УДК 004.891

В.М. ДЖУЛІЙ, Є.О. КОВРИГА
Хмельницький національний університет

МЕТОДИ ВПРОВАДЖЕННЯ НФОРМАЦИИ В ФАЙЛИ ФОРМАТУ WAV І MIDI

В статті наведено опис розроблених методів організації прихованого каналу зв'язку на основі WAV і MIDI-файлів і методу статистичного стегоаналіза звукового файлу. Дана характеристика стійкості до злому описаних методів і наведено оцінку пропускної спроможності прихованого каналу передачі інформації, організованого на основі зазначених методів.

Ключові слова: *стеганографія, контейнер, прихований канал, секретний ключ.*

V.M. DZULIY, E A. KOWRYHA
Khmelnytsk national university

METHODS OF INTRODUCTION OF INFORMATION IN FILES WAV AND MIDI

The paper describes the developed methods covert communication channel based on WAV and MIDI-files and statistical method stegoanalysis sound file. The characteristic resistance to cracking described methods and provides an assessment of the capacity of hidden information channels, organized on the basis of these methods.

Keywords: *steganography, container, hidden channel, the secret key*

Вступ. Захист інформації може бути забезпечений або криптографією, або стеганографією, або одночасно за допомогою криптографії та стеганографії. При використанні криптографії інформація модифікується за певним алгоритмом, в результаті перетворень ховається сенс повідомлення. Стеганографія приховує сам факт передачі або зберігання інформації шляхом впровадження інформації в різні мультимедійні об'єкти, які не втрачають від цього своїх споживчих властивостей. Відносно обчислювальної техніки виділився окремий напрямок - комп'ютерна стеганографія. Як контейнери тут використовуються файли різних форматів, мережеві пакети і т.д. Найпоширенішим методом впровадження інформації в звукові файли є метод заміни найменшого значущого біта (LSB - Least Significant Bit). В даний час більшість програм, які використовують в якості контейнерів дискретні звукові сигнали, впроваджують інформацію тільки методом LSB, на відміну від програм, що використовують текстові та графічні контейнери. Це пояснюється складністю реалізації альтернативних методів впровадження інформації в звукові сигнали (метод фазової варіації, метод розширення спектра, метод впровадження за допомогою луна-сигналу) і малим об'ємом секретної інформації, що пересилається по таємного каналу зв'язку, організованому на основі зазначених методів. З іншого боку, стеганографія може застосовуватися в протизаконних цілях, наприклад, для несанкціонованої передачі комерційних або державних секретів, листування терористичних угруповань. Тому з'являється необхідність у розробці ефективних методів виявлення прихованих вкладень в мультимедійних об'єктах.

В даний час нерідко спостерігаються випадки несанкціонованого використання мультимедійної продукції (фотографій, аудіо- та відеофайлів). Одним із прийомів захисту авторських прав є приховане впровадження міток (маркерів, водяних знаків) в мультимедійні файли, що захищаються. Виявлення цих міток дозволяє порушнику видалити водяні знаки з контейнера. Очевидно, що впровадження прихованої інформації в мультимедійні файли слід здійснювати таким чином, щоб порушник не зміг виявити і видалити зроблені зміни в контейнері. Файл формату WAV містить в собі квантовані цифрові значення амплітуди сигналу, виміряні в дискретні моменти часу (так звані відліки). Для файлу формату WAV найбільш відомим і поширеним методом приховування секретної інформації є метод заміни найменшого значущого біта. При впровадженні інформації в звукові файли формату WAV методом найменшого значущого біта, доводиться вирішувати завдання вибору номера розряду відліку, в який можна помістити приховувану інформацію, з урахуванням двох конфліктуючих вимог. З одного боку, необхідно збільшувати обсяг прихованої інформації в одному файлі (збільшувати пропускну здатність каналу), а з іншого боку, потрібно забезпечити високий ступінь скритності вкладеної інформації.

Основна чистина. Метод просторового розподілу інформації. Істотно ускладнити зловмисникові відновлення повідомлення можна шляхом розміщення біт повідомлення не в одному, а в кількох файл-контейнерах (здійснити передачу інформації, по декількох каналах). Порядок розподілу інформації по контейнерах визначається секретним ключем. У цьому випадку, навіть якщо знати про наявність в файлах прихованого повідомлення, відновити його стає складніше, ніж при простому методі LSB. Алгоритм просторового розподілу інформації полягає в наступному (рис. 1): перший біт приховуваного повідомлення записується в перший файл-контейнер, другий - в другий файл-контейнер, третій - в третій файл-контейнер; четвертий - в четвертий файл-контейнер; пятий - в перший, і так далі поки не закінчаться біти повідомлення. При використанні звукового потокового мовлення розпорошення ведеться між різними каналами зв'язку. В файл-контейнер біти записуються методом LSB. Інформацію перед впровадженням в файл-контейнер, доцільно зашифрувати симетричними шифрами, що використовуються в якості стандартів в США і в Україні – AES. Зазначений шифр при використанні, ключа довжиною 256 біт практично неможливо розкрити методом «грубої сили» (повного перебору).

