системах // Вісник Нац. ун-ту "Львівська політехніка": Комп'ютерні науки та інформаційні технології. – Львів, 2007. – № 604. – С. 220–227. 5. Притула Н.М., Притула М.Г., П'янило Я.Д. Розрахунок усталеного руху газу в магістральних газопроводах // Вісник Вісник Нац. ун-ту "Львівська політехніка": Комп'ютерні науки та інформаційні технології. – Львів, 2006. – № 565. – С. 270–274.

УДК 01.05.02; 05.13.06; 05.13.21

А. Ковальчук, Д. Пелешко, М. Навитка*
Національний університет "Львівська політехніка",
кафедра інформаційних технологій видавничої справи,
*кафедра інформаційних систем і технологій

ВИКОРИСТАННЯ АДИТИВНО-РІЗНИЦЕВИХ ОПЕРАЦІЙ У МОДИФІКАЦІЯХ АЛГОРИТМУ RSA

Запропоновано модифікації шифрування – дешифрування зображень у градаціях сірого, які грунтуються на використанні ідей базового алгоритму RSA з додатковим зашумленням зашифрованого зображення і без додаткового зашумлення.

Ключові слова: зображення, зашумлення, алгоритм RSA, градації сірого.

A modification of the encryption – decryption of images in grayscale, and are based on ideas using the basic algorithm of RSA, with additional noise encrypted image without any additional noise.

Keywords: image, noise, the algorithm RSA, grayscale.

Вступ

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

Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Але зображення є специфічним сигналом, який володіє разом із типовою інформативністю (інформативністю даних) ще й візуальною інформативністю.

Така інформативність з використанням сучасних методів обробки зображень дає можливість для організації несанкціонованого доступу. Реалізація атаки на зашифроване зображення можлива у двох варіантах: традиційним взломом методів шифрування або за допомогою методів візуальної обробки зображень (методи фільтрації, виділення контурів тощо). У зв'язку з цим до методів шифрування у випадку їх використання стосовно зображень висувається ще одне завдання – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів попередньої візуальної обробки зображень.

Проблема захисту від несанкціонованого доступу є складнішою порівняно з проблемою захисту використання. Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Це спричиняє перенесення класичних методів шифрування сигналів на випадок зображень. Але зображення є специфічним сигналом, який має, крім типової інформативності (інформативності даних), ще й візуальну інформативність. А остання привносить в питання захисту нові задачі.

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

Використання алгоритму шифрування RSA [1, 6, 7] як найбільш стійкого до несанкціонованого дешифрування кодованих сигналів стосовно зображень, які дають змогу дуже строго виділяти контури, не дає задовільних результатів – контури проступають на зашифрованому зображенні. Це дає можливість несанціоновано отримати інформативність з рисунка методами обробки зображень.

Мета роботи

Стосовно зображень актуальною задачею є розробка такої модифікації алгоритму RSA, щоби:

- зберегти криптографічну стійкість;
- забезпечити повну зашумленість зображення.

Одним із шляхів розв'язок цієї задачі є поєднання властивостей алгоритму RSA з вико ристанням деяких випадково вибраних натуральних чисел у програмній реалізації .

Характеристики зображення

Нехай задано рисунок $\boldsymbol{P}$ з шириною l і висотою h. Його можна розглядати як матрицю пікселів

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

де dtp_{ij} – піксел з координатами i та j, n і m – число точок по ширині l та висоті.

Матриці (1) у відповідність ставиться матриця інтенсивностей пікселів

$$C=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \tag{2}$$

де $\boldsymbol{c_{ij}}$ – значення інтенсивності у напівтонових зображень піксела dtp_{ij}. Тобто має місце відповідність [1]

$$P = \mathrm{P}_{l,h} = \left[pxl_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)} \to C=\left[c_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)}. \tag{3}$$

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

Важливою характеристикою зображення є наявність у зображенні контурів. Математично ідеальний контур – це розрив просторової функції рівнів яскравості у 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 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.

