УДК 681.142.2; 622.02.658.284; 621. 325

А. Ковальчук
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

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

Запропоновано алгоритм шифрування зображень тернарними дробово-лінійними формами з використанням елементів шифрування RSA як найстійкішого до несанкціонованого доступу до сигналів стосовно зображень із строго виділеними контурами.

An image encryption algorithm ternary fractional-linear forms using elements of encryption RSA, as the most resistant to unauthorized access to signals for images is strictly dedicated circuits.

Вступ

Важливою характеристикою зображення є наявність у 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 контуру означає пошук найрізкіших 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.

Вважатимемо, що зображенню відповідає матриця кольорів

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

Тернарна дробово-лінійна форма має вигляд

$$t(x,y,z)=\frac{ax+by+fz+g}{cx+dy+ez+h}. \tag{1}$$

Використавши (1), виконаємо перетворення

$$\begin{cases} u=\dfrac{Ax+By+Fz+G}{Cx+Dy+Ez+H}; \\ v=\dfrac{Dx+Cy+Fz+G}{Bx+Ay+Ez+H}; \\ w=\dfrac{Ax+Dy+Ez+H}{Cx+By+Ez+H}, \end{cases} \tag{2}$$

де $A = P$, $B = Q$, $F = e$, $G = d$, $C = P$, $D = -Q$, $E = d$, $H = e$ – елементи стандартного алгоритму RSA, P, Q – довільні прості числа.

Обернене до (2) перетворення має вигляд

$$\begin{cases}(uC-A)x+(uD-B)y+(uE-F)z=G-uH;\\(vB-D)x+(vA-C)y+(vE-F)z=H-vG;\\(wC-B)x+(wB-D)y+(wE-F)z=G-wH,\end{cases} \tag{3}$$

і якщо

$$\delta=\begin{vmatrix}uC-A & uD-B & uE-F\\ vB-D & vA-C & vE-F\\ wC-B & wB-D & wE-F\end{vmatrix}\neq 0, \tag{4}$$

то

$$x=\frac{\delta_x}{\delta}, y=\frac{\delta_y}{\delta}, z=\frac{\delta_z}{\delta}, \tag{5}$$

де

$$\delta_x=\begin{vmatrix}G-uH & uD-B & uE-F\\ H-vG & vA-C & vE-F\\ G-uH & wB-D & wE-F\end{vmatrix}, \tag{6}$$

$$\delta_y=\begin{vmatrix}uC-A & G-uH & uE-F\\ vB-D & H-vG & vE-F\\ wC-B & G-uH & wE-F\end{vmatrix}, \tag{7}$$

$$\delta_z=\begin{vmatrix}uC-A & uD-B & G-uH\\ vB-D & vA-C & H-vG\\ wC-B & wB-D & G-uH\end{vmatrix}. \tag{8}$$

Шифрування за одним рядком матриці зображення

Шифрування відбувається з використанням елементів одного рядка матриці **C** за формулами (2), де $x=c_{i,j}, y=c_{i,j+1}, z=c_{i,j+2}, i=\overline{1,n}, j=\overline{1,m}.$ Вибираються три сусідні елементи рядка матриці так, щоб кожний елемент було вибрано тільки один раз і тільки в одну трійку.

Дешифрування відбувається за формулами оберненого перетворення (5) – (8) з коефіцієнтами, обчисленими за алгоритмом RSA.

Результати шифрування і дешифрування наведені на рис. 3.35 – 3.37.

