повністю) актив здійснює акції паралельно (рис. 2). Цей процес не є лімітованим у часі і припиняється за умови завершення участі користувача WWW у акції, при завершенні суспільної акції, або припиненні існування хостингу суспільних акцій.

Висновки. Для чіткого визначення послідовності дій, що повинні бути здійснені в процесі персоніфікації, автор розробив алгоритм активної реферальної персоніфікації інформаційного наповнення WWW.

Література

1. Пелещишин А.М. Веб 2.0 та Семантичний Веб: порівняльний аналіз перспективних тенденцій розвитку WWW / А.М. Пелещишин, О.Л. Березко // Східно-Європейський журнал передових технологій. – Харків, 2006. – 6/2 (24). – С. 43-51.

2. Agichtein E. Finding high-quality content in social media with an application to community-based question answering // E. Agichtein, Castillo C., Donato D., Gionis A., Mishne G.; Yahoo! Research / Technical report. – 25.09 2007. – № YR-2007-005. – С. 24. **[**Електронний ресурс**]**. – Доступний з http://www.research.yahoo.com/files/2007-005_Agichtein_0.pdf.

3. Пелещишин А.М. Формальні аспекти ідентифікації особистості у WWW / А.М. Пелещишин, О.Л. Березко // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи та мережі. – Львів : Вид-во НУ "Львівська політехніка". – 2008. – № 546. – С. 126-131.

4. Березко О.Л. Суспільні акції як метод активної персоніфікації інформаційного наповнення у World Wide Web / О.Л. Березко // Вісник Кременчуцького державного політехнічного університету ім. М. Остроградського. – Кременчук, 2010. – 1/2010 (60). – С. 30-35.

Берёзко А.Л. Алгоритм активной реферальной персонификации информационного наполнения World Wide Web

Рассмотрены общественные акции как метод активной реферальной персонификации информационного наполнения в World Wide Web и предложен алгоритм такой персонификации с использованием графических кнопок в качестве персонификационных вставок, который предусматривает привлечение глобального Веб-сообщества к инициирующему собственных и участия в существующих общественных акциях.

***Ключевые слова*:** WWW, информационное наполнение, персонификация.

Berezko O.L. Algorithm of active referral World Wide Web content personification

We consider public actions as a method of active referral Web content personification and propose the algorithm of such personification with the use of web badges as personifying inserts. This algorithm allows members of global Web community to take act in the personification process via initiation of own public actions and taking part in existing ones.

***Keywords*:** WWW, content, personification.

УДК 681.142.2; 622.02.658.284; 621.325

Ст. викл. А.М. Ковальчук;
доц. Д.Д. Пелешко, канд. техн. наук;
ст. викл. Н.О. Кустра, канд. техн. наук – НУ "Львівська політехніка"

ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ АЛГОРИТМУ RSA ДРОБОВО-РАЦІОНАЛЬНИМИ N-АРНИМИ ФОРМАМИ

Запропоновано алгоритм шифрування і дешифрування зображень з чітко виділеними контурами дробово-лінійними формами порядку n з використанням елемен-

тів алгоритму RSA, як найбільш стійкого до несанкціонованого дешифрування сигналів. Встановлено, що незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення. Запропоновану модифікацію можна використовувати для будь-якого типу зображення, але найбільше переваг досягають у випадку використання зображень, які дають змогу чітко виділяти контури.

Вступ. Важливою характеристикою зображення є наявність на зображенні контурів. Задача виділення контуру потребує 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**]**.

Стосовно 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 у площині зображення. Тому виділення контура означає пошук найразючіших змін, тобто максимумів модуля вектора градієнта **[**1, 2 **]**. Це є однією з причин, через що контури залишаються в зображенні під час шифрування в системі RSA, оскільки шифрування тут базується на піднесенні до степеня за модулем певного натурального числа **[**4**]**. При цьому на контурі і на сусідніх до контуру пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

1. Постановка задачі**.** Основним завданням є розроблення модифікації методу RSA такої, щоб зберегти стійкість до несанкціонованого доступу та забезпечити повне зашумлення зображення, з метою унеможливити використання методів візуального оброблення зображень.

