УДК 621.391

Ю.Я. Бобало[1], Р.Л. Політанський[2], М.М. Климаш[1], Г.В. Косован[2]

[1] *Національний університет «Львівська політехніка», Львів*
[2] *Чернівецький національний університет ім. Ю. Федьковича, Чернівці*

ДОСЛІДЖЕННЯ АЛГОРИТМУ КРИПТОГРАФІЧНОГО ЗАХИСТУ ЗОБРАЖЕННЯ НА ОСНОВІ БАГАТОМІРНОГО УЗАГАЛЬНЕНОГО ПЕРЕТВОРЕННЯ ПЕКАРЯ

Задача шифрування зображень та іншої мультимедійної інформації є актуальною у зв'язку із ростом обсягу інформації, що проходить через Інтернет. Авторами досліджене узагальнене перетворення пекаря, що є нелінійним перетворенням пікселів зображення, що не змінює їх інтенсивності і зберігає початкові його розміри. Результатом проведених досліджень є встановлення оптимального розбиття зображення для ефективного застосовування вказаного алгоритму. Додатково була проведена дифузія, що змінила кольорову гаму цього зображення.

Ключові слова: *перетворення пекаря, дифузія, піксель.*

Вступ

Розроблення програмних методів шифрування зображень та інших мультимедіа є актуальною задачею оброблення інформації, що обумовлено зростанням її обсягів передавання засобами Internet.

Одним із методів криптоаналізу багатьох систем шифрування є статистичний аналіз, що використовує частоту виникнення окремих символів та їх комбінацій [1].

Шенон [2] запропонував дві концепції шифрування, що були названі ним «змішування» (confusion) та «дифузія» (diffusion).

Змішування – це перетворення підстановки, що значно ускладнює взаємозв'язок між ключем та шифрованим текстом. Дифузія – це перетворення, що зменшує статистичні відмінності між символами та їх комбінаціями.

Найбільш очевидним прикладом дифузії є додавання символів зашифрованої послідовності по модулю потужності алфавіту.

Для зображень потужністю алфавіту слугує кількість градацій базових кольорів (синій, червоний, зелений у системі RGB):

$$Y_n = \left(\sum_{i=0}^{K} X_{n+i} \right) \bmod 256 . \qquad (1)$$

Внаслідок такого перетворення розподіл частот символів наближається до рівномірного (у зображенні переважає сірий колір).

Змішуванням у сучасних системах шифрування як правило є нелінійне перетворення, що може використовувати побітові операції.

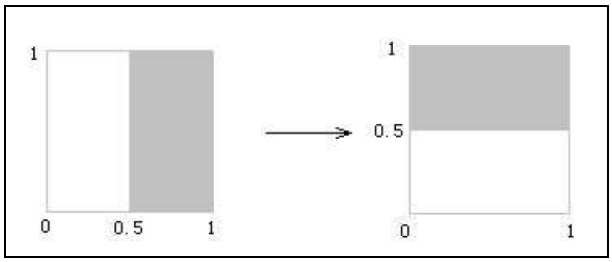
У досліджуваному нами алгоритмі використовувалося узагальнене перетворення пекаря [3], що переставляє місцями координати пікселів без зміни їх інтенсивності та загальних розмірів зображення (рис. 1).

Таке перетворення є нелінійним.

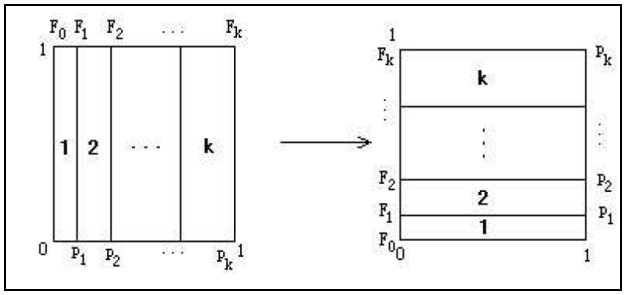
1. Алгоритм шифрування

Одно- та двовимірні карти хаосу, основою яких є відображення (2), є двовимірною картою хаосу, що перетворює множину $I \times I$ саму в себе таким чином, як це показано на рис. 1, а. Таке перетворення називається перетворенням пекаря.

