УДК 01.05.02; 05.13.06; 05.13.21

А. Ковальчук[1], Д. Пелешко[1], М. Хомин[2], Ю. Борзов[3]
[1]Національний університет «Львівська політехніка» ,
кафедра автоматизованих систем управління,
[2]Західний науковий центр,
[3]Львівський державний університет безпеки життєдіяльності

ПОЄДНАННЯ АЛГОРИТМУ RSA І ПОБІТОВИХ ОПЕРАЦІЙ ПРИ ШИФРУВАННІ-ДЕШИФРУВАННІ ЗОБРАЖЕНЬ

Стосовно зображень розроблено модифікації алгоритму RSA такі, що зберігається криптографічна стійкість і забезпечується повна зашумленість зображення, з метою унеможливити використання методів візуальної обробки зображень.

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

For images modified RSA algorithm is developed such that stored cryptographic and secured full noisy image in order to prevent the use of methods of visual imaging.

Keywords: image, image processing, noise, stability.

Вступ

Зображення є одними із найпоширеніших видів інформації в сучасному інформаційному суспільстві. Відповідно актуальним завданням 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.

Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Цим зумовлено перенесення класичних методів шифрування сигналів на випадок зображень. Але зображення є специфічним сигналом, який володіє, крім типової інформативності (інформативності даних), ще й візуальною інформативністю. А остання привносить в питання захисту нові завдання.

Саме ця інформативність із дуже розвинутими сучасними методами обробки зображень уможливлює організацію несанкціонованого доступу. Фактично можливі два варіанти організації хакерської атаки на зашифроване зображення: через традиційний злом 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 застосування методів візуальної обробки зображень.

Алгоритм RSA є одним із науживаніших 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 актуальним завданням є розроблення модифікації методу RSA такої, щоб

– зберегти криптографічну стійкість;

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

Одним зі способів розв'язання цієї задачі є поєднання властивостей алгоритму RSA з використанням побітових операцій в програмній реалізації.

Характеристики зображення

Нехай задано рисунок $\boldsymbol{P}$ з 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 – кількість точок по ширині l та висоті. В загальному випадку n і m є залежними від l та h, а тому коректнішим є запис

$$n = n(l) \text{ і } m = m(h). \quad (2)$$

Матриці (1) у відповідність ставиться матриця інтенсивностей пікселів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \tag{3}$$

де c_{ij} – значення інтенсивності у напівтонових зображень піксела dtp_{ij}. Тобто забезпечується відповідність [1]

$$P = \mathbf{P}_{l,h} = \left[pxl_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)} \to \mathbf{C}=\left[c_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)}. \tag{4}$$

Під градацію яскравості звичайно виділяється 1 байт, причому 0 – чорний колір, а 255 – білий (максимальна інтенсивність).

Важливою характеристикою зображення є наявність в зображенні контурів. Для виділення контуру необхідно використовувати операції над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто контури – це ті області, де виникають зміни, вони стають світлими, тоді як інші частини зображення залишаються темними [2].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контуру означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин того, що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування основане на піднесенні до степеня за модулем деякого натурального числа. На контурі і на сусідніх з контуром пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Опис модифікації алгоритму RSA

Шифрування і дешифрування за одним рядком матриці зображення.

Нехай P, Q – пара довільних простих чисел і $N = P * Q$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці 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. Формується число $A = (e << k) + (d << l) + (e << l) + (d << k)$, де $k < 16$, $l < 16$ – натуральні числа, $k \neq l$, << - операція логічного зсуву вліво.

3. В кожному рядку виконується логічний зсув вліво значення інтенсивності i-го піксела, $i = 1, 2, \dots, m$, m – кількість елементів у рядку, за правилом: якщо $i \bmod 7 = 0$, то виконується логічний зсув вліво значення інтенсивності піксела на величину $i \bmod 3$, якщо $i \bmod 11 = 1$, то виконується логічний зсув вліво значення інтенсивності піксела на величину $i \bmod 4$.

4. Визначається число B відніманням від отриманого значення інтенсивності піксела числа $(A - 3)$.

5. Зашифрованим значенням інтенсивності i-го піксела, $i = 1, 2, \dots, m$, m – кількість елементів у рядку, вибирається число $C \equiv B^e \pmod N$.

Дешифрування виконують у послідовності, протилежній до шифрування, після отримання числа $C^d \equiv (B^e)^d \pmod N$, виконанням протилежних операції до змісту пунктів 4), 3), 2), 1).

Результати наведено на рис. 1–3.

