УДК 01.05.02; 05.13.06; 05.13.21

[1)]А. Ковальчук, [1)]Д. Пелешко, [2)]М. Навитка, [3)] Ю. Борзов
Національний університет “Львівська політехніка”,
[1)]кафедра інформаційних технологій видавничих систем,
[2)] кафедра інформаційних систем і технологій,
[3)] Львівський державний університет безпеки життєдіяльності

ПРО ОДНУ МОДИФІКАЦІЮ АЛГОРИТМУ RSA ШИФРУВАННЯ – ДЕШИФРУВАННЯ ПІВТОНОВИХ ЗОБРАЖЕНЬ

Описано застосування модифікації алгоритму RSA для шифрування – дешифрування зображень. Шифрування – дешифрування проводиться без і з додатковим зашумленням.

Ключові слова: шифрування, дешифрування, алгоритм RSA, зашумлення.

We describe the use of modified RSA algorithm for encryption – decryption of images. Encryption – decryption is carried out without and with extra noisy.

Key words: encryption, decryption, algorithm RSA, noisy.

Вступ

Одним із найбільш поширених і стійких алгоритмів шифрування інформації є алгоритм RSA [1], який належить до найуживанішої групи алгоритмів з відкритим ключем. Безпека алгоритму RSA ґрунтується на ресурсно затратній факторизації великих натуральних чисел. До того ж відкритий і закритий ключі, як правило, є функціями двох простих чисел з розрядністю 100–200 десяткових цифр або більше.

Алгоритм RSA належить до універсальних алгоритмів [3], тобто його можна застосовувати до шифрування різної структури сигналів. Це є його перевагою і недоліком. Основний недолік полягає в тому, що зашифровані подання сигналів окремих класів, можуть бути принаймні частково відтворені іншими засобами обробки. До таких сигналів належать цифрові зображення. Через це виникає потреба в розробленні спеціалізованих алгоритмів шифрування або модифікації наявних, оскільки можливий тільки один об’єктивний та строгий математичний результат, який визначається властивостями зображення.

Вважатимемо, що зображенню у відповідність ставиться матриця інтенсивностей кольорів

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

Стосовно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [2]. Однією з причин, через що контури залишаються в зображенні під час шифрування в системі RSA, є та, що шифрування тут ґрунтується на піднесенні до степеня по модулю деякого натурального числа. На контурі і на сусідніх до контуру пікселах піднесення до степеня значення яскравостей дає ще більший розрив. Різні методи уникнення такого стану наведені в [4, 5].

Шифрування і дешифрування по двох рядках матриці зображення

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

1) випадково вибирається натуральне число $e < j(N)$ і знаходиться таке натуральне d, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ j(N))$;

2) будуються чотири числа $A \equiv (c_{k,i})^e (\mathrm{mod}\, N)$, $B \equiv (c_{k+1,i})^e (\mathrm{mod}\, N)$, $E \equiv (c_{k,i+1})^d (\mathrm{mod}\, N)$, $D \equiv (c_{k+1,i+1})^d (\mathrm{mod}\, N)$, де $1 \le k < n$, $1 \le i < m$;

3) будується матриця зашифрованих значень інтенсивностей пікселів

$$\tilde{C} = \begin{pmatrix} \tilde{c}_{1,1}, & \mathbf{K} & ,\tilde{c}_{1,m} \\ \mathbf{L} & & \mathbf{M} \\ \tilde{c}_{n,1}, & \mathbf{L} & ,\tilde{c}_{n,m} \end{pmatrix},$$

де $\tilde{c}_{k,i} = A$, $\tilde{c}_{k+1,i} = B$, $\tilde{c}_{k,i+1} = E$, $\tilde{c}_{k+1,i+1} = D$, $1 \le k < n$, $1 \le i < m$.

Дешифрують так:

1) дешифровані значення інтенсивностей пікселів отримуються з таких співвідношень: $c_{k,i} \equiv A^d (\mathrm{mod}\, N)$, $c_{k+1,i} \equiv B^d (\mathrm{mod}\, N)$, $c_{k,i+1} \equiv E^d (\mathrm{mod}\, N)$, $c_{k+1,i+1} \equiv D^d (\mathrm{mod}\, N)$, $1 \le k < n$, $1 \le i < m$.

На рис. 1–3 наведено результати шифрування – дешифрування для $P = 23$, $Q = 37$.