$$B(x) = \begin{cases} \left(2 \cdot x, \frac{y}{2}\right) \ldots\ldots 0 \le x < \frac{1}{2}; \\ \left(2 \cdot x - 1, \frac{y}{2} + \frac{1}{2}\right) \ldots\ldots \frac{1}{2} \le x < 1. \end{cases} \qquad (2)$$



а



б

Рис. 1. Класичне (а) та узагальнене (б) перетворення пекаря

Узагальнене перетворення пекаря визначається наступним чином: одиничний квадрат розділяється на k вертикальних прямокутників:

$$[F_{i-1}) \times [0,1), i = 1, \ldots, k ,$$

$F_i = p_1 + p_2 + \cdots p_i, F_0 = 0$, $p_1 + p_2 + \cdots + p_k = 1$.

Нижній правий кут i-го прямокутника розміщений у точці $F_i = p_1 + p_2 + \cdots p_i, F_0 = 0$. Узагальнена схема пекаря розтягує кожен прямокутник у горизонтальному напрямку з коефіцієнтом $1/p_i$, а у вертикальному напрямку прямокутник стискається з коефіцієнтом p_i (рис. 1, б).

Аналітично схема може бути представлена наступним чином:

$$B(x,y) = \left(\frac{1}{p_i}\cdot(x - F_i), p_i \cdot y + F_i\right), \qquad (3)$$

при $(x,y) \in [F_i, F_i + p_i) \times [0,1)$ Дискретизована схема пекаря необхідна для того, щоб встановлювати взаємно однозначну відповідність між пікселями початкового та зашифрованого зображень. Якщо розділити квадрат розміром $N \times N$ на вертикальні прямокутники розміром $N \times N_i$ пікселів, то дискретизована схема пекаря описується таким чином:

$$(r,s) =$$

$$= \left(\frac{N}{n_i}\cdot(r - N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}\cdot\left(s - s \bmod \frac{N}{n_i}\right) + N_i\right), \qquad (4)$$

де піксель (r,s) знаходиться в межах

$$N_i \le r < N_i + n_i,\ 0 \le s < N. \qquad (5)$$

Послідовність, утворена k цілими числами, $n_1, n_2, \ldots, n_k$ вибирається таким чином, щоб кожне ціле число n_i ділилося на N, і $N_i = n_1 + n_2 + \cdots + n_i$, $N = n_1 + \cdots + n_k$. Якщо не всі числа $\{n_i\}$ діляться на N, і множина точок являє собою прямокутник, що має розміри $M \times N$, то схема, що встановлює відповідність між пікселями (i,j) та (r,s), може бути описана за допомогою наступного алгоритму:

$$\begin{pmatrix} r \\ s \end{pmatrix} = B_d \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} (M_{i-1} \cdot N + j \cdot m_i + i - M_{i-1})/M \\ (M_{i-1} \cdot N + j \cdot m_i + i - M_{i-1}) \bmod M \end{pmatrix}. \qquad (6)$$

Прямокутник розмірами $M \times N$ розділяється на вертикальні прямокутники N пікселів по висоті та m_i пікселів по ширині зображення. Послідовність, утворена k цілими числами, $m_1, m_2, \ldots, m_k$, вибирається таким чином, щоб $M_i = m_1 + \cdots + m_i$, $M = m_1 + m_2 + \cdots + m_k$, а $M_0 = 0$. Таким чином, дискретизована двомірна карта хаосу, що ґрунтується на перетворенні пекаря, може бути описана аналітичним виразом (6).

Для шифрування зображень також використані триохмірні перетворення пекаря, і як показали експерименти, має у 2-3 рази більшу швидкодію за одновимірну і може використовуватись у системах реального часу.

