УДК 01.05.02; 05.13.06; 05.13.21

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

ВИКОРИСТАННЯ ПОБІТОВИХ ОПЕРАЦІЙ ПРИ ШИФРУВАННІ-ДЕШИФРУВАННІ КОЛЬОРОВИХ ЗОБРАЖЕНЬ У МОДИФІКАЦІЯХ АЛГОРИТМУ RSA

Запропоновано модифікації шифрування - дешифрування кольорових зображень, які грунтуються на використанні ідей базового алгоритму RSA з використанням побітових операцій. Розроблено модифікації алгоритму RSA такі, що зберігається криптографічна стійкість і забезпечується повна зашумленість зображення для запобігання використанню методів візуальної обробки зображень.

Ключові слова: кольорове зображення, обробка зображень, зашумленість, стійкість.

A modification of the encryption - decryption color images based on the use of the basic ideas of RSA algorithm using bitwise operations. A modification of RSA algorithm are stored by cryptographic resistance and provides full noisy image in order to prevent the use of methods of visual imaging.

Keywords: color image, image processing, noise, stability.

Вступ

Зображення є одними із найпоширеніших видів інформації в сучасному інформаційному суспільстві. Відповідно актуальною задачею є захист зображень від несанкціонованого доступу та використання.

Проблема несанкціонованого використання зображень на найнижчому рівні вирішується положеннями про авторське право, а на найвищому – методами криптографії і стеганографії, поліграфічними сітками тощо.

Основою для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Це дає змогу переносити класичні методи шифрування сигналів на випадок зображень. Але зображення є специфічним сигналом, який володіє, в додаток до типової інформативності (інформативності даних), ще й візуальною інформативністю. А остання привносить в питання захисту нові задачі [1].

Саме ця інформативність із дуже розвинутими сучасними методами обробки зображень дає можливість організовувати несанкціонований доступ. Фактично організація хакерської 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 до методів шифрування у випадку їх використання стосовно зображень висувається ще одна вимога – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуальної обробки зображень [2, 3].

Алгоритм RSA є одним із найпоширеніших промислових стандартів шифрування сигналів. Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [4, 5].

Мета роботи

Стосовно зображень актуальною задачею є розроблення такої модифікації методу RSA, щоб:

– зберегти криптографічну стійкість

– забезпечити повну зашумленість зображення для запобігання використанню методів візуальної обробки зображень.

Одним із шляхів вирішення цієї задачі є поєднання властивостей алгоритму RSA з використанням побітових операцій у програмній реалізації.

Характеристики зображення

Нехай задано рисунок ***P*** ширини ***l*** і висоти ***h***. Його можна розглядати як матрицю пікселів

$$<dtp_{ij}>_{1\le i\le n,\ 1\le j\le m}, \quad (1)$$

де dtp_{ij} – піксел з координатами ***i*** та ***j***, ***n*** і ***m*** – число точок за шириною ***l*** та висотою.

Матриці (1) відповідає матриця інтенсивностей кольорових пікселів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \quad (2)$$

де c_{ij} – значення інтенсивності зображень пікселя dtp_{ij} , $1\le i\le n$, $1\le j\le m$.

Важливою характеристикою зображення є наявність в зображенні контурів. Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні під час шифрування 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.

Опис модифікації алгоритму RSA

Нехай P, Q – пара довільних простих чисел і $N = P*Q$, $j(N) = (P-1)(Q-1)$. Випадково вибирають натуральне число $e < j(N)$ і знаходять таке натуральне ***d***, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ j(N))$. Шифрування відбувається поелементно для кожного *i*-го рядка з використанням таких перетворень елементів матриці зображення ***C***.

Шифрування

1. Якщо $j \bmod 2 \equiv 0$, то будується число : $jj = \mathrm{random}(j+P) \bmod 31 + 1$, $a_{i,j} \equiv jj^{e} \bmod N$, $X = j*a_{i,j}*P$.
2. Якщо $j \bmod 2 \equiv 1$, то будується число : $jj = \mathrm{random}(j+Q) \bmod 31 + 1$, $a_{i,j} \equiv jj^{d} \bmod N$, $X = j*a_{i,j}*Q$.
3. Будується число $K = c_{ij} \wedge X$.
4. Шифроване значення $\tilde{c}_{i,j}$ отримується циклічним зсувом числа ***K*** на $31 - jj$ розрядів .

Результатом роботи є матриця $\tilde{C} = \{\tilde{c}_{i,j}\}$ шифрованих значень інтенсивностей пікселів вхідної матриці $C = \{c_{i,j}\}$ і матриця ключів $A = \{a_{i,j}\}$.

