УДК 01.05.02; 05.13.06; 05.13.21

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

СУМІСНЕ ВИКОРИСТАННЯ КРИПТОСИСТЕМ ЕЛЬ-ГАМАЛЯ І RSA В ЗАХИСТІ ГРАФІЧНОЇ ІНФОРМАЦІЇ

Описано поєднання алгоритму RSA і алгоритму Ель-Гамаля для сумісного використання під час шифрування – дешифрування зображень. Шифрування – дешифрування проводиться без і з додатковим зашумленням.

Ключові слова: шифрування, дешифрування, алгоритм RSA, алгоритм Ель-Гамаля, зашумлення.

We describe a combination of the RSA algorithm and the algorithm of El-Gamal for sharing with encryption – decryption of images. Encryption – decryption performed with and without additional noisy.

Key words: encryption, decryption, algorithm RSA, El-Gamal algorithm, noise in.

Вступ

Задача захисту графічної інформації є однією із найважливіших складових проектів автоматизації процесів документообігу. Надійний захист забезпечується збалансованим набором різних криптографічних систем захисту, що в результаті може підвищти криптографічну стійкість отриманих алгоритмів шифрування.

Схема RSA являє собою блоковий шифр, у якому і відкритий, і шифрований текст представляються цілими числами з діапазону від 0 до $n - 1$ для якогось n. Алгоритм RSA належить до універсальних алгоритмів [3], тобто може застосовуватися до шифрування різної структури сигналів. Це є його перевагою і недоліком. Основний недолік полягає в тому, що зашифровані представлення 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 існуючих, оскільки можливий тільки один об'єктивний та строгий математичний результат, який визначається властивостями зображення.

Алгоритм RSA є одним із найстійкіших алгоритмів шифрування інформації [1], який належить до найвживанішої групи алгоритмів з відкритим ключем. Безпека алгоритму RSA ґрунтується на ресурсно затратній факторизації великих натуральних чисел. На відміну від RSA метод Ель-Гамаля заснований на проблемі дискретного логарифма. Цим він схожий на *алгоритм Діффі-Хелмана*. Якщо підносити число до степеня в скінченному полі достатньо легко, то відновити аргумент за значенням (тобто знайти логарифм) доволі важко.

Будемо вважати, що зображенню у відповідність ставиться матриця інтенсивностей кольорів

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

Відносно 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 при шифруванні в системі RSA, є та, що 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. Різні методи уникнення такого стану приводяться в [4, 5].

Шифрування і дешифрування за одним рядком матриці зображення

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

1. Випадково вибирається натуральне число $d < \varphi(N)$ і знаходиться таке натуральне e, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. Випадково вибирається натуральне число x, $1 < x < P-1$ і вибирається натуральне число k, $1 < k < P-1$.
3. Будуються чотири числа $a \equiv Q$, $b \equiv (Q^x (\mathrm{mod}\, P))^k (\mathrm{mod}\, P)$, $a_{i,j} \equiv i(i+j)^e (\mathrm{mod}\, N)$, $b_{i,j} \equiv j(ij)^d (\mathrm{mod}\, N)$, де $1 \le i \le n$, $1 \le j \le m$.
4. Будується матриця зашифрованих значень інтенсивностей пікселів

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

де $\tilde{c}_{i,j} = ac_{i,j} - bc_{i,j+1} + a_{i,j} + f(i,j)$, $\tilde{c}_{i,j+1} = ac_{i,j} + bc_{i,j+1} + b_{i,j+1} + b_{i,j} + g(i,j)$, $f(i,j)$, $g(i,j)$ – деякі функції зашумлення, $1 \le i \le n$, $1 \le j < m$.

Дешифрування відбувається так:

1. Дешифровані значення інтенсивностей пікселів отримуються з таких співвідношень:

$$ac_{i,j} - bc_{i,j+1} = \tilde{c}_{i,j} - a_{i,j} - f(i,j),\ ac_{i,j} + bc_{i,j+1} = \tilde{c}_{i,j+1} - b_{i,j} - g(i,j),\ 1 \le i < n,\ 1 \le j < m.$$

Тоді $c_{i,j} = (a(\tilde{c}_{i,j} - a_{i,j} - f(i,j)) + b(\tilde{c}_{i,j+1} - b_{i,j} - g(i,j)))/\delta$,

$c_{i,j+1} = (a(\tilde{c}_{i,j+1} - b_{i,j} - g(i,j)) - b(\tilde{c}_{i,j} - a_{i,j} - f(i,j)))/\delta$, $\delta = a^2 + b^2$.

На рис. 1–3 наведено результати шифрування – дешифрування для $P = 53$, $Q = 67$.