Для вирішення цієї задачі використовуються n-арні дробово-лінійними формами. Нехай задано рисунок P з ширини l і висоти h. Його можна розглядати як матрицю пікселів

$$<dtp_{ij}>_{1\le i\le n,\ 1\le j\le m}, \tag{1}$$

де: dtp_{ij} – піксел з координатами i та j, n і m – кількість точок за шириною l та висотою. У загальному випадку n і m є залежними від l та h, а тому більш коректним є запис

$$n = n(l) \text{ і } m = m(h). \tag{2}$$

Матриці (1) у відповідність ставиться матриця кольорів

$$C=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \tag{3}$$

де c_{ij} – значення інтенсивності у напівтонових зображень піксела dtp_{ij} чи значення кольору у кольорових зображеннях.

2. Алгоритм шифрування та дешифрування. Дробово-раціональна n-арна форма має такий вигляд

$$y = \frac{Ax^n - B}{Cx^n - D}. \tag{4}$$

Проективне відображення (4) переводить точки $x = \sqrt[n]{D/C}$ в ∞. Обернене до (4) відображення має вигляд

$$x = \sqrt[n]{\frac{Dy - B}{Cy - A}}. \qquad (5)$$

Обернене проективне відображення (5) переводить точку $y = A/C$ в точку ∞, тобто не є взаємно однозначним, якщо $A \neq D$. Це необхідно враховувати під час шифрування і дешифрування для отримання достовірного дешифрованого зображення.

Шифрування відбувається поелементно за формулою (4), де $x = c_{i,j}$, $i = \overline{1,n}$, $j = \overline{1,m}$, $A = D = Q$, $B = P - Q$, $C = e - d$.

Дешифрування здійснюють за формулами оберненого перетворення (2) з тими ж коефіцієнтами $A = D = Q$, $B = P - Q$, $C = e - d$. Результати шифрування і дешифрування наведено на рис. 1-3 за $n = 2$.

Рис. 1. Початкове зображення

Рис. 2. Дешифроване зображення

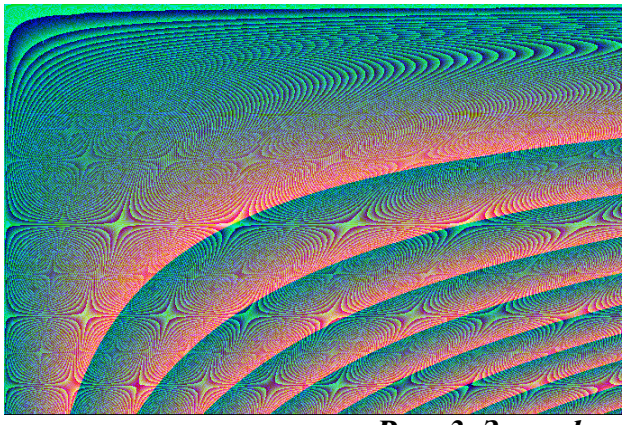
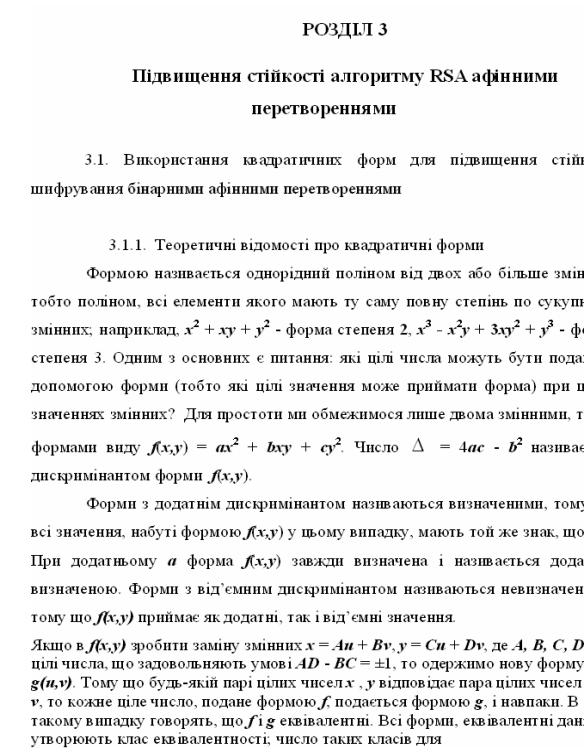


Рис. 3. Зашифроване зображення

Запропонованим методом може бути зашифровано і текстову інформацію, яка заздалегідь була приведена до графічного формату. Результати такого шифрування і дешифрування з використанням описаного методу наведено на рис. 4-6.