Математичною моделлю трьохвимірного перетворення (рис. 2) є такий вираз:

$$B(x,y,z) =$$

$$= \begin{cases} \left(2\cdot x, 2\cdot y, \frac{z}{4}\right) & 0 \le x < \frac{1}{2}, 0 \le y < \frac{1}{2}; \\ \left(2\cdot x, 2\cdot y - 1, \frac{z}{4} + \frac{1}{2}\right) & 0 \le x < \frac{1}{2}, \frac{1}{2} \le y < 1; \\ \left(2\cdot x - 1, 2\cdot y, \frac{z}{4} + \frac{1}{4}\right) & \frac{1}{2} \le x < 1, 0 \le y < \frac{1}{2}; \\ \left(2\cdot x - 1, 2\cdot y - 1, \frac{z}{4} + \frac{3}{4}\right) & \frac{1}{2} \le x < 1, \frac{1}{2} \le y < 1. \end{cases} \qquad (7)$$

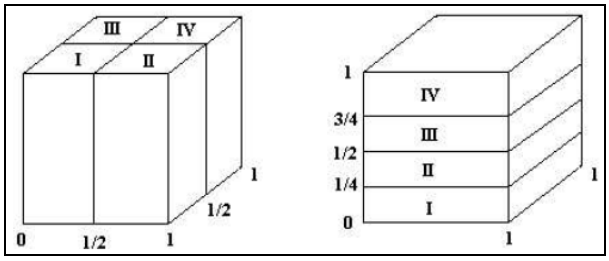


Рис. 2. Тривимірне відображення пекаря

Аналогічно до двовимірного перетворення пекаря трьохвимірне перетворення пекаря також має узагальнену форму. Одиничний куб розділяється на смужки (рис. 2), що стискуються в одному напрямку і розтягуються в іншому.

Далі смужки складаються таким чином, щоб вони утворили одиничний куб того ж об'єму. Інакше кажучи одиничний куб розідляється на $k \times t$ блоків $[W_{i-1}, W_i) \times [H_{j-1}, H_j) \times [0,1)$, $i = 1, \ldots, k$, $j = 1, \ldots, t$, $W_i = w_1, w_1, \ldots, w_i$, $W_0 = 0$ таким чином, щоб виконувались співвідношення:

$$w_1 + w_2 + \cdots + w_k = 1 \text{ і } H_j = h_1 + h_2 + \cdots + h_j,$$

$$H_0 = 0,\ h_1 + h_2 + \cdots + h_t = 1.$$

Тоді узагальнена 3-вимірна схема пекаря описується співвідношенням:

$$B_3(x,y,z) =$$

$$= \left(\frac{1}{w_i}\cdot(x - W_i), \frac{1}{h_j}\cdot(y - H_j), w_i \cdot h_j \cdot z + L_{ij}\right), \qquad (7)$$

де $(x,y,z) \in [W_{i-1}, W_i) \times [H_{i-1}, H_i) \times [0,1)$, $L_{ij} = W_i \times h_j + H_j$, $i = 1, \ldots, k$, $j = 1, \ldots, t$.

Потім трьохвимірна схема дискретизується, при цьому використовується довільний розмір кубу. Вважатимемо, що куб має розміри $W \times H \times L$ і розділяється на $k \times t$ блоків. Послідовність, утворена k цілими числами, $w_1, w_2, \ldots, w_k$, вибирається так, щоб виконувалися співвідношення: $W_i = w_1 + w_2 + \cdots + w_i$, $W = w_1 + w_2 + \cdots + w_k$ і $W_0 = 0$. Така ж процедура здійснюється для послі-

довності t цілих чисел, і $H_j = h_1 + h_2 + \cdots + h_j$, $H = h_1 + h_2 + \cdots + h_t$ і $H_0 = 0$.

