4. Ashby W. R. Principles of the Self-Organizing Dynamic System / W. R. Ashby // Journal of General Psychology. – 1947. – v. 37. — p. 125—128. 5. Хакен Г. Синергетика. Иерархия неустойчивостей в самоорганизующихся системах и устройствах / Г. Хакен. – М.: Мир, 1985. 6. Пригожин И. Порядок из хаоса. Новый диалог человека с природой: Пер. с англ. / И. Пригожин, И. Стенгерс. – М.: Эдиториал УРСС, 2003. – 312 с. 7. Хакен Г. Информация и самоорганизация. Макроскопический подход к сложным системам: Пер. с англ. / Г. Хакен. – М.: КомКнига, 2005. – 248 с. 8. Кравець П.О. Самоорганізація мультиагентної системи з локальними зв'язками / П.О. Кравець // Праці 12-ї науково-технічної конференції «Системний аналіз та інформаційні технології». – 25 – 29 травня 2010 р. – Київ: Навчально-науковий комплекс „Інститут прикладного системного аналізу" Національного технічного університету України „Київський політехнічний інститут". – С. 265. 9. Laywine C.F. Discrete Mathematics Using Latin Squares / C.F. Laywine, G.L. Mullen. – Wiley & sons inc., 1998. – 303 p. 10. Граничин О.Н. Введение в методы стохастической аппроксимации и оценивания: Учеб. пособие / О.Н. Граничин. – СПб.: Издательство С.-Петербургского университета, 2003. – 131 с.

УДК 01.05.02; 05.13.06; 05.13.21

Л. Фабрі, А. Ковальчук, Мар'яна Ступень
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ КВАДРАТИЧНИХ ФРАКТАЛЬНИХ АЛГОРИТМІВ

Запропоновано застосування квадратичних фрактальних перетворень до шифрування і дешифрування зображень в градаціях сірого кольору.

Ключові слова: шифруваня, дешифрування, фрактальний алгоритм, зображення

The use of quadratic fractal transforms to encryption and decryption of images in grayscale color.

Keywords: shyfruvanya, decoding, fractal algorithm, image

Вступ

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура 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].

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 грунтується на піднесенні до степеня за модулем деякого натурального числа. При цьому на контурі і на сусідніх до контура пікселах піднесеня до степеня значення яскравостей дає ще більший розрив.

Існують різні алгоритми, які виділяють контури, наприклад, відстежуючі алгоритми. Відстежуючі алгоритми грунтуються на тому, що на зображенні відшукується об'єкт (точка об'єкта, яка зустрілася першою) і контур об'єкта відстежується і векторизується. Перевагою цього алгоритму є його простота, до недоліків можна віднести їх послідовну реалізацію і деяку складність при пошуку і обробці внутрішніх контурів. Приклад такаго алгоритму – "алгоритму жука" – наведено на рис.1.

Жук починає рух з білої області у напрямку до чорної. Як тільки він потрапляє на чорний елемент, він повертає ліворуч і переходить до наступного. Якщо цей елемент білий, то жук повертає праворуч, інакше – ліворуч. Процедура повторюється доти, поки жук не повернеться у вихідну точку. Координати точок переходу з чорного на біле і з білого на чорне і описують контур об'єкта.

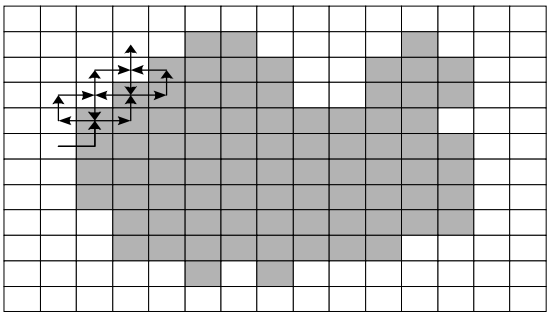

Рис. 1. Схема роботи відстежуючого алгоритму «жука»

Надалі вважатимемо, що зображенню відповідає матриця кольорів

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

Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [3, 4]. У [4] для шифрування – дешифрування зображень в градаціях сірого було запропоновано використовувати лінійні фрактальні перетворення. Тут для шифрування – дешифрування таких зображень пропонується використовувати квадратичні фрактальні перетворення.

Шифрування і дешифрування за одним рядком матриці зображення

Нехай P, Q –пара довільних простих чисел. Шифрування відбувається поелементно з використанням квадратичного фрактального перетворення елементів матриці зображення C за формулами:

$$x_n^{(k)} = P(x_n^{(k-1)} + f(n))^2 - Q \ , \quad n = 1, 2, \dots, N_0, \quad (2)$$

де N_0 – число елементів у рядку, $f(n)$ – функції зашумлення, k – номер фрактальної ітерації, $x_n^{(0)} = x_n$.