Опис модифікацій алгоритму RSA

Поелементне шифрування – дешифрування за чотирма послідовними елементами рядка матриці зображення

Нехай $\boldsymbol{P, Q, U, V}$ – довільні прості числа і $\boldsymbol{N = P*Q, L = U*V}$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення $\boldsymbol{C}$:

1. Випадково вибираються натуральні числа $\boldsymbol{e < j(N)}$, $\boldsymbol{e_1 < j(L)}$ і знаходяться такі натуральні $\boldsymbol{d}$ і $\boldsymbol{d_1}$, що виконуються конгруенції $\boldsymbol{ed \equiv 1 (\mathrm{mod}\ j(N))}$, $\boldsymbol{e_1 d_1 \equiv 1 (\mathrm{mod}\ j(L))}$.
2. Нехай $\boldsymbol{a}$ – одне з чисел $\boldsymbol{e}$ або $\boldsymbol{d}$, $\boldsymbol{b}$ – друге. Будуються два числа: $\boldsymbol{A = (c_{i,j})^a (\mathrm{mod}\ N)}$ і $\boldsymbol{B = (c_{i,j+3})^b (\mathrm{mod}\ N)}$.
3. Нехай a – одне з чисел $\boldsymbol{e_1}$ або $\boldsymbol{d_1}$, b – друге. Будуються два числа: $\boldsymbol{D = (c_{i,j+1})^a (\mathrm{mod}\ L)}$ і $\boldsymbol{E = (c_{i,j+2})^b (\mathrm{mod}\ L)}$ і два числа $\boldsymbol{u_{i,j+1} = D + E}$, $\boldsymbol{u_{i,j+2} = D - E}$.
4. Зашифрованими значеннями інтенсивностей $\boldsymbol{j}$ –го, $\boldsymbol{j+1}$ -го, $\boldsymbol{j+2}$ -го, $\boldsymbol{j}$ +3 -го, пікселів, $\boldsymbol{i = 1, 2, \dots, m}$, $\boldsymbol{m}$ – число елементів у рядку, вибираються числа: $\boldsymbol{A, u_{i,j+1}, u_{i,j+2}, B}$.

Дешифрування проводять так:

1. Знаходять інтенсивності $c_{i,j+1} = [(u_{i,j+1} + u_{i,j+2})/2]^b \pmod L$, $c_{i,j+2} = [(u_{i,j+1} - u_{i,j+2})/2]^b \pmod L$
2. Знаходять інтенсивності $c_{i,j} = A^b \pmod N$, $c_{i,j+3} = B^b \pmod N$.
3. Зашифрованими значеннями інтенсивностей j – го, $j+1$ -го, $j+2$ -го, $j+3$ -го, пікселів, $i = 1, 2, \dots, m$, m – число елементів у рядку, вибирають числа: $c_{i,j}$, $c_{i,j+1}$, $c_{i,j+2}$, $c_{i,j+3}$.

Результати наведено на рис.1.

Рис. 1. *1 – початкові зображення; 2 – зашифровані зображення; 3 – дешифровані зображення*

Поелементне шифрування – дешифрування за чотирма послідовними елементами рядка матриці зображення з додатковим зашумленням.

Нехай P, Q, U, V – довільні прості числа і $N = P*Q$, $L = U*V$. Шифрування відбувається поелементно з використанням наступного перетворення елементів матриці зображення C:

1. Випадково вибираються натуральні числа $e < j(N)$, $e_1 < j(L)$ і знаходяться такі натуральні d і d_1, що виконуються конгруенції $ed \equiv 1 \pmod{j(N)}$, $e_1 d_1 \equiv 1 \pmod{j(L)}$.
2. Нехай a – одне з чисел e або d, b – друге. Будуються числа: $A = (c_{i,j})^a \pmod N + f(i, j)$ і $B = (c_{i,j+3})^b \pmod N + f(i, j)$.
3. Нехай a – одне з чисел e_1 або d_1, b – друге. Будуються два числа: $D = (c_{i,j+1})^a \pmod L$ і $E = (c_{i,j+2})^b \pmod L$ і два числа $u_{i,j+1} = D + E + f(i, j)$, $u_{i,j+2} = D - E + f(i, j)$.