Перетворення

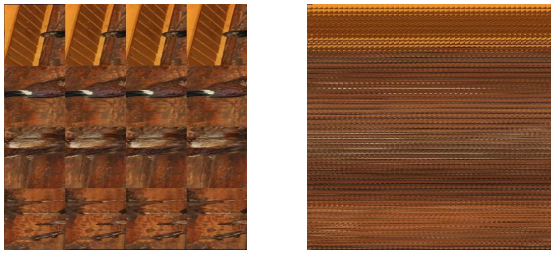
$$S = \left(H_{j-1} \times W + W_{i-1}\right) \times L + w_i \times h_j \times l + \left(n - H_{j-1}\right) \times$$
$$\times w_i + \left(m - W_{i-1}\right)\left(m', n', l'\right) = B_{3D}(m, n, l) = \quad (8)$$
$$= \left(\left(S \bmod \left(W \times H\right)\right) \bmod W, \left[\frac{S \bmod \left(W \times H\right)}{W}\right], \left[\frac{S}{W \times H}\right] \right)$$

переводить довільну точку (m, n, l) кубу у точку з координатами $\left(m', n', l'\right)$ нового кубу.

2. Результати та обговорення

Нами розроблена програмна реалізація та використане трьохвимірне перетворення пекаря для шифрування двохвимірних зображень. Результати шифрування зображення (рис. 3) приведені на рис. 4. На рис. 5 приведені результати шифрування з додатковим використанням дифузії.

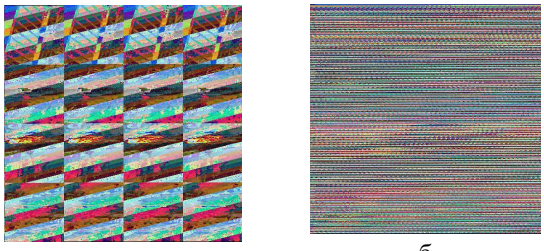
Рис. 3. Початкове зображення 480 на 480



а б

Рис. 4. Поступове перетворення Пекаря, розділене на 4 та 50 прямокутників, а та б відповідно

Додаткове застосування дифузії не суттєво впливає на результати шифрування



а б

Рис. 5. Перетворення пекаря з використанням дифузії розділене на 4 та 50 прямокутників а та б відповідно

Висновки

В результаті проведеної роботи досліджено та вдосконалено відомий алгоритм перетворення пекаря та розроблена програма шифрування зображень за перетворення пекаря.

Встановлено оптимальне розбиття початкового зображення для ефективного застосування алгоритму шифрування.

Список літератури

1. Feistel H. Cryptography and Computer Privacy / H. Feistel // Scientific American. – 1973. – Vol. 228. – P. 15-23.

2. Shannon C.E. Communication Theory of Secrecy Systems / C.E. Shannon // Bell Systems Technical Journal. – 1949. – Vol. 28. – P. 656-715.

3. Кузнецов С.П. Лекция 2. Хаос в простых моделях динамических систем / С.П. Кухнецов // Динамический хаос (курс лекций). – М: Физматлит, 2001. – С. 21-42.

Надійшла до редколегії 20.06.2014

Рецензент: д-р техн. наук, с.н.с. О.О. Можаєв, Національний технічний університет «ХПІ», Харків.

ИССЛЕДОВАНИЕ АЛГОРИТМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ГРАФИЧЕСКИХ ФАЙЛОВ, ОСНОВАННЫЙ НА МНОГОМЕРНОМ ОБОБЩЕННОМ ПРЕОБРАЗОВАНИИ ПЕКАРЯ

Ю.Я. Бобало, Р.Л. Политанский, М.М. Климаш, Г.В. Косован

Статья посвящена актуальной в связи с ростом трафика в Интернете проблеме криптографической защиты изображений. Мы использовали известное преобразование пекаря, которое является нелинейным алгоритмом и меняет местами координаты пикселей, оставляя неизменным размеры изображения.

Ключевые слова: *преобразование пекаря, диффузия, пиксель.*

THE RESEARCH OF CRYPTOGRAPHIC ALGORITHM BASED ON MULTIDIMENDIONAL GENERALIZED BAKER'S MAP APPLIED TO IMAGES

Y.J. Bobalo, R.L. Politanskiy, M.M. Klymash

Software encryption of images and other multimedia are relevant task for information processing due to the increasing amount of information transmitted across an Internet. We use the generalized baker's map which is nonlinear transformation algorithm and swaps coordinates of pixels without changing their intensity and keeping the same overall size. As a result of work done we have found the optimal partioning of the original image for the effective application of the algorithm.

Keywords: *baker's map, diffusion, pixel.*