Дешифрування проводиться у зворотному порядку за формулами

$$x_n^{(k-1)} = \sqrt{\left(x_n^{(k)} + Q\right)/P \ - f(n))} \ , \quad n = 1, 2, \dots, N_0 \quad (3)$$

Результати наведені на рис. 2–4.

Шифрування і дешифрування за двома рядками матриці зображення

Нехай P, Q, R, T – чотири довільні простих числа. Шифрування відбувається поелементно з використанням квадратичного фрактального перетворення елементів двох послідовних рядків матриці зображення C за такими формулами:

$$x_n^{(k)} = P(x_n^{(k-1)} + f(n))^2 - Q \ , \quad n = 1, 2, \dots, N_0 \ , \quad (4)$$

$$y_n^{(k)} = R(y_n^{(k-1)} + g(n))^2 - T \ , \quad n = 1, 2, \dots, N_0 \ , \quad (5)$$

де N_0 – число елементів у рядку, $f(n)$, $g(n)$ – функції зашумлення, k – номер фрактальної ітерації, $x_n^{(0)} = x_n$, $y_n^{(0)} = y_n$.

Рис. 2. Початкове зображення

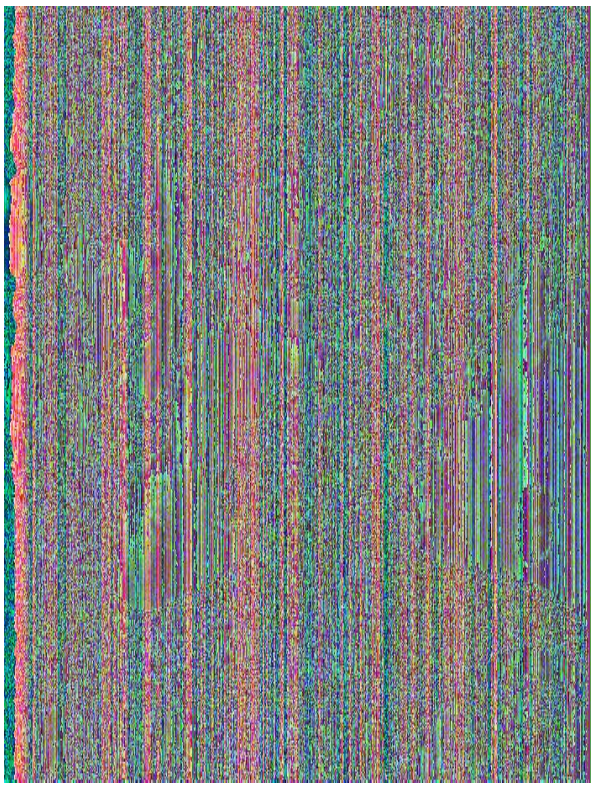

Рис. 3. Зашифроване зображення

Рис. 4. Дешифроване зображення

Дешифрування проводиться у зворотньому порядку за формулами

$$x_n^{(k-1)} = \sqrt{\left(x_n^{(k)} + Q\right)/P \; - f(n))}\,, \quad n = 1, 2, \ldots, N_0 \tag{6}$$

$$y_n^{(k-1)} = \sqrt{\left(y_n^{(k)} + T\right)/R \ - g(n))}\ , \quad n = 1, 2, \ldots, N_0 \qquad (7)$$

Результати наведено на рис. 5 – рис. 7. Очевидно, що шифрування і дешифрування істотно залежить від вибору простих $\boldsymbol{P}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{T}$, а також від числа фрактальних ітерацій.