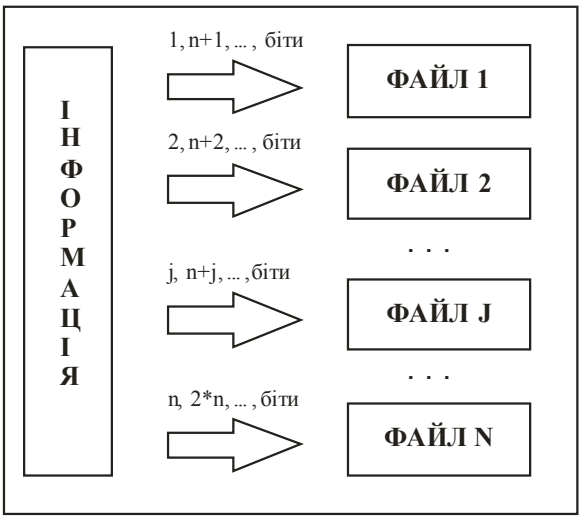

Рис. 1. Схема просторового розподілу інформації

Розподіл інформації по декількох контейнерів дозволяє істотно підвищити стійкість інформації до розкриття зловмисниками. Захищеність впровадженої інформації залежить від кількості використовуваних файл-контейнерів, тобто від довжини ключа. При використанні чотирьох файл- контейнерів кількість додаткових ключів становить $k = n! = 4! = 24$, де n - довжина ключа в бітах. При використанні десяти файл-контейнерів кількість можливих ключів досягає $k = n! = 10! = 3628800$. Слід мати на увазі, що це додаткові ключі. Поле ключів, використовуване при шифруванні (воно визначено відповідним стандартом), залишається незмінним. Вважаючи, що комп'ютер може перебрати мільйон ключів в секунду, повний перебір 128-бітного криптографічного ключа займе 10^{25} років. Зауважимо, що планета Земля існує $5 \cdot 10^9$ років. З урахуванням часу, що витрачається на перебір 128-бітного криптографічного ключа для дешифрування повідомлення, розкриття повідомлення методом повного перебору всіх можливих комбінацій десяти файл-контейнерів потребує 10^{37} років. Ще однією перевагою розподілу інформації по декільком контейнерам (просторовий розподіл) є можливість передавати файл-контейнери по декількох відкритих каналах зв'язку. Це істотно знижує ймовірність перехоплення зловмисником всіх частин повідомлення.

Прихований канал зв'язку, заснований на використанні даного методу, має пропускну здатність, рівну пропускної здатності прихованого каналу зв'язку, організованого методом LSB. Пропускна здатність методу LSB дорівнює 1000 біт / с на 1000 Гц частоти дискретизації звукового сигналу. Отже, якщо врахувати розподіл повідомлення по декільком файл-контейнерів, інформацію можна передавати паралельно по декільком прихованим каналам зв'язку. У такому випадку пропускна здатність прихованого каналу зв'язку складе:

$$P = \sum_{i=0}^{n} P_i \qquad (1)$$

де n - кількість файл-контейнерів, P - пропускна здатність i - ого файл-контейнера. При частоті дискретизації звукового сигналу 44100 Гц, пропускна здатність прихованого каналу зв'язку на основі метода- LSB складає 44100 біт/с. При організації прихованого каналу зв'язку методом просторового розподілу інформації на основі десяти файл-контейнерів, пропускна здатність прихованого каналу зв'язку у відповідності з формулою (1) буде становити $P = n \cdot P = 10 \cdot 44100 = 441000$ біт/с.

Іншим методом, що дозволяє підвищити стійкість, є метод часового розподілу інформації. В даному методі біти повідомлення розподіляються рівними частинами по файл-контейнеру, не змінюючи відліків, що містять «тишу». На рис. 2 показані відліки аудіо-файлу, що містять звуковий сигнал і «тишу», а також впровадження інформації тільки в ті з них, в яких присутній сигнал.

