Система також має низку недоліків, які є результатом не стільки проектування, скільки результатом недоліків самої СУБД. Один з основних недоліків – це недостатній захист інформації через неможливість введення ролей. СУБД передбачає використання паролів, але це, на нашу думку, зовсім не вирішує поставленої проблеми перш за все тому, що такий підхід негнучкий у самій своїй основі. Він не забезпечить захист інформації у тому плані, що не дасть розподілу прав маніпулювання даними і роботи з об'єктами бази даних (тобто бухгалтерія і офіціант у разі правильного введення паролю для їх груп з однаковими правами можуть змінювати інформацію у базі даних).

Існує можливість розширення розробленої системи, якщо виникне така необхідність. Це дасть змогу використовувати систему не лише в сфері автоматизації обслуговування клієнтів, а й охопити весь процес діяльності закладів ресторанного бізнесу. Сьогодні розроблена система працює лише для внесення даних про замовлення, їх обробки, оплаті по рахунках. Можливо розширити систему, якщо додати підсистему доставки продукції в ресторан, підсистему постійних клієнтів (знижки та бонуси), підсистему приготування страв та напоїв (розрахунок пропорцій інгредієнтів на одну порцію страви чи напою) і таке інше.

1. Мацелюх А.В. Актуальні проблеми підвищення професійного рівня працівників сфери послуг // Збірник матеріалів науково-практичної конференції "Краєзнавчі ресурси регіону у створенні сучасної туристичної інфраструктури для відпочинку та оздоровлення людей". – Львів: ЛІЕТ 2007. – С. 22–26. 2. ДСТУ 4281: 2006 Заклади ресторанного господарства. Класифікація. 3. Стеченко Д.М., Чмир О.С. Методологія наукових досліджень: Підручник. – 2-ге вид. – К.: Знання, 2007. – С.317–318. 4. ГОСТ 30523. Услуги общественного питания. Общие требования.

УДК 004.8; 932.72; 511; 512; 004.932; 004.932.4

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

ЗАСТОСУВАННЯ ФРАКТАЛЬНИХ АЛГОРИТМІВ ДЛЯ ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ

Запропоновано застосування алгоритму фрактальних перетворень до шифрування і дешифрування зображень з чітко виділеними контурами.

Ключові слова: фрактал, шифрування, дешифрування, контур.

An application of fractal transformation algorithm to encrypt and decrypt image with clearly labeled contours.

Keywords: fractal, encryption, decryption, contour.

Вступ

Вважатимемо, що зображенню відповідає матриця кольорів

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

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 зберігають контури на різко флуктуаційних зображеннях [3, 4].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контуру 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 піднесеня до степеня значення яскравостей дає ще більший розрив.

Фрактал (лат. fractus – подрібнений, дробовий) – нерегулярна, самоподібна структура. В широкому розумінні фрактал означає фігуру, малі частини якої в довільному збільшенні є подібними до неї самої. Термін “фрактал” ввів в 1975 році Бенуа Мандельброт.

Коротко зупинимося на застосуванні фракталів:

1. Генерування зображень природних об’єктів (геометричні фрактали застосовуємо для одержання зображень дерев, кущів, берегових контурів та ін.)

2. Алгебраїчні та стохастичні фрактали застосовуємо для побудови зображень ландшафтів, поверхонь, текстури, зображення морів на картах, розфарбування моделей біологічних об’єктів.

3. В механіці рідин фракталами добре описувати динаміку турбулентності складних потоків, моделювати полум’я, візуалізувати пористість матеріалів (наприклад, у нафтохімії).

4. В біології фракталами моделюємо популяції, біосенсорні взаємодії, процеси в середині організму людини і тварин, наприклад, серцебиття, процеси дихання.

5. Фрактальні антени із застосуванням фрактальної геометрії застосовуються для проектування антенних пристроїв. Вперше таке застосування запропонував американський інженер Натан Коен, який проживав у місті Бостоні (тут було заборонено встановлення на будинках зовнішніх антен). Тоді Натан Коен вирізав із алюмінієвої фольги фігуру у вигляді кривої Коха і наклеїв її на лист паперу та під’єднав до приймача телевізійних радіохвиль. Виявилося, що така фрактальна антена працює не гірше від спеціально сконструйованих громіздких антен. І хоч фізичні принципи такої фрактальної антени і досі ретельно не вивчені, це дозволило Коену заснувати власну компанію і налагодити серійний випуск фрактальних антен.

6. Стиснення зображень на основі створених алгоритмів за допомогою фрактальних моделей. Метод Майкла Барнслі застосовується в Microsoft Encarta.

7. Децентралізовані мережі і системи, призначені для використання IP-адрес у мережі Netsukuku, використовують стиснення інформації на основі фрактальних моделей для компактного зберігання інформації про вузли мережі. Кожен вузол мережі Netsukuku зберігає 4 кб інформації про стан сусідніх вузлів і при цьому будь-який новий вузол приєднується до загальної мережі без необхідності централізованого регулювання IP-адрес, що характерно для сучасної мережі Інтернет. Принцип фрактального стиснення інформації гарантує цілком децентралізовану, а отже і максимально усталену (стабільну) роботу усієї мережі.

