УДК 681.142.2; 622.02.658.284; 621. 325

А.М. Ковальчук, М.Л. Навитка, Д.Д. Пелешко

ВИКОРИСТАННЯ АФІННИХ ПЕРЕТВОРЕНЬ В ШИФРУВАННІ І ДЕШИФРУВАННІ ДВОХ ЗОБРАЖЕНЬ

Робота присвячена модифікації алгоритму шифрування RSA на випадок шифрування та дешифрування одночасно двох зображень. Основним базисом модифікації є використання афінних перетворень та піксельних наборів двох зображень однакової розмірності. Розвитком запропонованої модифікації є додаткова можливість зашумлення, що дає можливість покращити криптографічну стійкість від несанкціонованого доступу.

Ключові слова: криптографія, зображення, шифрування, дешифрування, афінні перетворення, зашумлення зображення.

Вступ

Криптографія (від грецького kryptys — прихований і grбphein — писати) — наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри.

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що допускають використання обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. До таких алгоритмів відносять Twofish, IDEA, RC4 та ін [1].

Широкі академічні дослідження криптографії з'явились порівняно нещодавно — починаючи з середини 70-х, разом із появою відкритої специфікації стандарту DES (Data Encryption Standard) Національного Бюро Стандартів США (National Bureau of Standards, NBS), публікацій Діффі-Хелмана та публікації алгоритму RSA. Відтоді, криптографія перетворилась на загальнопоширений інструмент для передавання даних в комп'ютерних мережах та захисту інформації загалом. Сучасний рівень безпеки багатьох криптографічних методів базується на складності деяких обчислювальних задач, таких як розклад цілих чисел, або проблеми з дискретними логарифмами. В бага-

тьох випадках, існують докази безпечності криптографічних методів лише за умови неможливості ефективного розв'язання певної обчислювальної задачі. Тут окремим винятком є шифрування за схемою одноразових блокнотів.

У багатьох країнах прийнято національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжинами ключів 128, 192 і 256 біт. Алгоритм AES прийшов на зміну колишньому алгоритмові DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

RSA — криптографічна система з відкритим ключем. RSA став першим алгоритмом такого типу, придатним і для шифрування і для цифрового підпису. Алгоритм використовується у великій кількості криптографічних додатків. Безпека алгоритму RSA побудована на принципі складності факторизації. Алгоритм використовує два ключі - відкритий і закритий

По відношенню до зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [3, 4]. Однією з причин, через що контури залишаються в зображенні, наприклад, при шифруванні в системі RSA, є та, що шифрування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому, на контурі і на сусідніх до контура пікселах піднесеня до степеня значення яскравостей дає ще більший розрив. Тому актуальною завданням є така модифікація алгоритму RSA, яка б дозволила його використовувати стосовно зображень.

Постановка задачі

Нехай задано прямокутне зображення P ширини l і висоти h. Його можна розглядати як матрицю пікселів [2]

$$<\mathrm{dtp}_{i,j}>_{1\le i\le n,\ 1\le j\le m}. \qquad (1)$$

де $\mathrm{dtp}_{i,j}$ – піксел з координатами i та j, а n і m – число пікселів по ширині l та висоті h. В загальному випадку n і m є залежними від l та h, а тому більш коректним є запис

$$n = n(l)\ ,\ m = m(h). \qquad (2)$$

Матриці (1) у відповідність ставиться матриця кольорів (інтенсивностей

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

де $c_{i,j}$ – значення інтенсивності у напівтонових зображень піксела $\mathrm{dtp}_{i,j}$. Тобто має місце відповідність

$$P = \mathbf{P}_{l,h} = \left[\mathrm{dtp}_{i,j} \right]_{1 \le i \le n(l), 1 \le j \le m(h)} \to \mathbf{C}_{\mathbf{P}_{l,h}} = \left[c_{i,j} \right]_{1 \le i \le n(l), 1 \le j \le m(h)} \quad (4)$$

У випадку кольорових зображень $c_{i,j}$ треба розглядати як вектор основних характеристик кольорової палітри. Наприлад якщо задано зображення у 24-бітному форматі палітри RGB, то

$$\mathbf{c}_{i,j} = \{c_{i,j}^R, c_{i,j}^G, c_{i,j}^B\},$$

де $c_{i,j}^R, c_{i,j}^G, c_{i,j}^B$ - значення червоного, зеленого та синього кольорів піксела $\mathrm{dtp}_{i,j}$ відповідно. Тоді наведений нижче алгоритм треба застосувати до кожної характеристики окремо.

