**УДК 01.05.02; 05.13.06; 05.13.21**

**[1]А. Ковальчук, [2]І. Цмоць, [2]М. Ступень**
Національний університет "Львівська політехніка",
[1]кафедра інформаційних технологій видавничих систем,
[2]кафедра автоматизованих систем управління

# КУБІЧНІ І ЛІНІЙНІ ФРАКТАЛИ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA В ШИФРУВАННІ І ДЕШИФРУВАННІ ЗОБРАЖЕНЬ



**Запропоновано застосування кубічних фрактальних перетворень до шифрування і дешифрування зображень у градаціях сірого кольору з використанням елементів алгоритму RSA.**

**Ключові слова: шифрування, дешифрування, фрактальний алгоритм, зображення**

**Proposed application of cubic fractal changes to the encryption and decryption, grayscale color using elements of the RSA algorithm.**

**Key words: encryption, decryption, fractal algorithm, image**

## Вступ

Як і у випадку традиційного шифрування, схема шифрування з відкритим ключем уразлива з погляду аналізу з перебором всіх ключів. І контрзаходи тут ті самі – використання довгих ключів. Однак у цьому випадку є й інші варіанти захисту. Криптосистеми з відкритим ключем залежать від деякої оборотної математичної функції зі спеціальними властивостями. Складність обчислення такого роду функцій може залежати не лінійно від числа бітів у ключі, а зростати швидше. Тому довжина ключа повинна бути достатньо великою для того, щоб аналіз із перебором всіх ключів став практично нездійсненним, але достатньо малою для того, щоб на практиці можна було використати операції шифрування й дешифрування. Пропоновані для використання на практиці довжини ключів, звичайно ж, забезпечують практичну неефективність аналізу з перебором всіх ключів, але при цьому виявляються занадто повільними для того, щоб відповідні алгоритми можна було рекомендувати для універсального застосування. Тому, як уже згадувалося вище, шифрування з відкритим ключем у цей час обмежується областями керування ключами й додатками цифрового підпису.

Іншою формою атаки є спроба знайти спосіб обчислення особистого ключа за відомим відкритим ключем. Сьогодні немає математичного доказу неможливості такої форми атаки для жодного алгоритму шифрування з відкритим ключем. Із цього погляду будь-який конкретний алгоритм цього типу, зокрема поширений алгоритм RSA, виявляється таким, що не викликає довіри. А історія криптографії показує, що проблема, яка здається нерозв'язною, може виявитися цілком розв'язною, якщо подивитися на неї з якогось, зовсім нового погляду. Це стосується і зображень.

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].

У контурі зображення сконцентрована інформація, яка характеризує його форму, що є важливо для сприйняття і розпізнаванні образів. Контурні точки є незначною частиною всього зображення. За допомогою них можна ефективно і аналітично просто описувати зображення об'єктів, які є інваріантні до основних перетворень (перенесення, масштабування і повороту). Задачі контурного аналізу актуальні в автоматизованих системах обробки зображень різноманітної природи: технічного зору, біологічних, медичних тощо [3].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через яку контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут основано на піднесенні до степеня за модулем деякого натурального числа. При цьому на контурі і на сусідніх до контуру пікселах піднесення 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 належать їх послідовна реалізація і деяка складність під час пошуку і оброблення внутрішніх контурів.

Для визначення контурів у зображенннях використовують статистичний аналіз фрагментів зображення та їх взаємну кореляцію з метою знаходження стрибкоподібних змін кольору і освітленості. Велика група методів основана на використанні математичних моделей, що відображають певну взаємодію між окремими пікселями або фрагментами зображень. Також для розв’язання задач розпізнавання об’єктів застосовують різні методи фільтрації, наприклад, інверсні фільтри, фільтри Вінера, Байєса. При цьому використовують аналогію між динамікою зображень та фізичними процесами, наприклад, дифузії. Для розв’язання деяких задач використовують стохастичні моделі.

Алгоритми сегментації зображень грунтуються на одній з двох характеристик сигналу яскравості – розривності або однорідності. В першому випадку підхід грунтується на розбитті зображення на основі різких змін сигналу, таких як перепади яскравості на зображенні. Зазвичай шукають розриви за допомогою ковзних масок. Друга категорія методів грунтується на визначенні однорідності зображення за наперед обраними критеріями.