Рис. 1. Початкове зображення

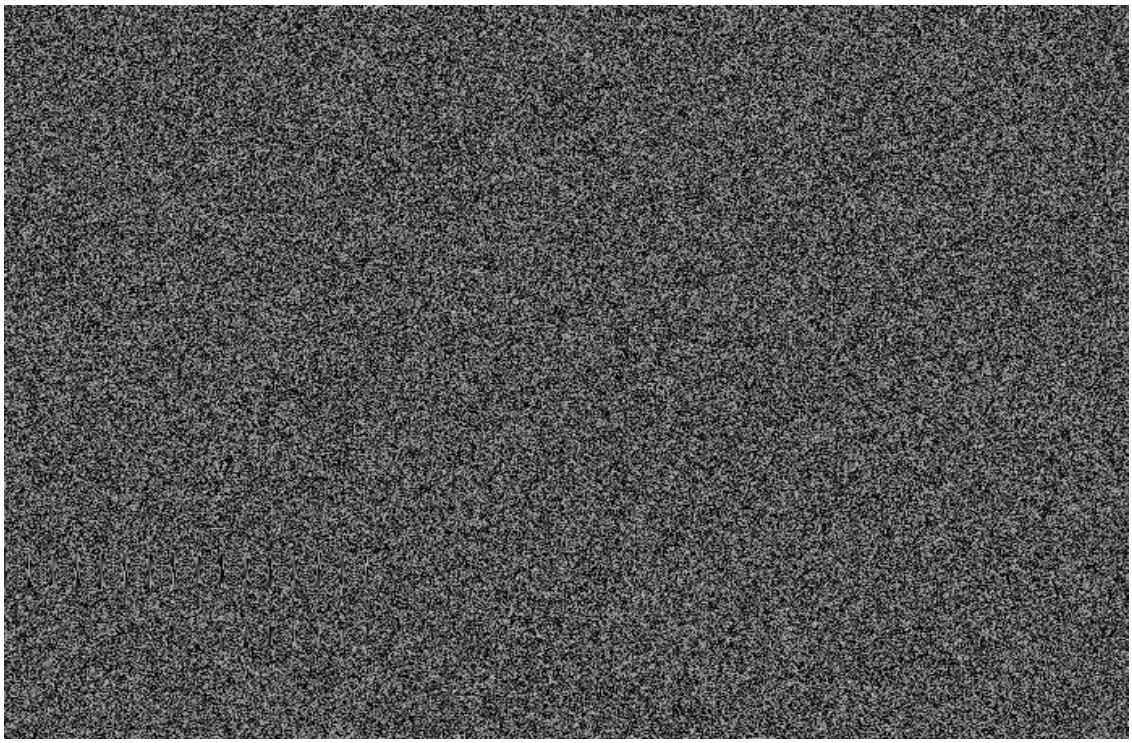

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування за трьома рядками матриці зображення

Шифрування відбувається з використанням елементів трьох рядків за формулами (2), де $x = c_{i,j}, y = c_{i+1,j}$, $z = c_{i+2,j}$, $i = \overline{1,n}$, $j = \overline{1,m}.$ Вибирають три елементи з однаковими номерами, по одному з кожного рядка так, щоби в кожну трійку кожний елемент було вибрано тільки один раз.

Дешифрування відбувається за формулами оберненого перетворення (5) – (8) з коефіцієнтами *A = P, B = Q, F = e, G = d, C = P, D = -Q, E = d, H = e.*

Результати шифрування і дешифрування наведені на рис. 4 – 6.