8. Прогнозування погоди. Сьогодні за допомогою супутників стало можливим збирати інформацію про атмосферний тиск і рух повітряних мас. Найпотужніший комп’ютер здатен точно передбачити погоду тільки в глобальному масштабі. Для точних локальних прогнозів потрібна обробка більшої кількості даних, що поки неможливо.

9. Конвертація графічного зображення у фрактальну музику [5]. Для цього фрактал перетворюють на двовимірну палітру (координати: висота і час), причому може враховуватись як графічне розміщення точок, так і їх колір, наприклад, для зміни тембру.

Фрактальна компресія – алгоритм із втратою інформації. Він з’явився у 1992 році. Алгоритм дає змогу компактно задавати складні структури. Фрактальні алгоритми забезпечують вдале співвідношення між коефіцієнтом стиснення та якістю і володіють унікальною властивістю деталізації при довільному масштабуванні.

Фрактальні алгоритми можна застосовувати і для шифрування і дешифрування зображень.

Шифрування і дешифрування за одним рядком матриці зображення

Нехай P, Q – пара довільних простих чисел. Шифрування відбувається поелементно з використанням фрактального перетворення матриці зображення $\boldsymbol{C}$ за такими формулами:

$$x_n = Px_{n-1} - Q, \quad n = 1,\ 2,\ \ldots,\ N_0, \tag{2}$$

де числа P, Q – задані, N_0 – число елементів в рядку.

Дешифрування проводиться у зворотній послідовності за формулами

$$x_{n-1} = (x_n + Q)/P, \quad n = 1,\ 2,\ \ldots,\ N_0. \tag{3}$$

Результати наведено на рис. 1–3.

Рис. 1. Початкове зображення

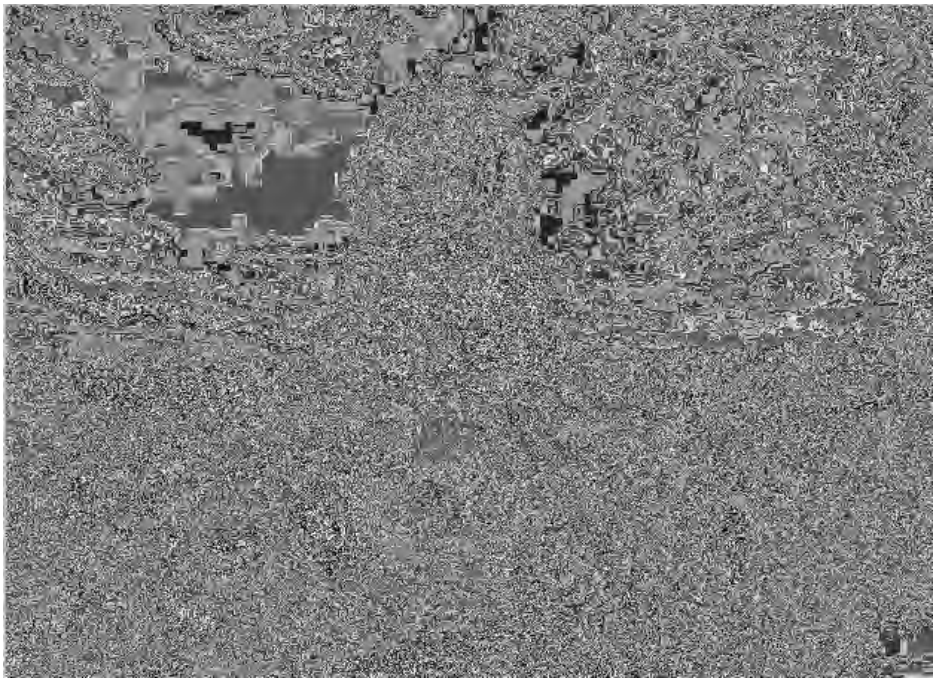

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування і дешифрування за двома рядками матриці зображення

Нехай P,Q,R,T – чотири довільні прості числа. Шифрування відбувається поелементно з використанням фрактального перетворення матриці зображення $\boldsymbol{C}$ за такими формулами:

$$x_n = Px_{n-1} - Q, \quad n = 1,\ 2,\ \ldots,\ N_0 \tag{4}$$

$$y_n = Ry_{n-1} - T, \quad n = 1,\ 2,\ \ldots,\ N_0 \tag{5}$$

де відповідно числа P,Q,R,T задані, N_0 – число елементів у рядку.

Дешифрування проводиться у зворотній послідовності за формулами

$$x_{n-1} = (x_n + Q)/P, \quad n = 1,\ 2,\ \ldots,\ N_0 \tag{6}$$

$$x_{n-1} = (x_n + T)/R, \quad n = 1,\ 2,\ \ldots,\ N_0 \tag{7}$$

Результати наведено на рис. 4–6.