*Рис. 1. Виокремлення контурів у зображенні*

Надалі приймемо, що зображенню відповідає матриця кольорів [4,5]

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

Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [4]. У [5] для шифрування – дешифрування зображень в градаціях сірого було запропоновано використовувати квадратичні фрактальні перетворення. Тут для шифрування – дешифрування таких зображень пропонується використовувати кубічні фрактальні перетворення.

**Шифрування і дешифрування за одним рядком матриці зображення**

Нехай ***P, Q*** – пара довільних простих чисел і $N = PQ$, $e \times d \equiv 1 (\mathrm{mod}\ \varphi(N))$, $\varphi(N) = (P-1)(Q-1)$, $F = P^e (\mathrm{mod}\ \varphi(N))$, $G = Q^d (\mathrm{mod}\ \varphi(N))$.

Шифрування відбувається з використанням кубічного фрактального перетворення двох сусідніх елементів рядка в матриці зображення ***C*** за такими співвідношеннями:

$$\begin{cases} u_{n,k} = F^3 u_{n,k-1}^3 + G^3 u_{n+1,k-1}^3 \\ u_{n+1,k} = F u_{n,k-1} + G u_{n+1,k-1} \end{cases} \quad (2)$$

$n = 1, 2, \ldots, N_0$, $N_0$ – число елементів у рядку; ***k*** – номер фрактальної ітерації, $u_{n,0} = u_n$, $u_{n+1,0} = u_{n+1}$. Дешифрують формулами

$$u_{n,k-1} = \frac{3u_{n,k} \pm \sqrt{D}}{6F}; \quad (3)$$

$$u_{n+1,k-1} = \frac{3u_{n,k} \mp \sqrt{D}}{6G}, \quad (4)$$

де $D = 12u_{n,k} / u_{n+1,k} - 3u_{n+1,k}$.

Результати наведено на рис. 2–4.

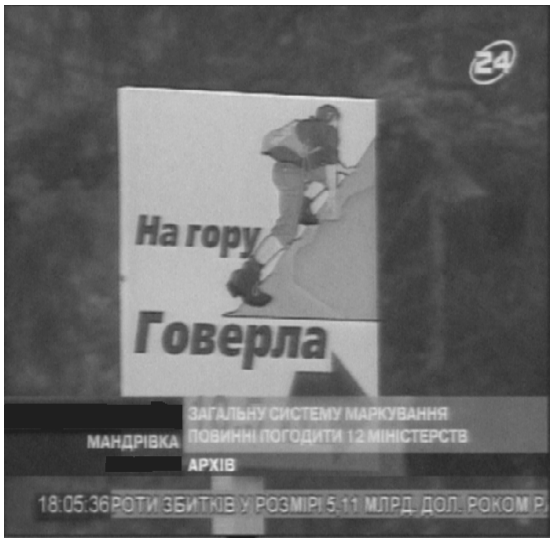


*Рис. 2. Початкове зображення*

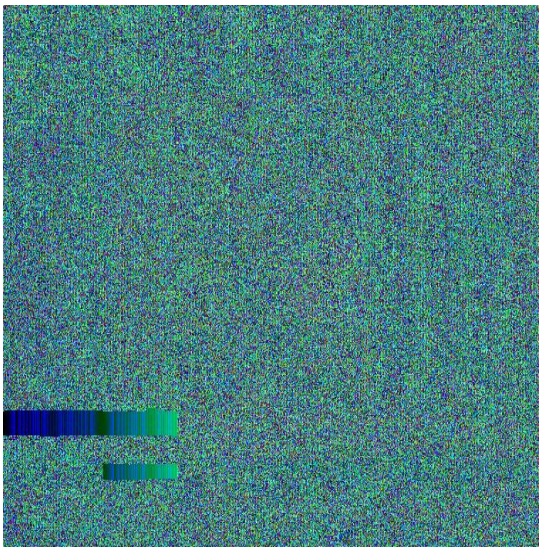

*Рис. 3. Зашифроване зображення*


*Рис. 4. Дешифроване зображення*

Шифрування з використанням іншого кубічного фрактального перетворення двох сусідніх елементів рядка в матриці зображення $\boldsymbol{C}$ реалізовується за такими співвідношеннями:

$$\begin{cases} u_{n,k} = F^3 u_{n,k-1}^3 - G^3 u_{n+1,k-1}^3 \\ u_{n+1,k} = F u_{n,k-1} - G u_{n+1,k-1} \end{cases}, \tag{5}$$