Рис. 5. Початкове зображення

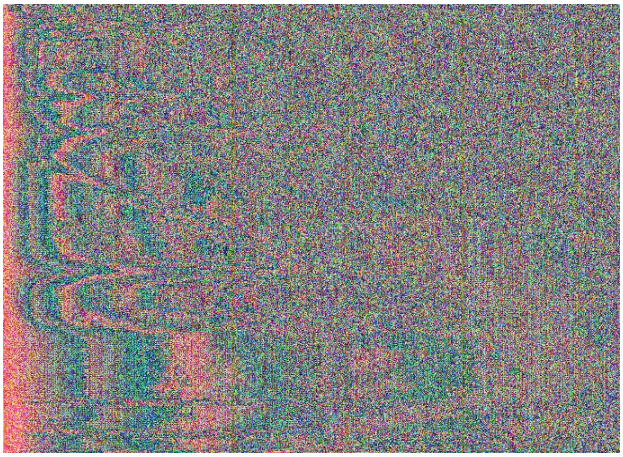

Рис. 6. Зашифроване зображення

Рис. 7. Дешифроване зображення

Висновок

З порівняння рис. 3 і рис. 6 видно, що шифрування за одним рядком матриці зображення відрізняється від шифрування за двома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Дешифровані зображення в обох випадках є візуально еквівалентними. Зашифровані зображення відрізняються структурно і за кольором. Вказані алгоритми можуть бути використані для передавання графічних зображень і можуть давати задовільний результат стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дають змогу чітко виділяти контури. Окрім того, підвищується стійкість шифрування, оскільки для шифрування і дешифрування використовуються довільні прості числа, які можуть бути доволі великими. А від цього залежить стійкість криптографічного алгоритму.

Обидва типи запропонованих алгоритмів шифрування – дешифрування можна використовувати і стосовно кольорових зображень. Однак, незалежно від типу зображення, можуть виникати проблеми при розв'язуванні відповідних алгебраїчних неоднорідних лінійних систем рівнянь.

1. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с. 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. Фабрі Л., Ковальчук А., Ступень М. Застосування фрактальних алгоритмів для шифрування і дешифрування зображень // Вісник НУ «Львівська політехніка», «Комп'ютерні науки та інформаційні технології». – №672. – С. 262–267.

УДК 004.032.026

П. Тимощук
Національний університет "Львівська політехніка",
кафедра САП

МОДЕЛЮВАННЯ ОБРОБКИ KWTA-НЕЙРОННОЮ СХЕМОЮ ЗМІННИХ ДИСКРЕТИЗОВАНИХ СИГНАЛІВ

Описується математична модель KWTA-нейронної схеми ("K-winners-take-all"), призначеної для ідентифікації K максимальних серед N невідомих, змінних у часі дискретизованих сигналів, де $1 \le K < N$. Для коректного функціонування моделі динамічний зсув вхідних сигналів протягом перехідних процесів повинен змінюватись набагато швидше, ніж вхідні сигнали. Представлено відповідні результати комп'ютерного моделювання.

Ключові слова: математична модель, KWTA-нейронна схема, дискретизований сигнал, динамічний зсув, комп'ютерне моделювання.

Mathematical model of discrete-time KWTA-neural circuit (K-winners-take-all) that can identify K maximal among N unknown, variable in time sampled signals, where $1 \le K < N$ is described. In order to have correct model functioning a dynamic shift of input signals should be changed much faster than input signals during transients. Corresponding computer modeling results are given.

Keywords: mathematical model, KWTA-neural circuit, sampled signal, dynamical shift, computer simulation.

1. Вступ

Як відомо, нейронні мережі типу "K-winners-take-all" (KWTA-мережі) здійснюють вибір K серед N елементів, де $1 \le K < N$, з більшими значеннями активаційних функцій, ніж у решти $N - K$ елементів. Коли K дорівнює одиниці, KWTA-мережа є мережею типу "Winner-takes-all" (WTA-мережею), яка може розрізняти нейрон з максимальною активацією [5, 8, 9]. Вибір K найбільших елементів з множини даних N дійсних чисел є ключовою задачею мереж прийняття рішень, розпізнавання образів, пов'язаних пам'ятей і конкуруючого навчання [10, 12]. Задачі такого типу зустрічаються під час розв'язання задач класифікації і застосовуються для розроблення класифікаційних нейронних мереж, для розв'язання задач розпізнавання і класифікації зразків [4]. KWTA-мережі застосовуються в телекомунікації, особливо для керування пакетними перемикачами даних [1]. KWTA-механізми мають важливі застосування у машинному навчанні, зокрема, при розв'язанні задач класифікації k найближчих об'єктів, кластеризації k значень та ін. [3, 6].

Існує низка нейронних мереж типу "K-winners-take-all", які мають як свої переваги, так і обмеження. Так, наприклад, динамічна система з глобальною збіжністю до єдиних стабільних станів рівноваги пропонується в [7]. Нейромережева схемотехнічна реалізація системи містить N комірок, представлених підсилювачами, глобальним зворотним зв'язком і щонайбільше 2N взаємозв'язками, де N – кількість входів. Конструюється і тестується числовими методами застосування мережі (так званий "К-селектор"), сигнали якого визначають К найбільших елементів