Рис. 4. Початкове зображення

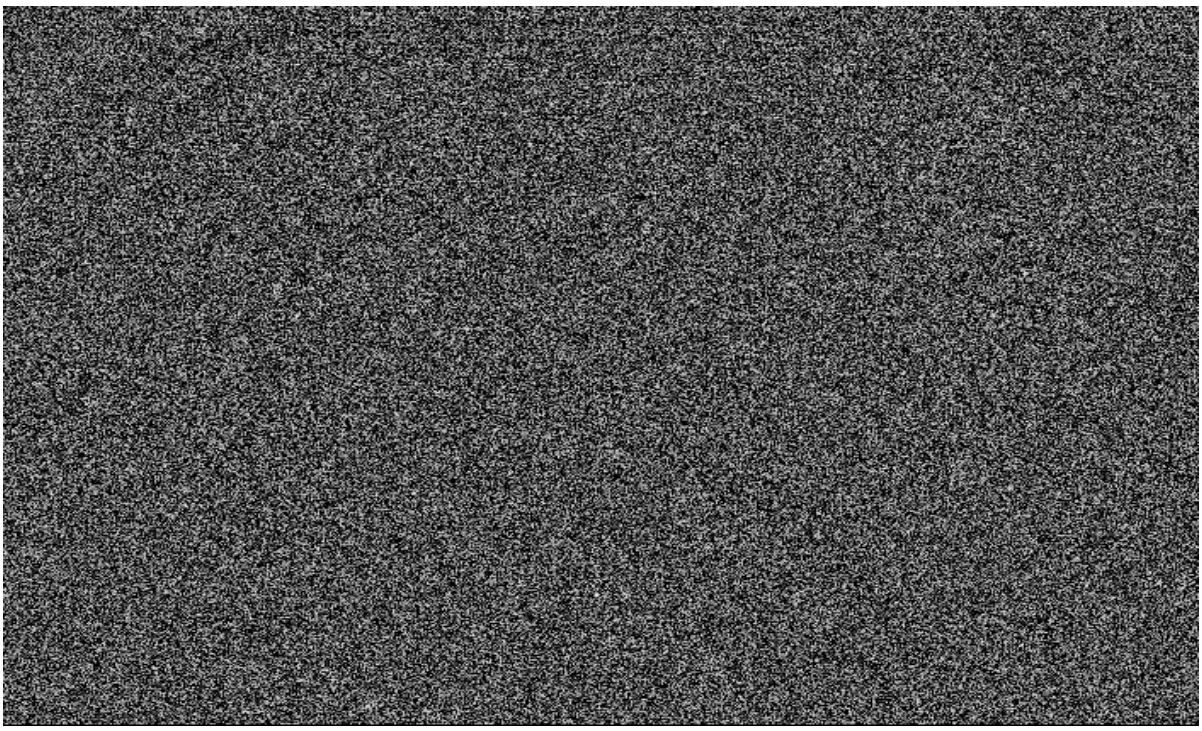

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Висновок

З 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 найбільшого ефекту 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 можна використати для 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 004.83; 004.89

Я. Ковівчак, Ю. Кущев
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

ПРОГРАМНИЙ ЗАСІБ ВІДОБРАЖЕННЯ ПРОСТОРОВО-ЧАСОВИХ ДАНИХ

Наведено основні можливості та функціональні особливості програмного продукту опрацювання та візуалізації просторово-часових даних. Показано переваги розробленого програмного пакета порівняно з наявними засобами побудови відображень просторових даних.

The basic features and functional features of the software processing and visualization of spatial-temporal data is proposed. The advantage of developed software package to existing means of constructing maps of spatial data.

Вступ

Використання сучасної техніки і новітніх інформаційних технологій у повсякденній діяльності людини пов’язане з опрацюванням великої кількості даних. Цей процес переважно відбувається без безпосередньої участі людини, і його кінцевою метою є практична реалізація необхідного набору функцій відповідного технічного обладнання.

З розвитком науки і техніки зростає складність проблем, які необхідно розв’язувати, а отже, і обсяги оперування даними. Для полегшення цього процесу дані подаються в наочній формі за допомогою графіків, діаграм, багатовимірних залежностей. Це спрощує аналіз даних, отримання потрібної інформації та прийняття необхідних рішень.

Всі процеси у навколишньому світі мають часовий вимір, тому отримані і опрацьовані дані відповідають тільки певному поточному моменту часу і характеризують процес лише відповідно до нього. На практиці в системах реального часу існує необхідність отримувати, опрацьовувати та відображати в різних формах великі обсяги даних у реальному часі їх надходження. Також в складних швидкоплинних або тривалих процесах фізичних об’єктів у різних масштабах реального часу виникає потреба у проведенні всебічного, багатоаспектного опрацювання та відображення отриманих даних. Як правило, ці дані мають просторово-часовий характер, що значно ускладнює завдання (рис. 1). Для розв’язання такого класу задач необхідно розробляти програмні засоби, які здатні не тільки швидко обробляти велику кількість даних, а і візуалізовувати їх без значних затрат апаратних ресурсів. З розвитком комп’ютерної техніки вирішення цієї проблеми стало можливим.