Зашифрованими значеннями інтенсивностей ***j***-го, ***j*** +**1**-го, ***j*** +**2**-го, ***j*** +3-го, пікселів, ***i*** **= 1, 2, … ,** ***m***, ***m*** – число елементів у рядку, вибираються числа: ***A***, $u_{i,j+1}$,$u_{i,j+2}$, ***B***.

Дешифрування проводять так:

Знаходяться інтенсивності $c_{i,j} = A^b \pmod N - f(i,j) = A^b \pmod N$, $c_{i,j+3} = B^b \pmod N - f(i,j)$, $c_{i,j+1} = [(u_{i,j+1} + u_{i,j+2})/2]^b \pmod L - f(i,j)$, $c_{i,j+2} = [(u_{i,j+1} - u_{i,j+2})/2]^b \pmod L - f(i,j)$.

Зашифрованими значеннями інтенсивностей ***j***-го, ***j*** +**1**-го, ***j*** +**2**-го, ***j*** +3-го пікселів, ***i*** **= 1, 2, … ,** ***m***, ***m*** – число елементів у рядку, вибираються числа: $c_{i,j}$, $c_{i,j+1}$, $c_{i,j+2}$, $c_{i,j+3}$.

Результати наведені на рис.2. Для шифрування вибиралися такі функції для додаткового зашумлення: $f(i,j) = i^2$, $f(i,j) = i^2 + j^2$, $f(i,j) = j^2$.