Рис. 1. Початкове зображення

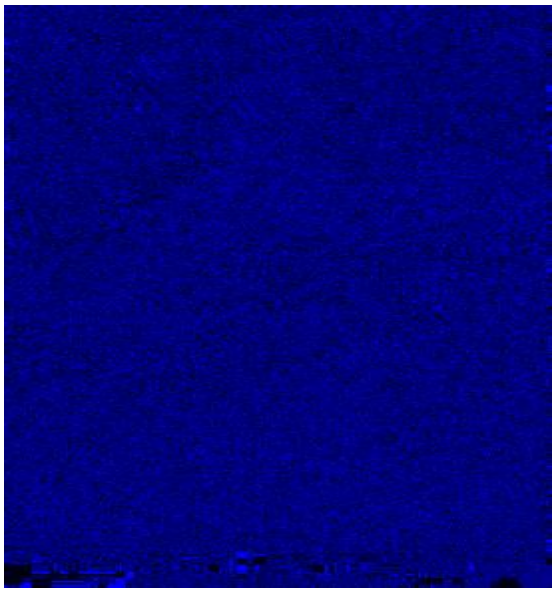


Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування і дешифрування по двох рядках матриці зображення з додатковим зашумленням

Нехай P,Q – пара довільних простих чисел і $N = P*Q$, $\varphi(N) = (P - 1)(Q - 1)$ Шифрування відбувається поелементно з використанням такого перетворення елементів матриці інтенсивностей кольорів 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) будуються чотири числа

$A \equiv (c_{k,i})^e (\mathrm{mod}\, N)$, $B \equiv (c_{k+1,i})^e (\mathrm{mod}\, N)$, $E \equiv (c_{k,i+1} + i^2/(ed))^d (\mathrm{mod}\, N)$,

$D \equiv (c_{k+1,i+1} + k^2/(ed))^d (\mathrm{mod}\, N)$, де $1 \le k < n$, $1 \le i < m$;

3) будується матриця зашифрованих значень інтенсивностей пікселів

$$\tilde{C} = \begin{pmatrix} \tilde{c}_{1,1}, & \cdots & ,\tilde{c}_{1,m} \\ & \cdots & \vdots \\ \tilde{c}_{n,1}, & \cdots & ,\tilde{c}_{n,m} \end{pmatrix},$$

де $\tilde{c}_{k,i} = A + f(k,i)$, $\tilde{c}_{k+1,i} = B + g(k,i)$, $\tilde{c}_{k,i+1} = E + F(k,i)$, $\tilde{c}_{k+1,i+1} = D + G(k,i)$,
$1 \le k < n$, $1 \le i < m$.

Дешифрують так.

1) дешифровані значення інтенсивностей пікселів отримують з таких співвідношень:

$$c_{k,i} \equiv (\tilde{c}_{k,i} - f(k,i))^d (\mathrm{mod}\, N),\ c_{k+1,i} \equiv (\tilde{c}_{k+1,i} - g(k,i))^d (\mathrm{mod}\, N),$$

$$c_{k,i+1} \equiv (\tilde{c}_{k,i+1} - F(k,i))^e (\mathrm{mod}\, N) - i^2/(ed),\ c_{k+1,i+1} \equiv (\tilde{c}_{k+1,i+1} - G(k,i))^e (\mathrm{mod}\, N) - k^2/(ed),$$

$$1 \le k < n,\ 1 \le i < m.$$

На рис. 4–6 наведено результати шифрування – дешифрування для $P = 13$, $Q = 97$, $f(k,i) = P - k^2 - i^2$, $g(k,i) = Q - k^2 - i^2$, $F(k,i) = e - k^2 - i^2$, $G(k,i) = P - k^2 - i^2$.

Рис. 4. Початкове зображення

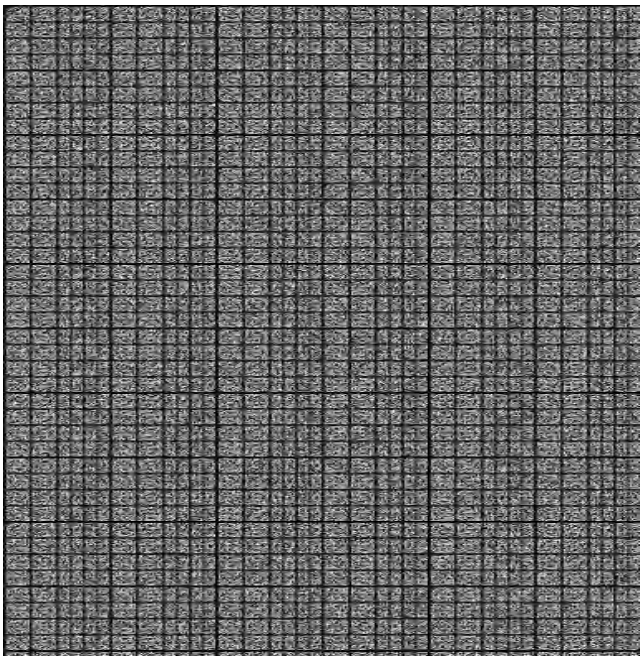
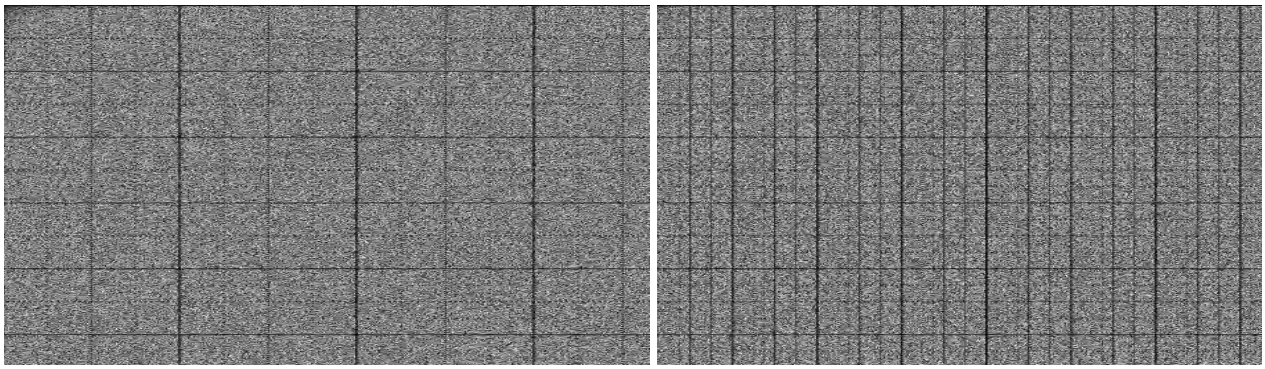


Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Зауважимо, що під час шифрування з додатковим зашумленням структура і властивості зашифрованого зображення візуально істотно відрізняються залежно від вибору структури зашумлення. Цей факт може бути використано в топологічній модифікації алгоритму шифрування–дешифрування. На рис. 7 показано результати використання різних функцій зашумлення.



$P = 43, Q = 67$

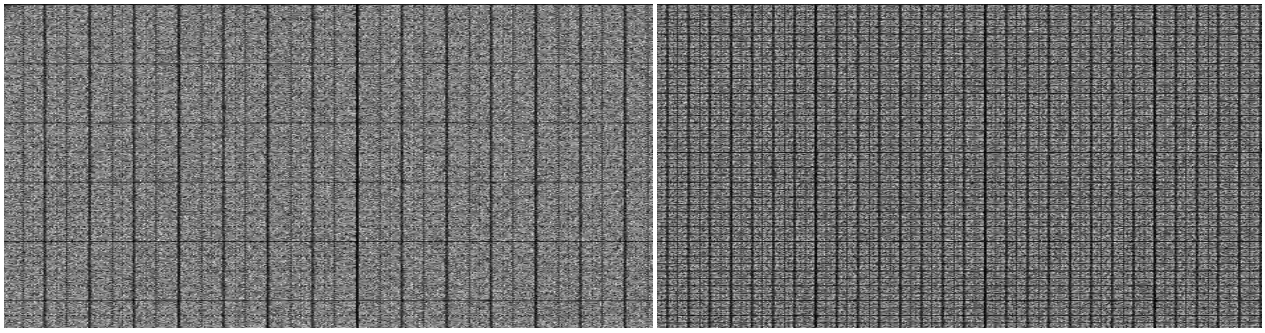
$f(k,i) = P\text{-}k^2\text{-}i^2,\ g(k,i) = Q\text{-}k^2\text{-}i^2,$

$F(k,i) = e\text{-}k^2\text{-}i^2, G(k,i) = P\text{-}k^2\text{-}i^2.$

$P = 43, Q = 67$

$f(k,i) = P\text{-}k^3\text{-}i^2,\ g(k,i) = Q\text{-}k^3\text{-}i^2,$

$F(k,i) = e\text{-}k^2\text{-}i^2, G(k,i) = P\text{-}k^2\text{-}i^2.$



$P = 43, Q = 67$

$f(k,i) = P\text{-}k^3\text{-}i^2,\ g(k,i) = Q\text{-}k^3\text{-}i^2,$

$F(k,i) = e\text{-}k^3\text{-}i^2, G(k,i) = P\text{-}k^3\text{-}i^2.$

$P = 43, Q = 67$

$f(k,i) = P\text{-}k^3\text{-}i^4,\ g(k,i) = Q\text{-}k^3\text{-}i^4,$

$F(k,i) = e\text{-}k^3\text{-}i^4, G(k,i) = P\text{-}k^3\text{-}i^4.$

Рис. 7. Структура зашумлення зашифрованих зображень

Висновки

1. Запропоновані модифікації шифрування призначені для шифрування зображень у 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 разі 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 розмір шифрованого зображення.

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

5. Реалізація стійкості модифікованих криптографічних алгоритмів з одночасним забезпеченням якості зображення не вимагають значних обчислювальних ресурсів.

1. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. Бином, 2002. – 384 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера , 2007. – 583 с. 3. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 4. 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. 5. Ковальчук А., Пелешко Д., Навитка М., Борзов Ю. Використання побітових операцій при шифруванні-дешифруванні кольорових зображень в модифікаціях алгоритму RSA // Вісник Нац. ун-ту «Львівська політехніка» «Комп'ютерні науки та інформаційні технології», 2011, № 719. – С.133–137.