АЛГОРИТМ НЕПРЯМОГО МАСКУВАННЯ ДАНИХ НА БАЗІ ПОТОКОВИХ КОНТЕЙНЕРІВ У ДИНАМІЧНОМУ ВІДЕОСЕРЕДОВИЩІ

Столяренко А.Г.
ХНУРЕ, кафедри ІМІ, студент
Костромицький А.І.
ХНУРЕ, кафедри ІМІ, доцент
Твердохліб В.В.
ХНУРЕ, кафедри ІМІ, асистент

Сьогоднішня структура інформаційних потоків, що надсилаються мережею, характеризується ростом відсотку даних, які мають бути захищеними від несанкціонованого доступу. При цьому, останнім часом частішають випадки зламу шифрованих даних, як наслідок морального старіння ряду традиційних методів, зокрема, RSA, так і розширення технічних можливостей зловмисників. За таких умов альтернативою шифруванню можуть виступати технології маскування критичних даних, у першу чергу – технології стенографії. Разом з тим, існуючим стегосистемам властивий ряд недоліків та обмежень, головними з яких є:

- низька захищеність (P) прихованих даних від засобів стегоаналізу;
- недостатня ємність (V) стегосистеми.

Такі недоліки викликані:

- залежністю між величинами P та V, що має наступний характер:

$$V \uparrow \rightarrow P \downarrow \qquad (1)$$

- архітектурною недосконалістю переважної більшості традиційних стеганографічних методів [3,4].

Зокрема, LSB-методи є вразливими до таких методів стегоаналізу, як візуальна атака, гістаграмний та RS-методи, атака на базі архівування.

У зв’язку з цим, пропонується до використання модифікований алгоритм стеганографічного вбудовування на базі LSB-підходу, що використовує контейнери графічного типу має такі відмінності відносно базового методу:

1. Застосовуються контейнери потокового типу. При цьому, середовищем передавання є відео реального часу.
2. Контейнери реалізуються на базі кадрів B-типу відеопотоку.
3. Не використовується пряме вбудовування даних секретного повідомлення. Модифікації підлягає динамічний діапазон двійкового опису трансформованого сегменту даних. У цьому випадку може бути задіяно як сегменти яскравості, так і хроматичні сегменти.

Вибір B-кадрів тут пояснюється практичною відсутністю структурних відмінностей для пустого контейнеру, та контейнеру, заповненого у запропонований спосіб. При цьому, забезпечується достатня ємність стегосистеми без зниження степеню захищеності від викриття. Додатково може бути задіяно механізми вибору B-кадрів з потоку для інкапсуляції як з використанням фіксованих правил, так і на базі хеш-функції від кадрів з певними індексами.

Ключове завдання, яка потребує вирішення для успішної реалізації методу, є розробка універсального способу відновлення модифікованих сегментів на прийомному боці.

Список літератури:

1. Недоліки алгоритму цифрового підпису RSA [Електронний ресурс] – Режим доступу: http://um.co.ua/9/9-4/9-48994.html.

2. Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355-372

3. Fridrich Y. Steganography in Digital Media: Principles, Algorithms and Applicaticks. Cambridge Press, 2010. 462 p.

4. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. - К.: МК-Пресс, 2006. - 288 с.