де $n = 1, 2, \ldots, N_0$, $N_0$ – число елементів у рядку; $k$ – номер фрактальної ітерації; $u_{n,0} = u_n$, $u_{n+1,0} = u_{n+1}$.

Для дешифрування використовуться формули

$$u_{n,k-1} = \frac{3u_{n,k} \pm \sqrt{D}}{6F}; \tag{6}$$

$$u_{n+1,k-1} = \frac{-3u_{n,k} \mp \sqrt{D}}{6G}, \tag{7}$$

Результати наведено на рис. 5–7. Очевидно, що шифрування і дешифрування суттєво залежать від вибору простих $P$, $Q$, $R$, $T$, а також від числа фрактальних ітерацій.


*Рис. 5. Початкове зображення*

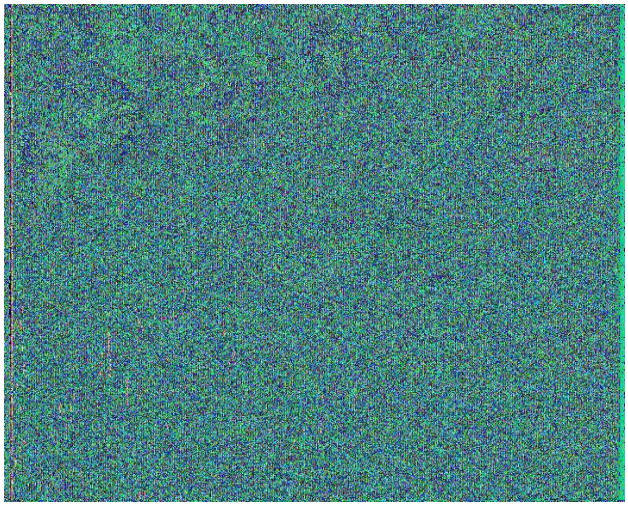

*Рис. 6. Зашифроване зображення*


*Рис. 7. Дешифроване зображення*

Загальний вигляд форми програмного ужитку шифрування-дешифрування за формулами (2)–(7) наведено на рис. 8.