Рис. 4. Початкове зображення

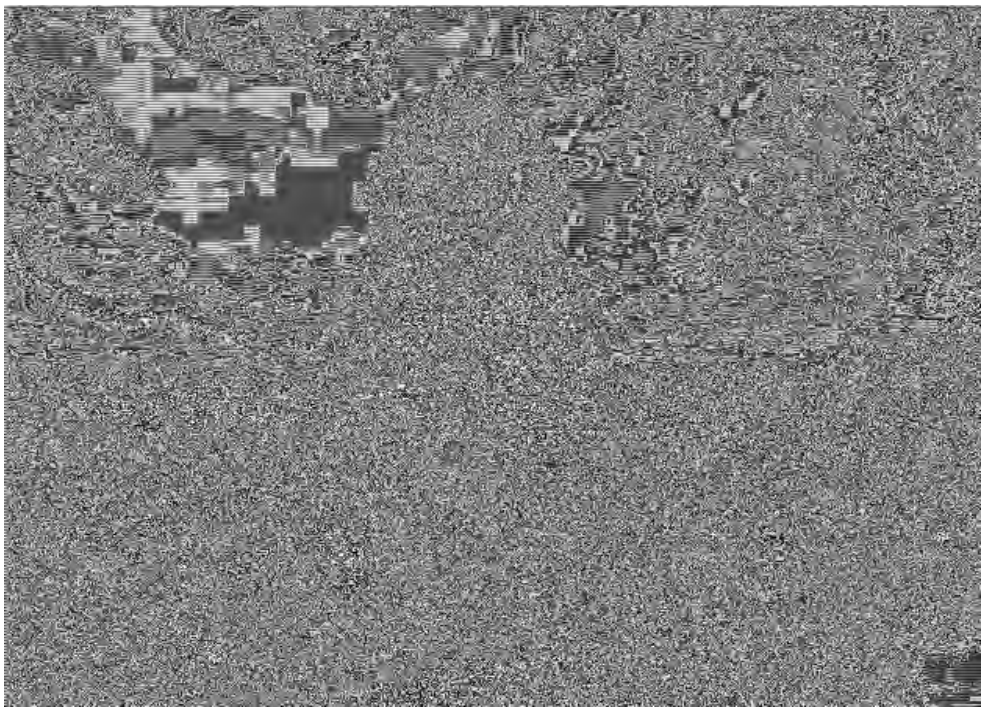

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Висновок

Порівнюючи рис. 2 і 5, видно, що шифрування за одним рядком матриці зображення відрізняється від шифрування за двома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Але дешифроване зображення в першому випадку (рис. 3) виглядає кращим від зображення (рис. 6) дешифрованого за другим алгоритмом. Відрізняються також зашифровані зображення структурно і за кольором. Вказані алгоритми можна використати для передавання графічних зображень і застосовувати до будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень з чітко виділеними контурами.

Обидва типи модифікацій без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зростає розмір шифрованого зображення.

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. – P. 469–473. 5. http://timara.con.oberlin.edu/~gnelson/mp3s/Long.mp3s.html.

УДК 681.3.06(075)

О. Кузьмін, О. Мицько, В. Грицак
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

КЛАСИФІКАЦІЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ У БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

Наведено класифікацію протоколів маршрутизації в сенсорних мережах. Описано основні їх властивості, переваги та недоліки.

In this article were described the classification routing protocols in Wireless Sensor Network. The basic properties, advantages and lacks are described.

Вступ

Безпровідні сенсорні мережі (Wireless Sensor Network*)* – це нові технології в галузі телекомунікацій та комп’ютерних мереж. Ключовим елементом WSN є сенсори, які реєструють зміни певних параметрів, наприклад, температури, тиску, вологості повітря, звуку, магнітних полів, радіації і т.п. WSN повинна задовольняти такі критерії:

• покривати задану територію і виконувати покладені на неї завдання з високою надійністю;

• сенсори, які входять до її складу, повинні самоорганізовуватися в бездротову мережу, через яку передається інформація з необхідною швидкістю без втрат;

• споживати мінімально можливу кількість енергії і при цьому працювати якнайдовше;

• швидко реагувати на події в зоні покриття;

• мати найменшу вартість.

Досягнення цих вимог значною мірою залежить від протоколів взаємодії між сенсорами та алгоритмів маршрутизації, які вони підтримують.

Метою роботи є проведення класифікації протоколів маршрутизації у WSN, їх системного аналізу та висвітлення переваг і недоліків кожного з них.

Характеристики протоколів маршрутизації у WSN

WSN призначені для контролю навколишнього середовища. Основне завдання бездротового сенсорного вузла – сприймати й отримувати дані з певної області, обробляти їх і передавати його приймачеві, в якому розташований ужиток. Забезпечення прямого зв’язку між давачем і приймачем