Рис. 1. Початкове зображення

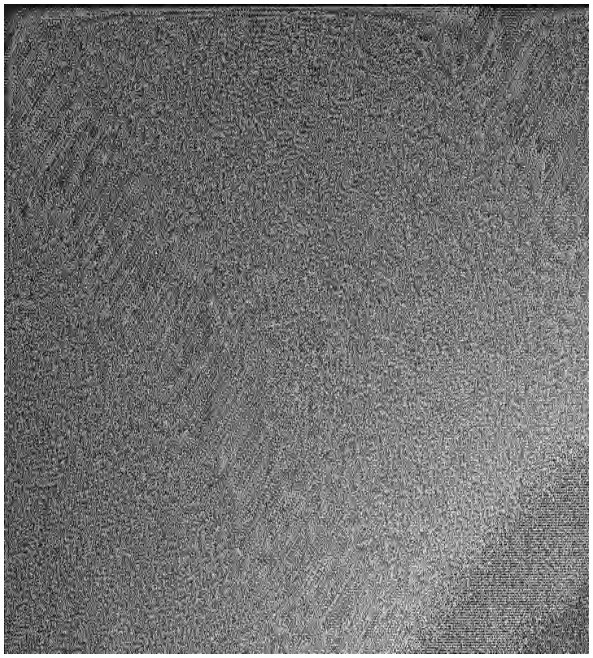

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування і дешифрування за двома рядками 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 наступного перетворення елементів матриці інтенсивностей кольорів зображення C:

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

6. Випадково вибирається натуральне число x, $1 < x < P-1$, і вибирається натуральне число k, $1 < k < P-1$.

7. Будуються чотири числа $a \equiv Q$, $b \equiv (Q^x (\mathrm{mod}\, P))^k (\mathrm{mod}\, P)$, $a_{i,j} \equiv i(i+j)^e (\mathrm{mod}\, N)$, $b_{i,j} \equiv j(ij)^d (\mathrm{mod}\, N)$, де $1 \le i \le n$, $1 \le j \le m$.

8. Будується матриця зашифрованих значень інтенсивностей пікселів

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

де $\tilde{c}_{i,j} = ac_{i,j} - bc_{i+1,j} + a_{i,j} + f(i,j)$, $\tilde{c}_{i+1,j} = ac_{i,j} + bc_{i+1,j} + b_{i,j} + b_{i,j} + g(i,j)$, $f(i,j)$, $g(i,j)$ – деякі функції зашумлення, $1 \le i \le n$, $1 \le j < m$.

Дешифрування відбувається так:

2. Дешифровані значення інтенсивностей пікселів отримуються з таких співвідношень:

$$ac_{i,j} - bc_{i+1,j} = \tilde{c}_{i,j} - a_{i,j} - f(i,j),\ ac_{i,j} + bc_{i+1,j} = \tilde{c}_{i+1,j} - b_{i,j} - g(i,j),\ 1 \le i < n,\ 1 \le j < m.$$

Тоді $c_{i,j} = (a(\tilde{c}_{i,j} - a_{i,j} - f(i,j)) + b(\tilde{c}_{i+1,j} - b_{i,j} - g(i,j)))/\delta$,

$$c_{i+1,j} = (a(\tilde{c}_{i+1,j} - b_{i,j} - g(i,j)) - b(\tilde{c}_{i,j} - a_{i,j} - f(i,j)))/\delta,\ \delta = a^2 + b^2.$$

Рис. 4. Початкове зображення

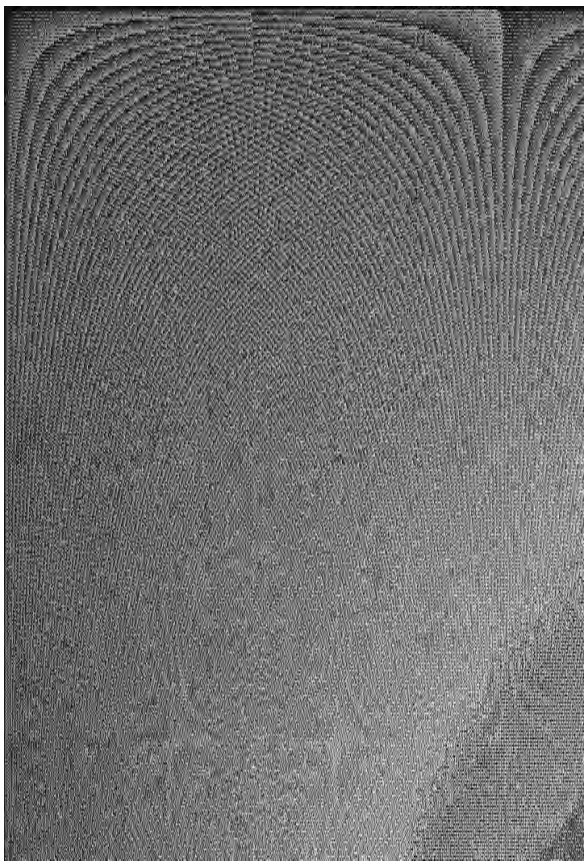

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Зауважимо, що при шифруванні з додатковим зашумленням структура властивості зашифрованого зображення візуально суттєво відрізняються залежно від вибору структури зашумлення і порядку вибору пікселів вхідного зображення. Цей факт можна використати в топологічній модифікації алгоритму шифрування–дешифрування.

Висновки

1. Запропонована модифікація шифрування призначена для шифрування зображень у градаціях сірого і грунтуються на використанні ідей базового алгоритму RSA та алгоритму Ель-Гамаля.
2. Запропонована модифікація може бути використана стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дозволяють чітко виділяти контури.
3. Описану модифікацію 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. Реалізація стійкості модифікованого криптографічного алгоритму визначається стійкістю двох викоистаних алгоритмів: Ель-Гамаля та RSA – і з одночасним забезпеченням якості зображення не вимагають значних обчислювальних ресурсів.

1. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. – М.: 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., Борзов Ю. Використання побітових операцій і додаткового зашумлення в алгоритмі RSA при шифруванні-дешифруванні зображень // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології", 2012. – № 744. – С. 132–137.