УДК 681.142.2; 622.02.658.284; 621. 325

Ю. Рашкевич, А. Ковальчук, Д. Пелешко
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ ДРОБОВО-ЛІНІЙНИМИ ФОРМАМИ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ АЛГОРИТМУ RSA

Запропоновано алгоритм шифрування зображень дробово-лінійними формами з використанням елементів алгоритму RSA як найстійкішого до несанкціонованого дешифрування сигналів стосовно зображень зі строго виділеними контурами.

The algorithm of encoding of the images by the linear-fractional forms with usage of members of algorithm RSA, as most nonperishable to unauthorized decoding of signals, concerning the images with strictly discharged contours is offered.

Вступ

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контуру вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [2].

Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [3, 4].

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 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.

Дробово-лінійні функції і форми

Загальна дробово-раціональна функція дійсної або комплексної змінної s має вигляд:

$$F(s) = \frac{B(s)}{A(s)} = \frac{b_0 s^m + b_1 s^{m-1} + \cdots + b_{m-1} s^1 + b_m}{a_0 s^n + a_1 s^{n-1} + \cdots + a_{n-1} s^1 + a_n}$$

де $A(s)$, $B(s)$ – поліноми чисельника й знаменника, a_i, bi – дійсні числа, m – порядок чисельника, n – порядок знаменника.

Поліноми дробово-раціональної функції можуть бути представлені у вигляді добутку біномів (розкладання багаточлена на співмножники). Тоді функція може бути подана у формі Боде

$$F(s) = \frac{b_0 (s - s_{b_1})(s - s_{b_2}) \ldots (s - s_{b_m})}{a_0 (s - s_{a_1})(s - s_{a_2}) \ldots (s - s_{a_n})}$$

де $s_{b_1}, s_{b_2}, \ldots,$ – корені рівняння $B(s) = 0$, $s_{a1} \ldots s_{an}$ – корінь характеристичного рівняння $A(s) = 0$.

Корені рівняння $B(s) = 0$ називають нулями дробово-раціональної функції $F(s)$, тому що

$$F(s_{b1} \ldots s_{bn}) = 0.$$

Корінь характеристичного рівняння $A(s) = 0$ називають полюсами дробово-раціональної функції, тому що

$$F(s_{a_1},\ldots,s_{a_n}) = \pm\infty .$$

Множина всіх дробово-раціональних функцій має властивість замкненості щодо обертання і композиції, тобто функція, обернена до дробово-раціональної функції, є дробово-раціональною, і композиція дробово-раціональних функцій є також дробово-раціональною (отже, на множині невироджених дробово-раціональних функцій виявляється структура некомутативної групи щодо композиції функцій як групової операції).

3.4.1. Шифрування і дешифрування з елементами алгоритму RSA дробово-лінійними функціями першого порядку по одному рядку матриці зображення

Дробово-лінійна функція першого порядку – це функція вигляду

$$y = \frac{ax + b}{cx + d}$$

тобто частка двох лінійних функцій. Дробово-лінійна функція — найпростіша серед раціональних функцій При $ad — bc = 0$ – зводиться до тотожної константи; якщо $ad — bc \neq 0$, але якщо $c = 0$, то дробово-лінійна функція зводиться до цілої лінійної функції $y = \alpha x + \beta$.

Якщо x набуває довільних комплексних значень (a, b, c и d — фіксовані комплексні числа), то дробово-лінійна функція здійснює взаємно однозначне й конформне відображення площини (доповненої точкою ∞) на себе, називане дробово-лінійним відображенням (це єдина аналітична функція, що володіє зазначеною властивістю). Дробово-лінійна функція характеризується також тим, що переводить прямі й кола, що лежать у комплексній площині, знову в прямі й кола. Будь-яке конформне відображення внутрішності кола на себе здійснюється за допомогою дробово-лінійної функції. Подвійне відношення чотирьох точок

$$\frac{x_4 - x_1}{x_4 - x_2} : \frac{x_3 - x_1}{x_3 - x_2}$$

є інваріантом дробово-лінійної функції.

Шифрування за одним рядком матриці зображення

Будемо вважати, що зображенню у відповідність ставиться матриця кольорів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \ldots & c_{1,m} \\ \ldots & \ldots & \ldots \\ c_{n,1} & \ldots & c_{n,m} \end{pmatrix}.$$

Для шифрування вибираються чотири послідовні точки матриці зображення $x = c_{i,j}, u = c_{i,j+1}$, $\eta = c_{i,j+2}, \tau = c_{i,j+3}$ $i = \overline{1,n}$, $j = \overline{1,m}$ і будуються перетворення:

$$y = \frac{Ax + B}{Cx + D}, v = \frac{Cu + B}{Au + D}, \xi = \frac{D\eta + B}{A\eta + C}, \varepsilon = \frac{D\tau + A}{B\tau + C}. \quad (1)$$

Отримані чотири значення записуються послідовно в один рядок зашифрованого зображення. Коефіцієнти ***A,B,C,D*** в (1) вибираються такими, щоб $\boldsymbol{AD - BC \neq 0, CD - AB \neq 0.}$