РОЗДІЛ 3

Підвищення стійкості алгоритму RSA афінними перетвореннями

3.1. Використання квадратичних форм для підвищення стійкості шифрування бінарними афінними перетвореннями

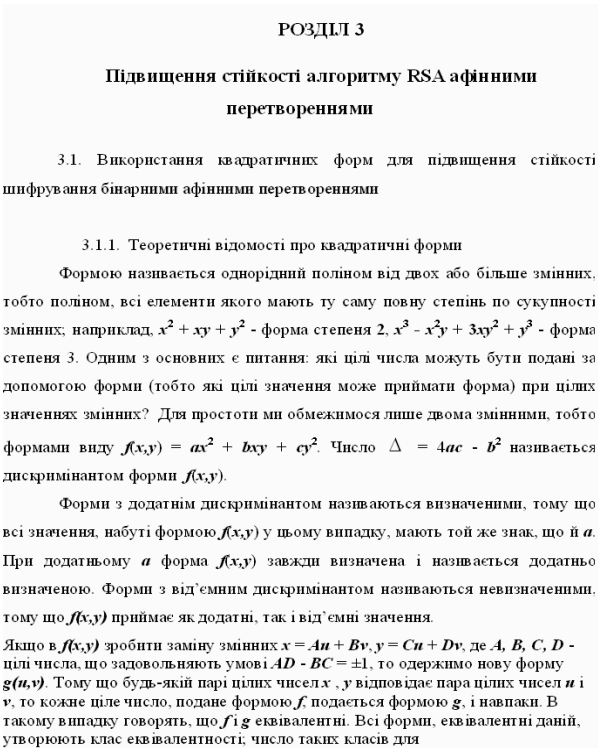
3.1.1. Теоретичні відомості про квадратичні форми

Формою називається однорідний поліном від двох або більше змінних, тобто поліном, всі елементи якого мають ту саму повну степінь по сукупності змінних; наприклад, $x^2 + xy + y^2$ - форма степеня 2, $x^3 - x^2y + 3xy^2 + y^3$ - форма степеня 3. Одним з основних є питання: які цілі числа можуть бути подані за допомогою форми (тобто які цілі значення може приймати форма) при цілих значеннях змінних? Для простоти ми обмежимося лише двома змінними, тобто формами виду $f(x,y) = ax^2 + bxy + cy^2$. Число $\Delta = 4ac - b^2$ називається дискримінантом форми $f(x,y)$.

Форми з додатнім дискримінантом називаються визначеними, тому що всі значення, набуті формою $f(x,y)$ у цьому випадку, мають той же знак, що й a. При додатньому a форма $f(x,y)$ завжди визначена і називається додатньо визначеною. Форми з від'ємним дискримінантом називаються невизначеними, тому що $f(x,y)$ приймає як додатні, так і від'ємні значення.

Якщо в $f(x,y)$ зробити заміну змінних $x = Au + Bv$, $y = Cu + Dv$, де A, B, C, D - цілі числа, що задовольняють умові $AD - BC = \pm 1$, то одержимо нову форму $g(u,v)$. Тому що будь-якій парі цілих чисел x , y відповідає пара цілих чисел u і v, то кожне ціле число, подане формою f, подається формою g, і навпаки. В такому випадку говорять, що f і g еквівалентні. Всі форми, еквівалентні даній, утворюють клас еквівалентності; число таких класів для

Рис. 4. Початкове зображення



РОЗДІЛ 3

Підвищення стійкості алгоритму RSA афінними перетвореннями

3.1. Використання квадратичних форм для підвищення стійкості шифрування бінарними афінними перетвореннями

3.1.1. Теоретичні відомості про квадратичні форми

Формою називається однорідний поліном від двох або більше змінних, тобто поліном, всі елементи якого мають ту саму повну степінь по сукупності змінних; наприклад, $x^2 + xy + y^2$ - форма степеня 2, $x^3 - x^2y + 3xy^2 + y^3$ - форма степеня 3. Одним з основних є питання: які цілі числа можуть бути подані за допомогою форми (тобто які цілі значення може приймати форма) при цілих значеннях змінних? Для простоти ми обмежимося лише двома змінними, тобто формами виду $f(x,y) = ax^2 + bxy + cy^2$. Число $\Delta = 4ac - b^2$ називається дискримінантом форми $f(x,y)$.

Форми з додатнім дискримінантом називаються визначеними, тому що всі значення, набуті формою $f(x,y)$ у цьому випадку, мають той же знак, що й a. При додатньому a форма $f(x,y)$ завжди визначена і називається додатньо визначеною. Форми з від'ємним дискримінантом називаються невизначеними, тому що $f(x,y)$ приймає як додатні, так і від'ємні значення.

