pmod{N}$, $Z = (j+2)*B*P$, $1 \le j \le l$, $1 \le i \le h$.

4. З використанням бінарної операції ^ – порозрядного виключеного "АБО – будують числа $a = z_{i,\,j} \wedge X$, $b = z_{i,\,j+1} \wedge Y$, $c = z_{i,\,j+2} \wedge Z$.

5. Виокремлюють кожний розряд a_n числа 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. Виконують циклічне заміщення $jj + 1$ розрядів числа a за схемою: $k = a_{jj+1}$, $a_{jj+1} = a_{jj}$, …, $a_2 = a_1$, $a_1 = k$.

7. Виокремлюють кожний розряд b_n числа b за такою схемою: $b_1 = b$ & 01; $b_2 = b$ & 02; $b_3 = b$ & 04; $b_4 = b$ & 010; $b_5 = b$ & 020; $b_6 = b$ & 040; $b_7 = b$ & 0100; $b_8 = b$ & 0200; $b_9 = b$ & 0400; $b_{10} = b$&01000; $b_{11} = b$&02000; $b_{12} = b$ &04000; $b_{13} = b$ &010000; $b_{14} = b$ &020000; $b_{15} = b$ & 040000; $b_{16} = b$ & 0100000; $b_{17} = b$ & 0200000; $b_{18} = b$ & 0400000; $b_{19} = b$ & 01000000; $b_{20} = b$ & 02000000; $b_{21} = b$ & 04000000; $b_{22} = b$ & 010000000; $b_{23} = b$ & 020000000; $b_{24} = b$ & 040000000; $b_{25} = b$ & 0100000000; $b_{26} = b$ & 0200000000; $b_{27} = b$ & 0400000000; $b_{28} = b$ & 01000000000; $b_{29} = b$ & 02000000000; $b_{30} = b$ & 04000000000; $b_{31} = b$ & 010000000000; $b_{32} = b$ & 020000000000, де & – операція арифметичного "І".

8. Виконують циклічне заміщення $jj + 1$ розрядів числа b за схемою: $k = b_{jj+1}$, $b_{jj+1} = b_{jj}$, …, $b_2 = b_1$, $b_1 = k$.

9. Виокремлюють кожний розряд c_n числа c за такою схемою: $c_1 = c$ & 01; $c_2 = c$ & 02; $c_3 = c$ & 04; $c_4 = c$ & 010; $c_5 = c$ & 020; $c_6 = c$ & 040; $c_7 = c$ & 0100; $c_8 = c$ & 0200; $c_9 = c$ & 0400; $c_{10} = c$&01000; $c_{11} = c$&02000; $c_{12} = c$ &04000; $c_{13} = c$ &010000; $c_{14} = c$ &020000; $c_{15} = c$ & 040000; $c_{16} = c$ & 0100000; $c_{17} = c$ & 0200000; $c_{18} = c$ & 0400000; $c_{19} = c$ & 01000000; $c_{20} = c$ & 02000000; $c_{21} = c$ & 04000000; $c_{22} = c$ & 010000000; $c_{23} = c$ & 020000000; $c_{24} = c$ & 040000000; $c_{25} = c$ & 0100000000; $c_{26} = c$ & 0200000000; $c_{27} = c$ & 0400000000; $c_{28} = c$ & 01000000000; $c_{29} = c$ & 02000000000; $c_{30} = c$ & 04000000000; $c_{31} = c$ & 010000000000; $c_{32} = c$ & 020000000000, де & – операція арифметичного “І”.

10. Виконують циклічне заміщення $jj + 1$ розрядів числа c за схемою: $k = c_{jj+1}$, $c_{jj+1} = c_{jj}$, …, $c_2 = c_1$, $c_1 = k$.

11. Дешифрованим є зображення після кроків 4 – 11.

При $P = 83$, $Q = 53$ результати наведено на рис. 1–3.

Рис. 1. Початкове зображення

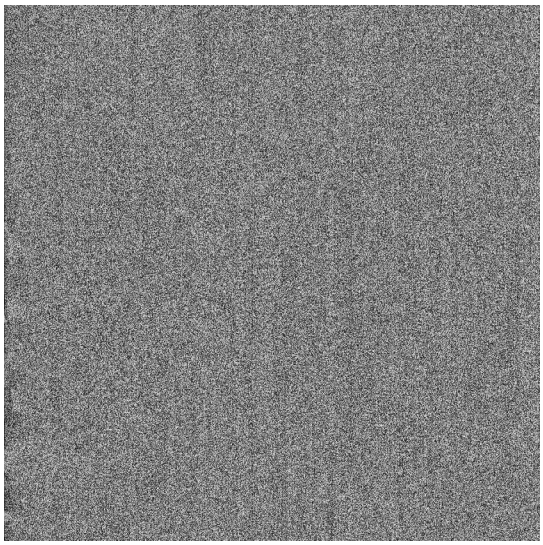

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

При $P = 101$, $Q = 103$ для іншого зображення результати наведені на рис. 4 – 6.

Порівнюючи рис. 2 і 5, бачимо, що шифрування за різних значень простих чисел P і Q, відрізняється. Контури в обох зашифрованих зображеннях відсутні. Початкові і дешифровані зображення тільки незначно відрізняються рівнем яскравості.

Рис. 4. Початкове зображення

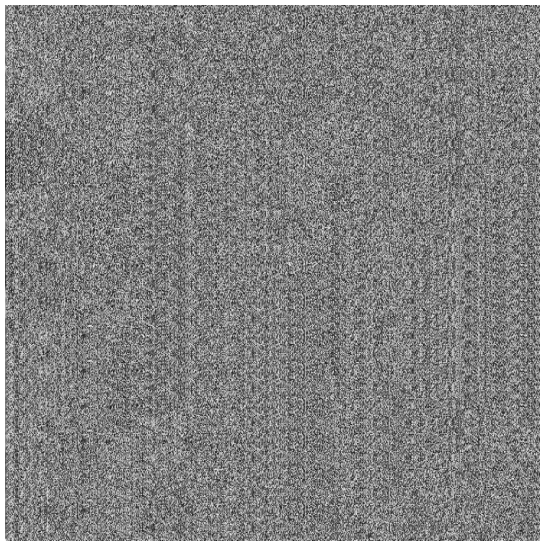

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Висновки

1. Запропоновану модифікацію шифрування можна використовувати для будь-якого типу зображень, зокрема зображення, в яких чітко можна виокремити контури, мають найбільші переваги. Ця модифікація грунтується на використанні ідей базового алгоритму RSA.

2. Розмір шифрованого зображення зростає пропорційно до розмірності вхідного зображення незалежно від типу зображення. Тому описану модифікацію можна використати і стосовно монохромних зображень.

3. Сумісне використання побітових операцій і алгоритм RSA забезпечує стійкість до несанкціонованого дешифрування запропонованою потоковою модифікацією.

1. Павлидис Т. Алгоритмы машиной графики и обработки изображений. – М.: Радио и связь, 1986. – 399 с. 2. Б. Яне. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Брюс Шнайер. 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, Pp. 469–473. 6. Ковальчук А. М., Попадинець К. С. Бінарні перетворення з елементами алгоритму RSA у захисті зображень за додаткового зашумлення // Вісник "Комп'ютерні науки та інформаційні технології". – № 843. – С. 79–84.