УДК 004.415.24:004.056.5

ПРИХОВУВАННЯ ДАНИХ У ПСЕВДОВИПАДКОВО ОБРАНИХ БІТАХ РАСТРОВОГО ЗОБРАЖЕННЯ

Кордунова Ю. С.

Кухарська Н. П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук, доцент

Можна виокремити такі напрямки цифрової стеганографії:

1. Watermarking – вбудовування цифрових водяних знаків.
2. Fingerprinting – вбудовування ідентифікаційних номерів.
3. Captioning – вбудовування заголовків.
4. Вбудовування інформації з метою її прихованої передачі.

Зосередимо свою увагу на четвертому з переліку напрямку застосування стеганографічних підходів. Потреба у впровадженні секретних даних у зовнішньо-безневинні об'єкти, так звані, контейнери, з метою непомітної для сторонніх осіб їх передачі виникла давно, і залишається актуальною досі. Для збереження конфіденційності листування абоненти комп'ютерної мережі поряд із криптографічними засобами можуть використати і стеганографічні, що дасть змогу приховати сам факт передачі секретних даних.

У наш час найбільш поширеним, але найменш стійким до спотворень носія інформації, є стеганографічний метод заміни найменш значущих бітів або LSB-метод. Згідно алгоритму цього методу секретна інформація впроваджується у контейнер шляхом заміни останніх бітів його елементів на біти повідомлення. Чим же пояснюється популярність LSB-методу серед стеганографічних алгоритмів? По-перше, метод дає змогу вбудувати досить велику кількість інформації без якихось помітних спотворень контейнера. По-друге, реалізація LSB-методу для більшості файлів-контейнерів не вимагає значних затрат часу і сил – ідея методу проста і зрозуміла.

Свої експерименти ми проводили на растрових зображеннях поданих у системі RGB. У цій колірній системі зображення представляється у вигляді матриці, кожен елемент якої (піксель) відповідає видимій точці і задається значеннями яскравості трьох складових – червоного (R), зеленого (G) і синього (B) кольорів. Яскравість кожної складової записується 8-бітовим числом, а отже може приймати значення в діапазоні від 0 до 255 (значення 0, 0, 0 відповідають чорному кольору, а 255, 255, 255 – максимально яскравому білому).

Для підвищення стеганостійкості LSB-алгоритму заповнення контейнера бітами повідомлення здійснюємо за псевдовипадковим порядком, що залежить від ключа $\boldsymbol{K_0}$ (рис. 1). Цей ключ сам по собі не містить послідовності координат пікселів зображення, проте однозначно визначає їх. У нашому випадку, $\boldsymbol{K_0}$ – деяке число, яке має бути відоме і відправнику, і отримувачу повідомлення. На його основі формується вектор $\boldsymbol{K}$, елементами

якого є R пар ключів. Цей вектор щораз потрібен генераторові псевдовипадкових послідовностей для обчислення (за R раундів) координат x та y пікселя зображення, у якому приховуватиметься i-ий біт текстового повідомлення [1]:

$$x = div(i,Y) + 1;$$
$$y = mod(i,Y) + 1;$$
$$\begin{cases} x = mod\left(x + f_{K_{2s-1}}(y), X\right) + 1; \\ y = mod\left(y + f_{K_{2s}}(x), Y\right) + 1, \quad s = \overline{1,R}. \end{cases}$$

де X та Y – розміри зображення;

$div(i,Y)$ і $mod(i,Y)$ – функції, що повертають, відповідно, ціле і залишок від ділення i на Y;

$f_{K_{2s}}(x)$ – функція побітового додавання за модулем 2 двох аргументів: двійкового вектора ключа K_{2s} та двійкового вектора x.

Вбудовування даних здійснюємо в канал синього кольору, так як до його модифікацій система людського зору найменш чутлива. Оскільки конфіденційну інформацію записуємо у молодші (найменш значущі) біти зображення, то це дає підстави віднести розглядуваний метод до класу, так званих, LSB-методів.

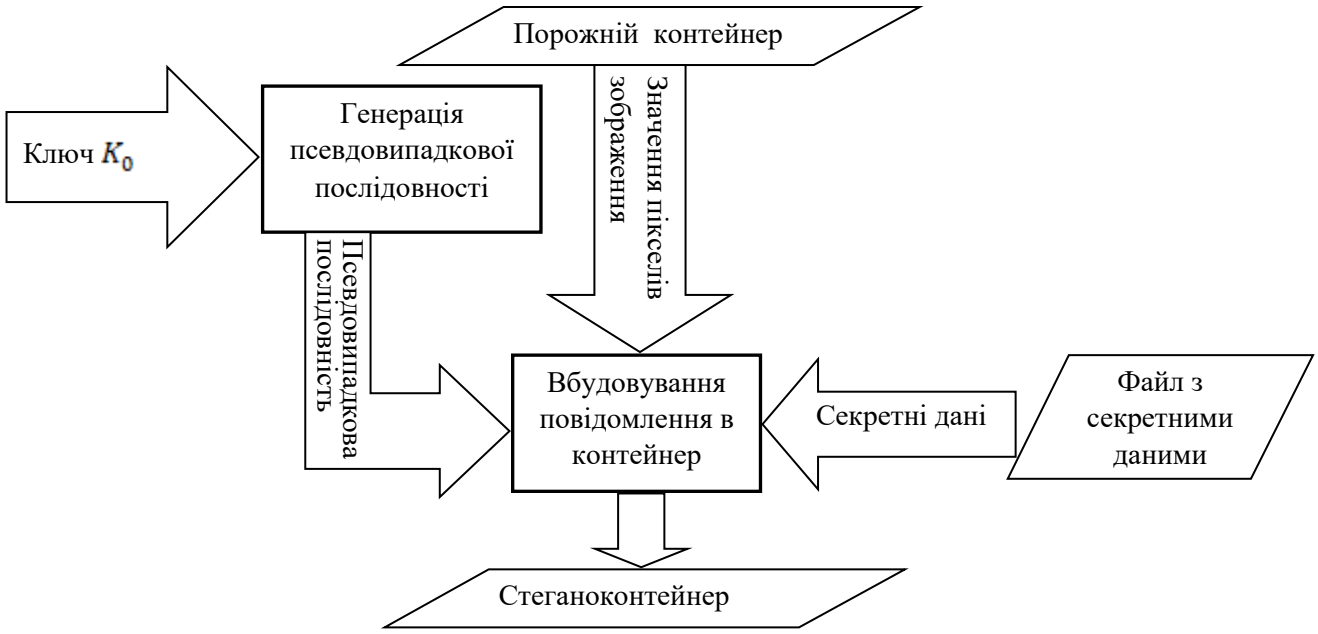

Рис. 1. Схема процесу вбудовування повідомлень у зображення

На основі описаного вище алгоритму нами були створені у середовищі MathCAD програми, які дають змогу приховати у растрових зображеннях конфіденційні повідомлення для того, щоб їх таємно передати відкритими каналами мережі.

ЛІТЕРАТУРА

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : Изд-во "МК-Пресс", 2006. – 288 с.