Уникнути збереження контурів при шифруванні зображення можна, шифруючи одночасно два зображення. Тоді математично завдання модифікації алгоритму шифрування RSA полягає у побудові перетворення вихідних зображень $\mathbf{C}_{\mathbf{P}_{1\,l,h}}$ та $\mathbf{C}_{\mathbf{P}_{2\,l,h}}$

$$\begin{cases} \mathbf{C}_{\mathbf{P}_{1\,l,h}} = \left[c_{i,j} \right]_{1 \le i \le n(l), 1 \le j \le m(h)} \\ \mathbf{C}_{\mathbf{P}_{2\,l,h}} = \left[c_{i,j} \right]_{1 \le i \le n(l), 1 \le j \le m(h)} \end{cases} \to \mathbf{C}'_{\mathbf{P}_{l,h}} = \left[c'_{i,j} \right]_{1 \le i \le n(l), 1 \le j \le m(h)}.$$

так, щоб на $\mathbf{C}'_{\mathbf{P}_{l,h}}$ не проступали контури $\mathbf{C}_{\mathbf{P}_{1\,l,h}}$ та $\mathbf{C}_{\mathbf{P}_{2\,l,h}}$.

Шифрування. Нехай $\mathbf{C}_1$ і $\mathbf{C}_2$ – матриці інтенсивностей двох зображень однакової розмірності. Нехай p і q пара довільних простих чисел. Виберемо числа

$$N = pq, \varphi(N) = (p-1)(q-1), \; ed \equiv \left(\mathrm{mod}\, \varphi(N)\right), \quad (5)$$

Шифрування здійснюється з використанням елементів рядків за наступною схемою:

з кожного рядка матриці зображення $\mathbf{C}_1$ вибирається значення інтенсивності кольору $x_i \in \mathbf{C}_1$, а з кожного рядка матриці зображення

$\mathbf{C}_2$ вибирається значення інтенсивності кольору $y_i \in \mathbf{C}_2$ і обчислюються наступні дві величини

$$\begin{cases} u_{i-1} = A_i x_{i-1} + B_i y_{i-1}; \\ v_{i-1} = C_i x_{i-1} + D_i y_{i-1}, \end{cases} \tag{6}$$

де $A_i\ D_i$ - $C_i\ B_i \neq 0$

$$\begin{cases} A_i \equiv A_0^i \pmod N, B_i \equiv B_0^i \pmod N; \\ C_i \equiv C_0^i \pmod N, D_i \equiv D_0^i \pmod N, \end{cases} \tag{7}$$

Тут $A_0 = q$, $B_0 = p$, $C_0 = e$, $D_0 = d$, $1 \leq i \leq n$, n - число пікселів в кожному рядку.

Величини $u_i v_i$, отримані з (6), записуються у два послідовні рядки зашифрованого зображення, кожне значення в один рядок.

Дешифрування. Умовою можливості дешифрування є виконання умови $A_i\ D_i$ - $C_i\ B_i \neq 0$. Тоді

$$x_{i-1} = \frac{D_i u_{i-1} - B_i v_{i-1}}{A_i D_i - C_i B_i}; \quad y_{i-1} = \frac{A_i u_{i-1} - C_i v_{i-1}}{A_i D_i - C_i B_i}.$$

Результати наведені на Рисунок1 – Рисунок5.

Рисунок 1 – Перше початкове зображення

Рисунок 2 – Друге початкове зображення

 ISSN 1562-9945

Рисунок 3 – Зашифровані зображення

Рисунок 4 – Перше дешифроване зображення

Рисунок 5 – Друге дешифроване зображення

Шифрування і дешифрування з додатковим зашумленням. Шифрування здійснюється з використанням елементів рядків за наступною схемою: з кожного рядка матриці зображення C_1 вибирається значення інтенсивності кольору , а з кожного рядка матриці зображення C_2 вибирається значення інтенсивності кольору і обчислюються наступні дві величини

$$\begin{cases} u_{i-1} = A_i x_{i-1} + B_i y_{i-1} + f_{i-1}; \\ v_{i-1} = C_i x_{i-1} + D_i y_{i-1} + g_{i-1}, \end{cases}$$