Дешифрування за одним рядком матриці зображення

Для дешифрування вибираються чотири послідовні точки матриці зашифрованого зображення $\boldsymbol{y, v, \xi, \varepsilon}$ і будуються обернені до (1) перетворення:

$$x = \frac{B - Dy}{Cy - A}, u = \frac{B - Dv}{Av - C}, \eta = \frac{B - C\xi}{A\xi - D}, \tau = \frac{A - C\varepsilon}{B\varepsilon - D}. \quad (2)$$

Отримані чотири точки записуються послідовно в один рядок дешифрованого зображення. Коефіцієнти ***A,B,C,D*** в (1) вибираються також такими, щоб $\boldsymbol{AD - BC \neq 0, CD - AB \neq 0.}$

Результати наведені на рис. 1 – 3.

Рис.1. Початкове зображення

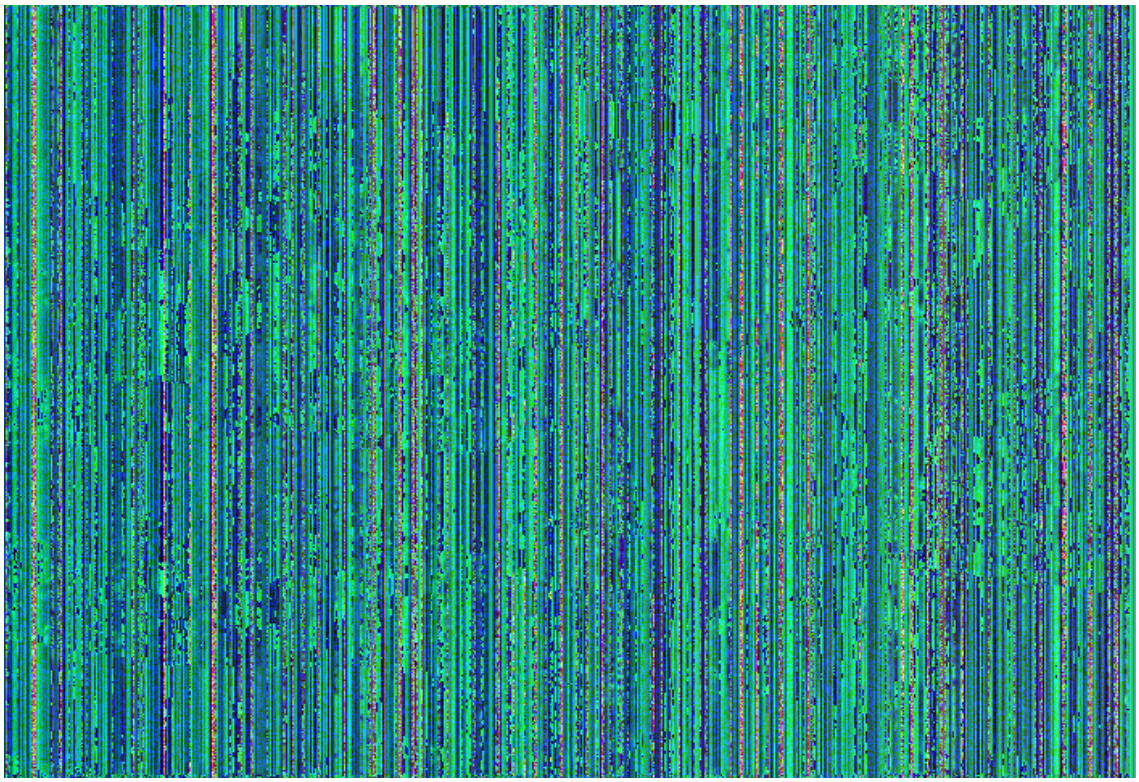

Рис. 2. Зашифроване зображення

Шифрування і дешифрування дробово-лінійними формами з елементами алгоритму RSA за чотирма рядками матриці зображення

Шифрування відбувається з використанням елементів чотирьох рядків за формулами (1), де $x = c_{i,j}, u = c_{i+1,j}$, $\eta = c_{i+2,j}, \tau = c_{i+3,j}$, $i = \overline{1,n}$, $j = \overline{1,m}$. Вибираються чотири елементи з однаковими

номерами, по одному з кожного рядка, так щоб в кожну четвірку кожний елемент був вибраний тільки один раз. Коефіцієнти ***A, B, C, D*** в (1) вибираються такими (елементами алгоритму RSA), щоб виконувалися умови $AD - BC \neq 0$, $CD - AB \neq 0$.

Рис. 3. Дешифроване зображення

Дешифрування проводиться за формулами оберненого перетворення (2) з тими самими коефіцієнтами.

Результати наведені на рис. 4 – 6.