Якщо в $f(x,y)$ зробити заміну змінних $x = Au + Bv$, $y = Cu + Dv$, де A, B, C, D - цілі числа, що задовольняють умові $AD - BC = \pm 1$, то одержимо нову форму $g(u,v)$. Тому що будь-якій парі цілих чисел x , y відповідає пара цілих чисел u і v, то кожне ціле число, подане формою f, подається формою g, і навпаки. В такому випадку говорять, що f і g еквівалентні. Всі форми, еквівалентні даній, утворюють клас еквівалентності; число таких класів для

Рис. 5. Дешифроване зображення

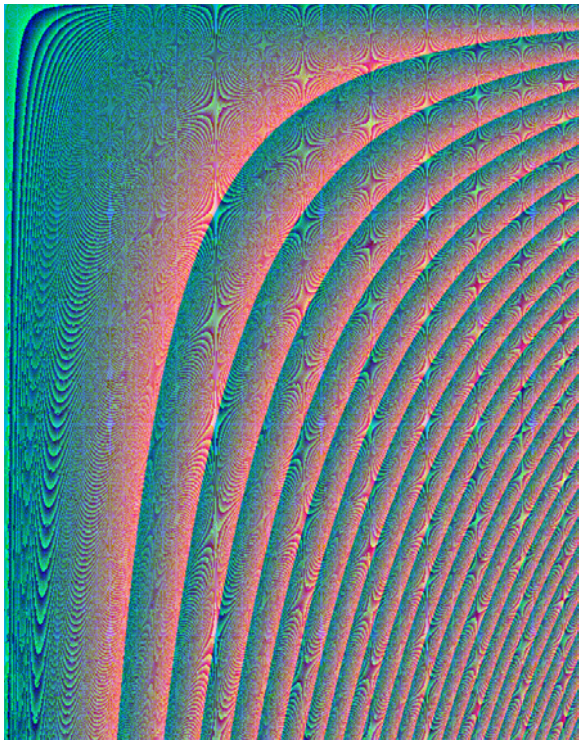


Рис. 6. Зашифроване зображення

Висновки. Запропонована модифікація шифрування призначена для зображень в градаціях сірого і ґрунтується на використанні ідей базового алгоритму RSA. Описану модифікацію без жодних застережень можна застосувати стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення. Запропоновану модифікацію може бути використано стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дають змогу чітко виділяти контури.

Література

1. Брюс Шнайер. Прикладная криптография / Брюс Шнайер. – М. : Изд-во "Триумф", 2003. – 815 с.

2. Яне Б. Цифровая обработка изображений / Б. Яне. – М. :, Техносфера, 2007. – 583 с.

3. Рашкевич Ю.М. Модифікація алгоритму RSA для деяких класів зображень / Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З. // Технічні вісті. – 2008/1(27), 2(28). – С. 59-62.

4. Rashkevych Yu. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM 2009 /

Yu. Rashkevych, A. Kovalchuk, D. Peleshko, M. Kupchak. 24-28 February 2009, Lviv-Polyana, Ukraine. – PP. 469-473.

Ковальчук А.М., Пелешко Д.Д., Кустра Н.О. **Шифровка и дешифрация изображений с использованием элементов алгоритма RSA дробно-рациональными N-арными формами**

Предложен алгоритм шифровки и дешифрации изображений с четко выделенными контурами дробно линейными формами порядка n с использованием элементов алгоритма RSA, как наиболее стойкого к несанкционированной дешифрации сигналов. Установлено, что независимо от типа изображения, пропорционально к размерности входного изображения, может вырасти размер шифрованного изображения. Предложенную модификацию можно использовать для любого типа изображения, но наибольшие преимущества достигаются в случае использования изображений, которые дают возможность четко выделять контуры.

Kovalchuk A.M., Peleshko D.D., Kustra N.O. **Encrypting and decrypting images using elements of RSA algorithm fractional-rational N-forms**

The algorithm of encoding and decoding of the images with legiblly discharged contours by the common fraction and linear forms of n degree with usage of members of algorithm RSA, as steadiest to unauthorized decoding of signals is offered. It is set that regardless of as an image, proportionally to the dimension of entrance image, the size of the coded image can grow. The offered modification can be utillized for any as an image, but most advantages are arrived at in the case of the use of images which enable expressly to select contours.