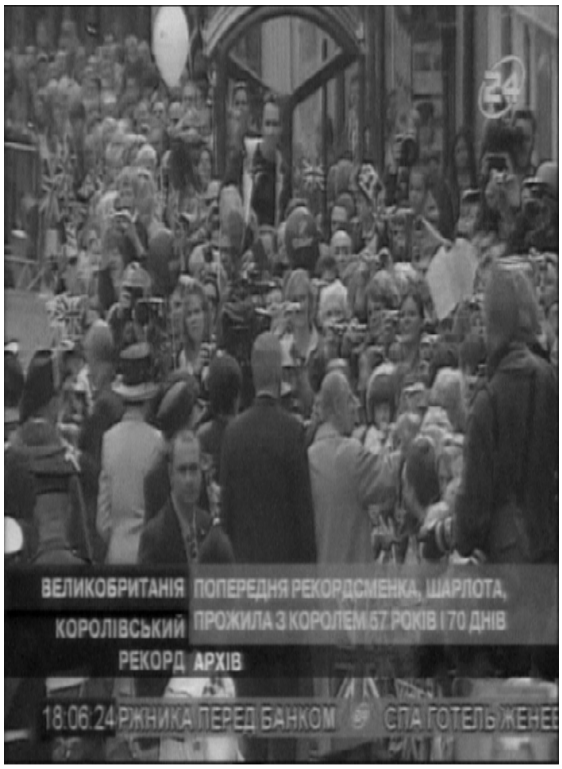

Рис. 1. Початкове зображення

Рис. 2. Зашифроване зображення

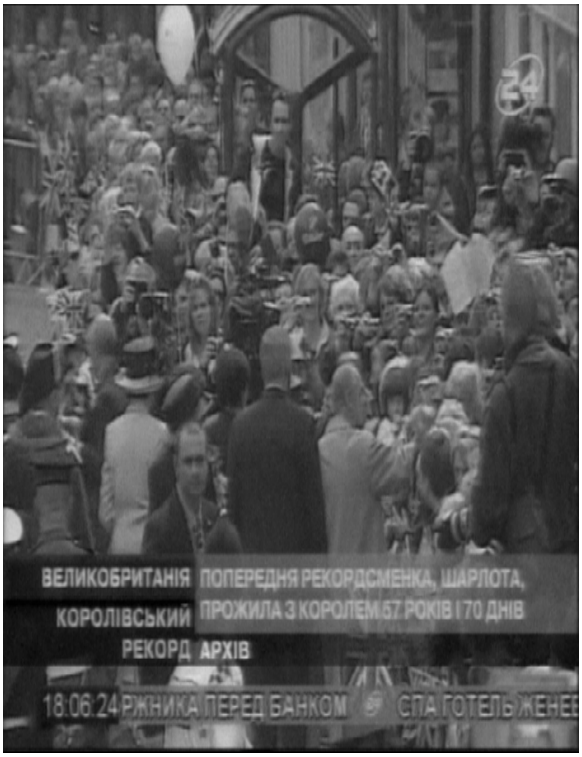

Рис. 3. Дешифроване зображення

Шифрування за двома рядками матриці

Шифрування відбувається з використанням елементів двох рядків за алгоритмом, який описано вище, для шифрування елементів одного рядка інтенсивностей, за винятком п. 5, причому кожний рядок з вибраних двох рядків шифрується незалежно за своїм алгоритмом, для нього модифікованим п. 5.

Пункт 5 має вигляд:

5.1. Для першого рядка зашифрованим значенням інтенсивності ***i***-го піксела, $i = 1, 2, \ldots, m$, m – кількість елементів у рядку, вибирається число $C \equiv B^e \pmod N$.

5.2. Для другого рядка зашифрованим значенням інтенсивності ***i***-го піксела, $i = 1, 2, \ldots, m$, m – кількість елементів у рядку, вибирається число $C \equiv B^d \pmod N$.

Дешифрування відбувається в протилежному порядку з урахуванням п.п. 5.1, 5.2.

Результати наведено на рис. 4–6.

Рис. 4. Початкове зображення

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

З порівняння рис. 2 і рис. 5 видно, що шифрування за одним рядком матриці (3) істотно не відрізняється від шифрування за двома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Початкові та дешифровані зображення тільки незначно відрізняються рівнем яскравості

Висновки

1. Запропоновані модифікації шифрування призначені для шифрування зображень в градаціях сірого і ґрунтуються на використанні ідей базового алгоритму RSA.

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. Обидва типи модифікацій без жодних застережень можна застосовувати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зрости розмір шифрованого зображення.

4. Стійкість до несанкціонованого дешифрування запропонованої потокової модифікації 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 Б. 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. – P. 469–473.

УДК 004.021

В. Самотий[1,2], У. Дзелендзяк[1]
[1.] Національний університет “Львівська політехніка”,
кафедра комп’ютеризованих систем автоматики
[2] Politechnika Krakowska, katedra Automatyki i Technik Informacyjnych, Polska

ВИКОРИСТАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ ДЛЯ АПРОКСИМАЦІЇ ФУНКЦІЙ ДІЙСНИМИ ПОЛІНОМАМИ

Наведено метод апроксимації функцій поліномами з дійсними степенями, в якому підбір степеня здійснюється за допомогою генетичного алгоритму.

Ключові слова: генетичний алгоритм, особина, популяція, мутація, функція цілі, апроксимація, поліном.

The method of approximation of functions by polynomials with real powers, which is the power of selection with a genetic algorithm.

Keywords: genetic algorithm, individual, population, mutation, function targets, approximation, polynomial.

Вступ

Задача апроксимації функцій, заданих у табличному або графічному вигляді, не нова. Проте, незважаючи на численні дослідження цього питання, воно і досі не втратило актуальності. Наведемо лише один з прикладів застосування апроксимації. Відома дуже перспективна технологія створення мап-територій, основана на лазерному скануванні поверхні Землі з літака. В результаті отримують точки з певними характеристиками. Застосувавши методи розпізнавання графічних зображень, ми можемо окреслити контури об’єктів. Кожен контур містить великий набір точок, необхідних для його точного відтворення. Апроксимація контурів об’єктів дає можливість істотно зменшити обсяг інформації для їх відтворення. Використання поліноміальних функцій для цієї мети часто супроводжується значними похибками, що негативно впливає на процес відтворення контурів об’єктів. Проблему цю було важко вирішити в зв’язку з обмеженістю аналітичних підходів. Поява