де $A_i\ D_i$ - $C_i\ B_i \neq 0$ визначаються за (7)

Умовою можливості дешифрування є виконання умови $A_i\ D_i$ - $C_i\ B_i \neq 0$. Тоді

$$x_{i-1} = \frac{D_i\left(u_{i-1} - f_{i-1}\right) - B_i\left(v_{i-1} - g_{i-1}\right)}{A_i D_i - C_i B_i};$$

$$y_{i-1} = \frac{A_i\left(u_{i-1} - f_{i-1}\right) - C_i\left(v_{i-1} - g_{i-1}\right)}{A_i D_i - C_i B_i}.$$

Результати наведені на Рисунок4 – Рисунок6.

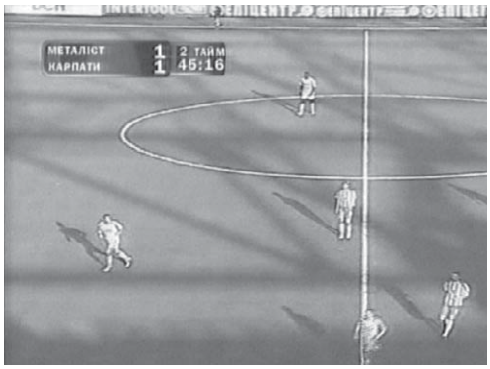

Рисунок 6 – Перше початкове зображення

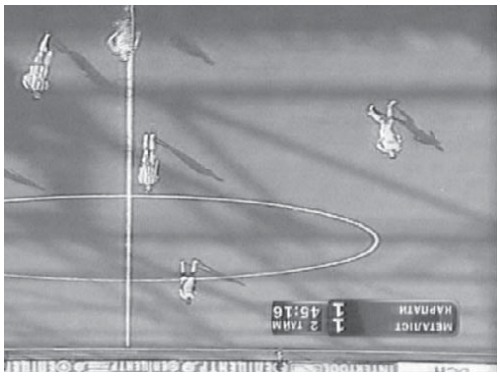

Рисунок 7 – Друге початкове зображення

Рисунок 8 – Зашифровані зображення.

ISSN 1562-9945

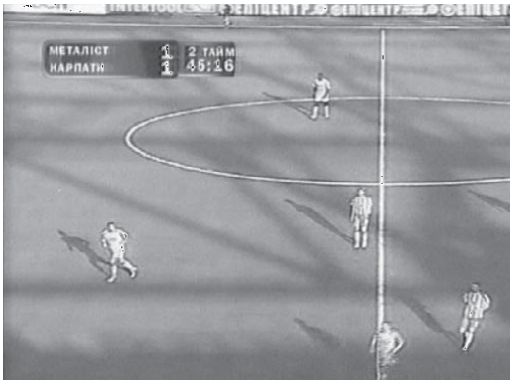

Рисунок 9 – Перше дешифроване зображення

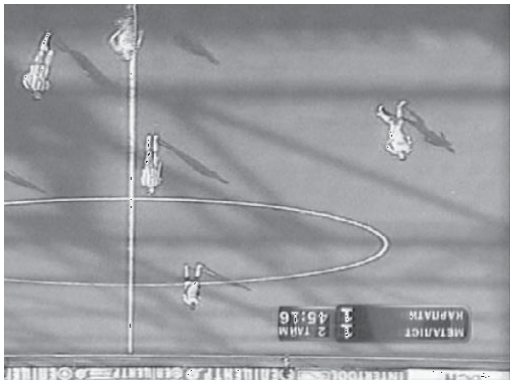

Рисунок 10 – Друге дешифроване зображення

Висновок

З порівняння Рис.2 і Рис.5 видно, що шифрування по одному рядку матриці зображення відрізняється від шифрування по трьох рядках цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Вказаний алгоритм може бути використаний при передачі графічних зображень. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дозволяють чітко виділяти контури.

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.

ЛІТЕРАТУРА

1. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с.
2. Б.Яне. Цифровая обработка изображений. – Москва, Техносфера , 2007.- 583с.
3. Ю.М. Рашкевич, Д.Д. Пелешко, А.М. Ковальчук, М.З. Пелешко. Модифікація алгоритму RSA для деяких класів зображень. Технічні вісті 2008/1(27), 2(28). С. 59 – 62.
4. Y.Rashkevych, A.Kovalchuk, D.Peleshko, M.Kupchak. 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