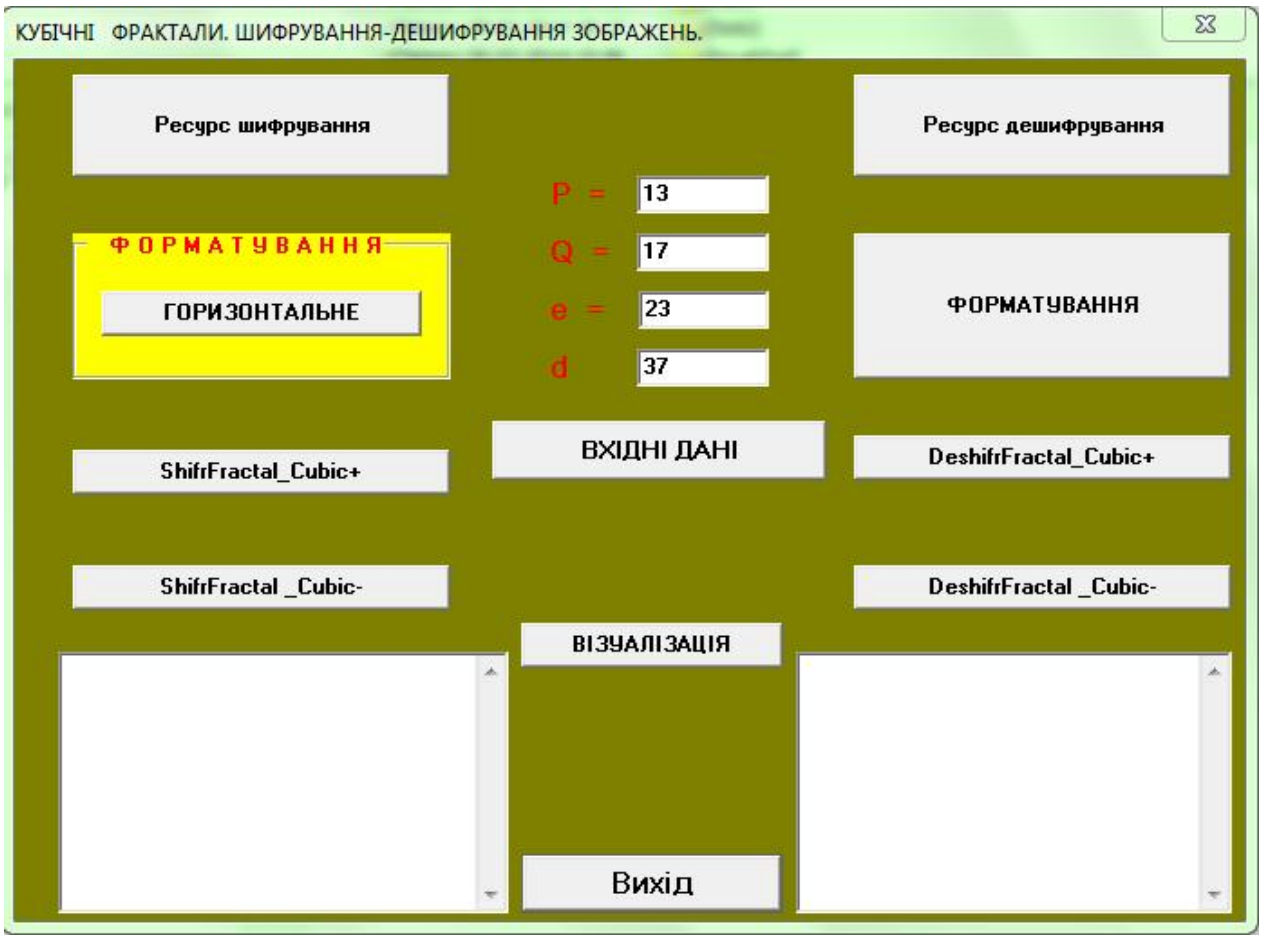


*Рис. 8. Загальний вигляд форми програмного ужитку*

**Висновки**

З порівняння рис. 3 і рис. 6 видно, що шифруванняза формулами (2) дещо структурно відрізняється від шифрування за формулами (5). Контури в обох зашифрованих зображеннях відсутні. Дешифровані зображення в обох випадках є візуально еквівалентними, хоча при дешифруванні за формулами (5) спостерігається незначне затемнення зображення. Вказані алгоритми можна використати для оперативного передавання графічних зображень для отримання задовільного результату стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дають змогу чітко виділяти контури. Підвищується стійкість шифрування, оскільки для шифрування і дешифрування використовуються довільні прості числа, які можуть бути доволі великими, і елементи алгоритму RSA. А від цього залежить стійкість криптографічного алгоритму. Криптографічна стійкість запропонованих алгоритмів вища, ніж алгоритму RSA.

Обидва типи запропонованих алгоритмів шифрування – дешифрування можна використовувати і стосовно кольорових зображень. Однак незалежно від типу зображення можуть виникати проблеми під час розв'язування відповідних алгебраїчних рівнянь.

*1. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Прэтт У. Цифровая обработка изображений. Кн. 1,2. – М.: Мир , 1982. 4.Фабрі Л., Ковальчук А., Ступень М. Шифрування і дешифрування зображень з використанням квадратичних фрактальних алгоритмів // Вісник Нац. ун-ту "Львівська політехніка", "Комп'ютерні науки та інформаційні технології". – № 694. – С. 180–184. 5. Цмоць І., Ковальчук А., Ступень М. Системи фрактальних алгоритмів в шифруванні – дешифруванні зображень з додатковим зашумленням // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – № 732. – С. 288–293.*