УДК 004.056.53

МЕТОДИКА ПРИХОВУВАННЯ ДАНИХ, ЯКА ЗАСНОВАНА НА ВИКОРИСТАННІ КЛІТИННО-АВТОМАТНОГО ПІДХОДУ

О. О. Цисар, к. т. н. К. В. Защолкін

Одеський національний політехнічний університет
Україна, м. Одеса
aleksandr.tsisar@mail.ru

Запропоновано методику вбудовування інформації в графічні контейнери, засновану на спільному застосуванні теорії стеганографії та теорії клітинних автоматів. Методика полягає у визначенні множини позицій, в яких розміщуються приховані дані, та порядку їх зчитування за рахунок використання клітинного автомата. Вбудовування та добування вбудованих даних відбувається за допомогою запропонованого протоколу приховання.

Ключові слова: стеганографія, клітинний автомат, захист інформації, стеганографічний контейнер.

Проблема захисту інформації від несанкціонованого доступу є надзвичайно актуальною на даний момент. Можливість використання традиційних криптографічних методів не знімає проблеми надійного захисту даних через те, що зашифровані дані самі по собі привертають увагу противної сторони [1]. Результатом цього може стати застосування противною стороною як методів дешифрування даних, так і «некомп'ютерних силових» методів для одержання зашифрованої інформації. Виходячи із цього, на теперішній час досить актуальними є дослідження в галузі стенографічного захисту інформації [2, 3], який на відміну від криптографії не закриває дані від противної сторони, а приховують від неї сам факт існування таких даних.

Мета даної роботи полягає в підвищенні якості захисту інформації (яка виражається в зменшенні ймовірності виявлення факту вбудовування даних в мультимедійний трафік) за рахунок розробки методики приховування даних. В роботі пропонується методика, основана на спільному застосуванні теорії стеганографії та теорії клітинних автоматів [4]. Методика являє собою послідовність дій, виконання яких приводить до приховування даних в растровий графічний контейнер. Первісними даними для процесу виконання методики є: протокол вбудовування даних P; растровий графічний контейнер I; секретна двійкова послідовність $s_0, s_1, s_2, \dots, s_k$, яку необхідно вбудувати в контейнер.

Запропонована методика передбачає використання клітинного автомату, що визначається як множина наступного виду:

$$C = \{c(x, y) \mid c(x, y) = <X, A, \delta, a_{\text{begin}}>\},$$

де $c(x, y)$ — квадратна клітина з 8 сусідами, яка ідентифікується двома координатами x та y;
$X = \{x_1, x_2, \dots, x_8\}$ — множина вхідних сигналів клітини;
$A = \{a_0, a_1, \dots, a_n\}$ — множина внутрішніх станів клітини, в найпростішому випадку клітина має два стани: $A = \{a_0=0, a_1=1\}$);
$\delta : X \times A \to A$ — функція переходів клітини;
a_{begin} — значення початкового стану клітини.

Растровий графічний контейнер, в який вбудовується секретна інформація, визначимо в такий спосіб:

$$I = \{p_I(x, y) \mid p_I(x, y) = (R_{pI}, G_{pI}, B_{pI})\},$$

де $p = p_I(x, y)$ — позиція (точка) в контейнері, яка задається двома цілими значеннями координат x та y;
R_{pI}, G_{pI}, B_{pI} — відповідно, красний, зелений та синій колірний канал точки.

Протокол вбудовування даних в графічний контейнер визначається як п'ятикомпонентний кортеж:

$$P = <InitCell, Rules, Evolution, Order, Color>,$$

де *InitCell* — множина початкових значень клітин автомата;
Rules — правила зміни станів клітин автомата (функція δ);

Evolution — кількість еволюцій (змін станів) клітинного автомата, які необхідно виконати для отримання маркування точок, що приховують дані;

Order — правило, яке задає порядок зчитування маркованих точок з графічного контейнера;

Color — колірна складова маркованої точки контейнеру, в яку вбудовані приховані дані.

Методика вбудовування секретних даних складається з семи кроків.

Крок 1: формування структури клітинного автомата шляхом визначення необхідної кількості його клітин.

Крок 2: встановлення для отриманого клітинного автомата правил зміни станів клітин, тобто функції їх переходів.

Крок 3: визначення системи двох цілих координат та зіставлення графічного контейнера з отриманим на попередніх кроках клітинним автоматом, відповідно до наступного відображення:

$$L_{CI}: C \to I = \{(c(x, y), p_I(x, y)) \mid x = 1..n, y = 1..m\}.$$

Дане відображення являє собою множину пар (двокомпонентних кортежів), перша компонента яких є клітиною з координатами (x, y) в клітинному автоматі, а друга – точкою мультимедійного контейнера з цими самими координатами (x, y).

Крок 4: застосування до клітин автомата початкових значень, які визначаються відповідно до компоненти *InitCell* протоколу *P*.

Крок 5: виконання еволюцій клітинного автомата з одночасним інкрементуванням лічильника еволюцій, доки значення лічильника не досягне значення компоненти *Evolution* протоколу *P*.

Крок 6: формування списку промаркованих клітинним автоматом точок графічного контейнеру.

Крок 7: вбудовування даних в точки, які містяться в списку промаркованих точок графічного контейнеру. Вбудовування розрядів секретної послідовності передбачає застосування будь-якого методу просторового стеганографічного вбудовування. При цьому колірна складова для вбудовування визначається компонентою *Color* протоколу *P*.

Отриманий за запропонованою методикою контейнер містить вбудовані дані в точках, промаркованих клітинним автоматом відповідно до розробленого протоколу вбудовування. За відсутності попередньої домовленості між відправником та отримувачем контейнера щодо протоколу вбудовування, інформація про порядок вбудовування та добування даних, яка міститься в протоколі *P*, інтерпретується як ключ приховування.

На основі теоретичних положень запропонованої методики було розроблено програмне забезпечення, яке реалізує відповідне вбудовування даних. В середовищі розробленого програмного забезпечення проведені дослідження запропонованої методики, які показали, що її використання на 4—8% зменшує ймовірність статистичного виявлення приховування порівняно з традиційними методами послідовного, детермінованого та псевдовипадкового приховування даних в просторовій області графічних контейнерів при використанні однакового методу вбудовування розряду секретної послідовності в точку контейнера.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Конахович Г.Ф., Пузыренко А. Ю. Компьютерная стеганография.— Киев: МК-Пресс, 2006.

2. Грибунин В. Г. Цифровая стеганография.— Москва: Салон-пресс.— 2002 г.

3. Аграновский А. В., Балакин А. В., Грибунин В. Г. Стеганография, цифровые водяные знаки и стегоанализ.— Москва: Вузовская книга.— 2009.

4. Тоффоли Т., Марголус Н. Машины клеточных автоматов.— Москва: Мир, 1991.

A. A. Tsisar, K. V. Zashcholkin

A method of data hiding based on the cellular automata approach.

The procedure of embedding data into a graphic container, based on the general application of the theory of steganography and the theory of cellular automata. The procedure consists in determining the number of positions, which house the hidden data, and the order they are read in by using a cellular automata. Incorporation and retrieval of the built-in data is done with the use of the proposed hiding protocol.

Keywords: *steganography, embedding data, cellular automata, information security, steganographic container.*