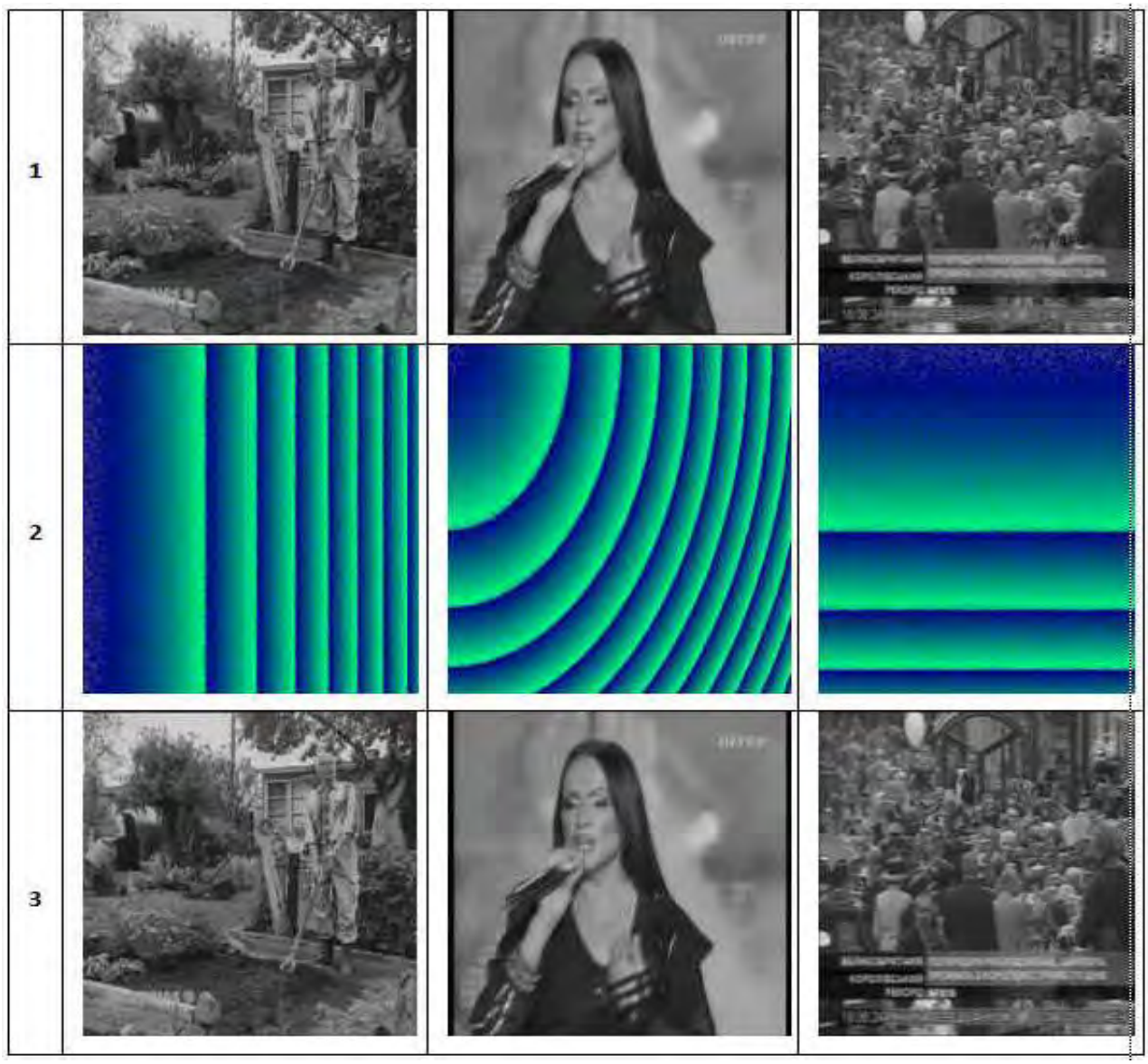

Рис. 2. *1 – початкові зображення;*
2 – зашифровані зображення; 3 – дешифровані зображення

З порівняння рис. 1 і рис. 2 видно, що шифрування з додатковим зашумленням відрізняється від шифрування без додаткового зашумлення. Контури в обох зашифрованих зображеннях відсутні. Початкові і дешифровані зображення тільки незначно відрізняються рівнем яскравості.Функції додаткової зашумлності ***f(i , j)*** можуть бути довільними цілозначними функціями і додатково до створюваної алгоритмом RSA зашумленості підвищують криптографічну стійкість вказаних модифікацій.

Висновки

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

2. Запропоновані модифікації можна використати стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку 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. Стійкість до несанкціонованого дешифрування запропонованою потоковою модифікацією забезпечується стійкістю алгоритмому RSA.

5. При шифруванні зберігається ізоморфність вхідного і дешифрованого набору, що можна використати для визначення інших характеристик зображення: розпізнавання, сегментації тощо.

6. Швидкість роботи запропонованих модифікованих методів шифрування є достатньою для того, щоб бути інтегрованими у комплексні системи реального часу, які вирішують завдання не лише шифрування об'єктів, а й розпізнавання, визначення відбракованих об'єктів, фасування тощо.

1. Павлидис Т. Алгоритмы машиной графики и обработки изображений. – М.: Радио и связь, 1986.-399с. 2. Б.Яне. Цифровая обработка изображений. – М., Техносфера, 2007. – 583с. 3. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с. 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. 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. 6. Вельшенбах М. Криптография на Си и С++ в действии: Учеб. пособие. – М.: Издательство Триумф, 2004. – 464 с. 7. Вербіцький О.В. Вступ до криптології. – Львів: Видавництво науково-технічної літератури, 1998. – 247 с.

УДК 681.513

С. Кухарєв
Національний технічний університет України "Київський політехнічний інститут",
Навчально-науковий комплекс "Інститут прикладного системного аналізу",
кафедра математичних методів системного аналізу

КОНЦЕПТУАЛЬНА МОДЕЛЬ ІМІТАЦІЙНОГО АЛГОРИТМУ МОДЕЛЮВАННЯ РОБОТИ МЕРЕЖІ З ТЕХНОЛОГІЄЮ MPLS

Описано концептуальну модель розробленого імітаційного алгоритму, призначеного для моделювання роботи мереж з технологією MPLS, програмна реалізація якого дає змогу досліджувати завантаженість мережевих елементів, аналізувати та оптимізувати характеристики мереж, а також досліджувати поведінку трафіка різних класів.

Ключові слова: імітаційний алгоритм, мережа, трафік, оптимізація характеристик

We describe a conceptual model developed simulation algorithm designed to simulate the networks with technology MPLS, software implementation which allows to study the workload of network elements, analysis and optimization characteristics of networks and study the behavior of different classes of traffic.

Keywords: imitation algorithm, network, traffic, optimizing performance

Вступ

При проектуванні комп'ютерних мереж з технологією MPLS (Multiprotocol Label Switching – багатопротокольна комутація за мітками) [1, 2] виникають такі проблеми: визначення типів та