Рис. 4. Початкове зображення

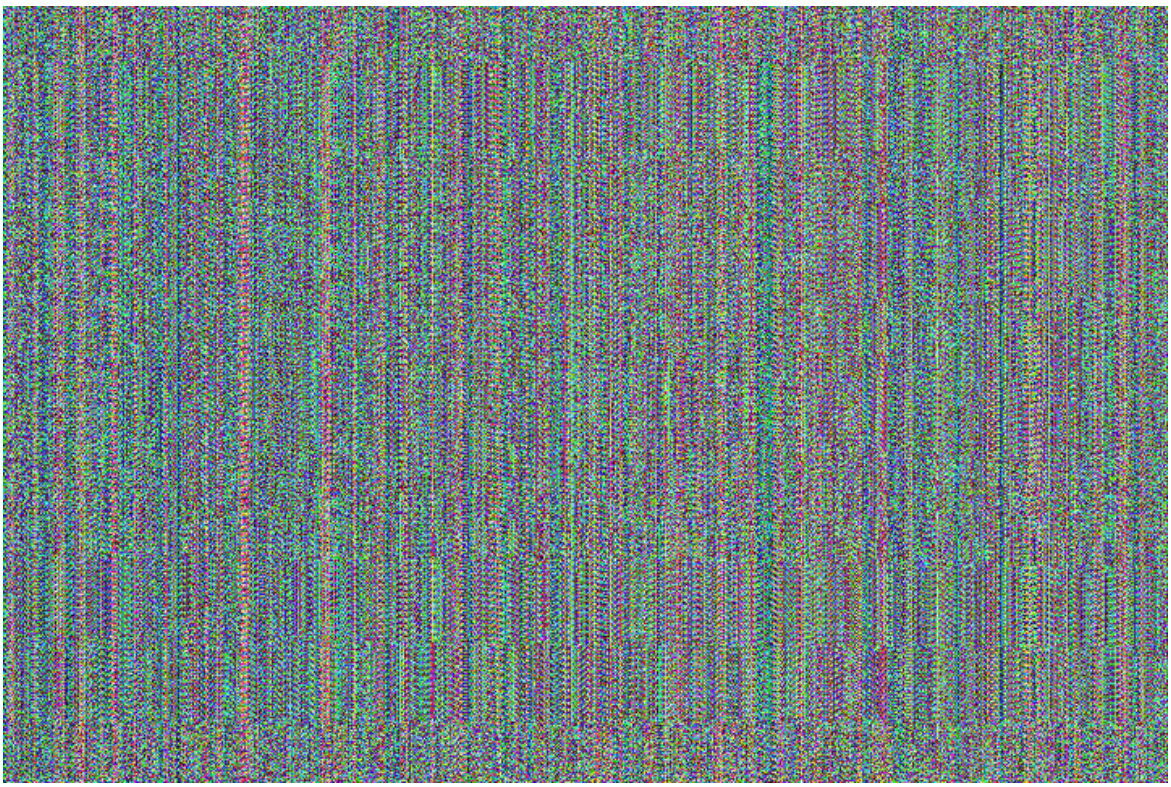

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Висновок

З порівняння рис. 2 і рис. 5 видно, що шифрування за одним рядком матриці зображення відрізняється від шифрування за трьома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дають

змогу 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.

Вказаний алгоритм може бути використаний при передачі графічних зображень.

1. Шнайер Б. 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.

УДК 681.3:519.15

В. Різник[*], Д. Скрибайло-Леськів, О. Ляхович
[*]Технологічно-природничий університет, м. Бидгощ (Польща)
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

СТРУКТУРНИЙ АНАЛІЗ МЕТОДІВ ОПТИМАЛЬНОЇ ПОБУДОВИ ЦИКЛІЧНИХ КОДІВ З ПОЛІПШЕНИМИ ХАРАКТЕРИСТИКАМИ

Досліджуються циклічні коди, побудовані на основі математичних конструкцій з унікальними комбінаційними властивостями – «ідеальних кільцевих в'язанок» (ІКВ) – та розглядаються методи оптимального синтезу за допомогою ІКВ циклічних кодів з поліпшеними можливостями щодо виправлення багаторазових помилок.

The cyclic coded design based on the mathematical constructions with special combinative properties, namely the "ideal ring bundles" (IRB)s are studied, and techniques for optimum synthesis of the cyclic codes with improved possibilities for correcting the multiple errors are regarded in this paper.

Вступ

Комбінаторні структури і методи комбінаторної оптимізації широко застосовують в інформаційних технологіях під час кодування, перетворення та пересилання даних, в інформаційно-вимірювальній та обчислювальній техніці, радіотехніці, зв'язку та суміжних галузях науки і техніки. Приклади постановки таких задач: проектування завадостійких систем кодування, розроблення ефективних технологій захисту цінних паперів від несанкціонованого доступу, удосконалення компонентів комп'ютерних систем, проектування радіосистем з високою роздільною здатністю. Тому актуальними є синтез математичних моделей систем та дослідження їх комбінаторних властивостей з метою поліпшення технічних характеристик систем та пристроїв комп'ютерної техніки та інформаційних технологій за такими показниками, як забезпечення достовірності інформації, підвищення надійності, функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем, зокрема вдосконалення інформаційних технологій для створення гарантоздатних автоматизованих систем перероблення інформації та