УДК 004.056.55

УДОСКОНАЛЕННЯ АЛГОРИТМУ ШИФРУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ДЕТЕРМІНОВАНОГО ХАОСУ

Нікольський Є.С.

Науковий керівник - доц. каф. «Інформаційних систем», канд. техн. наук

Болтєнков В.О.

Алгоритми шифрування зображень широко застосовуються у мережах передачі даних та у системах зберігання даних.

Основним недоліком існуючих хаотичних алгоритмів шифрування на основі детермінованого хаосу зображень є їх низька криптостійкість до статистичних атак.

Для зменшення впливу цього недоліку на якість криптографічних систем можна застосовувати такі варіанти поліпшення алгоритмів:

додавання додаткових хаотичних систем в алгоритм для збільшення хаотичності траєкторії системи;

використання нетипових або нових хаотичних систем;

збільшення розрядності даних, що використовуються у хаотичних системах.

Базовим алгоритмом був вибраний алгоритм Ліу, який представлений у [1]. У цьому алгоритмі початкове зображення перетворюється у потік бінарних даних. Він маскується за допомогою псевдовипадкової послідовності ключа, яка створюється генератором ключа, та отримується зашифроване зображення. Генератор ключа керується двома логістичними картами, що залежать від початкових значень $(a^{(1)}, x_0, a^{(2)}, y_0)$. Ці значення являються секретними та використовуються як ключ шифрування.

Із-за ітеративності алгоритму логістична карта генерує вихідне значення, яке дуже сильно залежить від вхідного значення (тобто, ключа користувача), воно використовується для визначення системних параметрів другої карти. Друга логістична карта також сильно залежить від вхідного значення ключа та вихідного значення першої карти. Вихідне значення другої карти використовується для маскування бітів вхідного зображення.

Дешифрування відбувається аналогічно шифруванню – за допомогою ключа користувача та логістичних карт генерується потік символів ключа, який за допомогою операції XOR відновлює вхідне зображення.

Цей алгоритм був удосконалений наступним чином: 1) у генератор ключа були додані дві додаткових логістичних системи, що збільшило хаотичність траєкторії; 2) генератор

ключа у роботі використовує 16-розрядні числа замість 8-розрядних чисел, як це було в оригіналі алгоритму.

Для оцінки криптографічних характеристик якості системи використовується статистичний аналіз та аналіз чутливості до ключа. Для опору статистичним атакам зашифровані зображення повинні мати певні випадкові властивості. До методів статистичного аналізу можна віднести: побудову та аналіз гістограм, визначення коефіцієнтів кореляції між сусідніми пікселями та між початковими та відповідними зашифрованими зображеннями.

Гістограма будується для трьох кольорових каналів: червоного, зеленого та синього. Гістограма зашифрованого зображення повинна відрізнятися від гістограми початкового зображення та бути рівномірно розподіленою. Це значно утрудняє статистичний аналіз зображення.

Коефіцієнт кореляції для двох сусідніх пікселей обчислюється за формулою, що була взята у [2]:

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{\left[N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right] \times \left[N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right]}},$$

де x та y – півтонові значення кольорів двох сусідніх пікселей зображення, N – кількість пікселей зображення, які були відібрані для розрахунку коефіцієнта. Цей коефіцієнт кореляції можна обчислити для початкового та зашифрованого зображення та порівняти результати. Графік кореляції між сусідніми пікселями може бути побудований як для горизонтальних, так і для вертикальних рядів пікселей.

Схема шифрування повинна бути чутливою до ключа, тобто найменша зміна у ключі повинна приводити до значної зміни у вихідних даних. Для аналізу цього можна провести два тести.

Перший тест. Вибрати ключ 1 та ключ 2, який відрізняється від ключа 1 одним бітом. Зашифрувати зображення за допомогою ключів 1 та 2, та обчислити показник змінення зашифрованого зображення за формулою:

$$\frac{\Delta Y}{Y} = \frac{|[\mathrm{D}(X, K)]^n - [\mathrm{D}(X, K + \Delta K)]^n|}{Y},$$

де Y – зашифроване зображення, D – операція шифрування, X – початкове зображення, K – ключ, ΔK – невелика зміна ключа, n – кількість ітерацій при шифруванні.

Другий тест. Зашифрувати зображення ключем 1. Розшифрувати зображення за допомогою ключа 2. Обчислити показник змінення зображення.

У результаті тестування отримано, що тестове зображення, зашифроване удосконаленим алгоритмом, має меншу кореляцію пікселей (C_r =-0,03), ніж зображення, зашифроване оригінальним алгоритмом (C_r =0,1). Гістограми в обох випадках являються рівномірно розподіленими. Для аналізу чутливості до ключа був проведений перший тест (див. вище). Два зображення, отримані у результаті зашифровування тестового зображення з двома ключами з різницею у один біт, мають низький коефіцієнт кореляції (C_r =0,009). Таким чином, удосконалений алгоритм перевершує початковий за статистичними характеристиками. Це збільшує стійкість до статистичних атак.

СПИСОК ЛІТЕРАТУРИ

1. Liu S., Sun J., Xu Zh. An improved image encryption algorithm based on chaotic system. Journal of Computers, Vol. 4, No. 11, November 2009.

2. Pareek N.K. et al. Image encryption using chaotic logistic map. Image and Vision Computing 24, 2006.