Дешифрування

1. Якщо $j \bmod 2 \equiv 0$, то будується число : $jj = \mathrm{random}(j+P) \bmod 31 + 1$, $a_{i,j} \equiv jj^{d} \bmod N$, $X = j*a_{i,j}*P$.
2. Якщо $j \bmod 2 \equiv 1$, то будується число : $jj = \mathrm{random}(j+Q) \bmod 31 + 1$, $a_{i,j} \equiv jj^{e} \bmod N$, $X = j*a_{i,j}*Q$.

3. Виконується циклічний зсув числа $\tilde{c}_{i,j}$ на **31 - *jj*** розрядів**.**

4. Результатом роботи є матриця шифрованих значень інтенсивностей пікселів, $c = \tilde{c} \wedge X$ (^ - операція виключаючого “АБО”).

Рис. 1. Вхідне зображення

Рис. 2. Дешифроване зображення

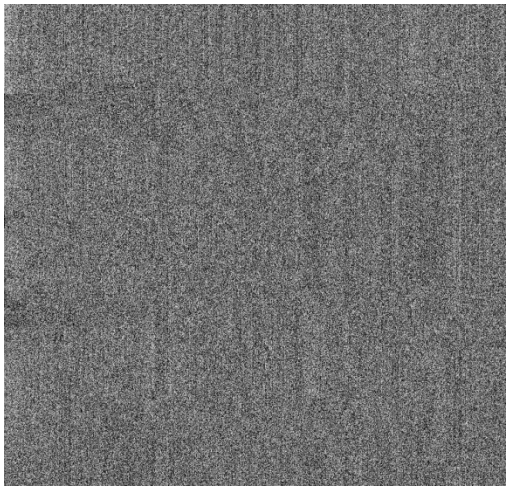

Рис. 3. Зашифроване зображення

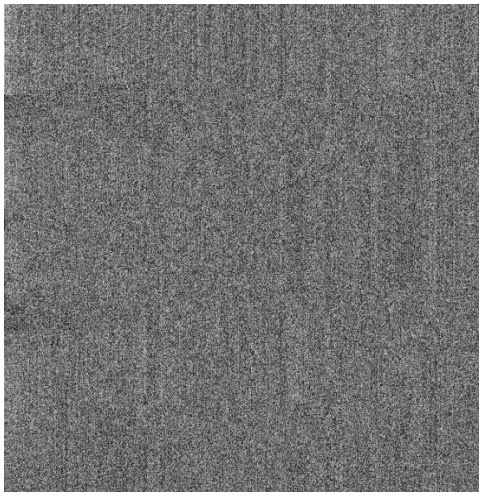

Рис. 4. Зображення матриці ключів

Рис. 5. Вхідне зображення

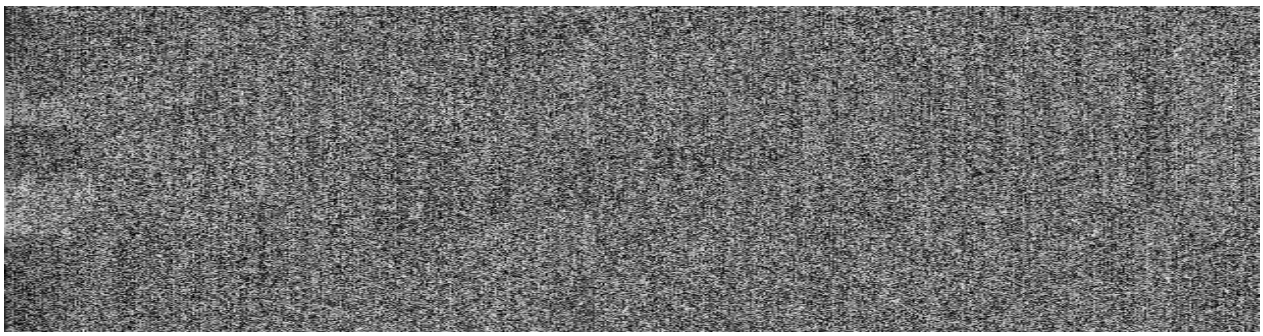

Рис. 6. Зашифроване зображення

Рис. 7. Дешифроване зображення

Рис. 8. Зображення матриці ключів

Висновок

Зроблено спробу поєднати і використати позитивні аспекти двох систем шифрування–дешифрування: симетричної та асиметричної. Негативна риса асиметричної системи – повільність шифрування-дешифрування – частково нейтралізується за такого поєднання швидкістю симетричної системи. Як видно з результатів, шифрування за такого підходу не втрачає того рівня стійкості, який притаманний для обох систем. Запропоновані модифікації можна використати стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дають змогу чітко виділяти контури.

1. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. 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. 4. 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. 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.