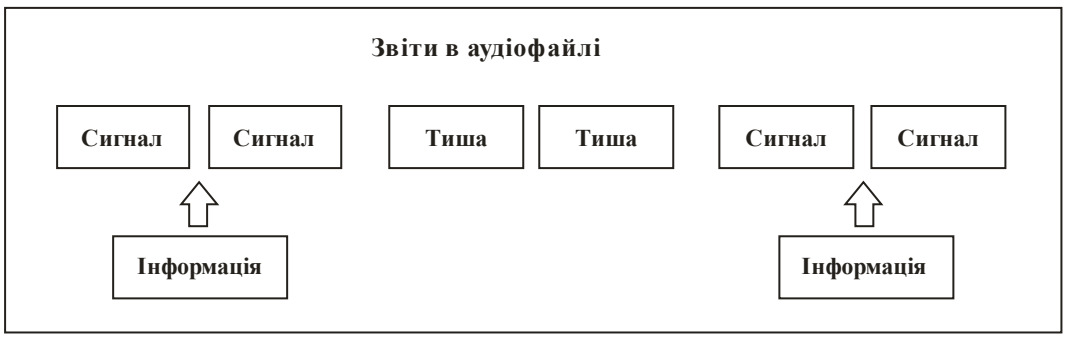

Рис. 2. Схема часового розподілу інформації

Суть методу полягає в тому, що в області даних аудіофайлу в кожному відліку замінюється кілька молодших біт в межах від 1 до 8 значеннями біт інформації користувача. Також область даних аналізується на наявність «тиші», і, якщо вона виявлена, то поточний відлік пропускається. Такий метод розподілу інформації по файл-контейнеру дозволяє захистити впроваджену інформацію від виявлення вкладення методом спектрального стегоаналіза. Відсутність вкладення в звітах, що містять «тишу», не дозволяє виявити це вкладення, аналізуючи характеристики амплітудного спектра звукового сигналу, що міститься в файл-контейнері. Пропускна спроможність прихованого каналу зв'язку, організованого на основі даного методу, складе:

$$P = \frac{(100 - k) \cdot P_L}{100}, \qquad (2)$$

де k - тривалість ділянок «тиші» у відсотках, PL – пропускна здатність методу LSB для розрахункового файл-контейнера. Для мовних звукових сигналів в середньому припадає 913 ділянок «тиші» на годину (0,2536 ділянок «тиші» в секунду), для музичних – 200 ділянок «тиші» на годину (0,0556 ділянок «тиші» в секунду). Тривалість ділянок «тиші» становить 5% часу звукового сигналу. Таким чином, пропускна здатність даного методу для файл-контейнера з частотою дискретизації 44100 Гц і пропускною здатністю методу LSB - 44100 біт/с відповідно до формули (2) становитиме $P = \frac{(100-5)\cdot 44100}{100} = 41895\,біт/с$. Це становить 95% від максимальної пропускної здатності каналу.

Для впровадження інформації в MIDI-файли можна використовувати наступні події і параметри: портаменто; text; lyric; номер ноти; гучність звучання ноти; тривалість звучання ноти. Портаменто - це ефект плавного переходу по висоті тону від однієї ноти до наступної ноти. Даний ефект полягає в тому, що нота починає звучати на висоті попередньої ноти, а закінчує звучання на своїй нормальній висоті. Задіяти режим портаменто можна за допомогою перемикача Portamento, що визначається повідомленням зміни режиму управління з параметром 65 зі значенням від 64 до 127. Щоб відключити режим портаменто, необхідно використовувати перемикач Portamento значенням від 0 до 63. Параметром ефекту портаменто, що впливає на відтворення ноти, є час портаменто, тобто час, за який відбувається зміна висоти тону. Часом портаменто керує подія Portamento Time - повідомлення зміни режиму керування з параметром 5, значення цієї події визначає старшу частину часу портаменто. Повідомлення зміни режиму керування з параметром 37 визначає молодшу частину часу портаменто. Text - це мета-подія, яка визначає текстовий рядок, що складається зASCII-символів. Дана подія ніяк не впливає на відтворення звуку, її можна побачити тільки в секвенсорі або музичному редакторі. Ця подія допомагає розробнику орієнтуватися у списку подій і полегшує спільну роботу над одним твором. Текстові події можуть розташовуватися в будь-якому місці треку в якості слів пісні або коментаря. Lyric - це мета-подія, що визначає слова пісні, які повинні бути виконані у визначений час. Кожен склад повинен бути представлений окремою мета-подією Lyric з заданим часом виконання, склад також складається з ASGII-символів.

Впровадження інформації в MIDI-файли можна робити зміною часу портаменто. Необхідною умовою роботи цього методу є відключений режим портаменто, щоб впроваджена інформацію не впливала на звучання музичного твору (не спотворювала його). Для впровадження інформації необхідно застосовувати подію зміни режиму керування з номером 5 і подію зміни режиму управління з номером 37, які визначають старшу і молодшу частину часу портаменто. У разі застосування цих подій для впровадження інформації, в їх значеннях будуть кодуватися старший і молодший півбайти символа.

Наявність текстової інформації в MIDI-файлі дозволяє скористатися прийомами текстової стеганографії для впровадження секретних повідомлень. З огляду на те, що дані текстові події не підтримують будь-яке форматування, крім зміни шрифту всього тексту, а подія Lyric також не може містити більше пропусків після слів, найбільш прийнятним способом впровадження інформації є заміна українських букв схожими за зображенням буквами латинського алфавіту. Якщо в слові присутні букви, схожі з латинськими, і перша з них замінена на латинську, то в даному слові закодована логічна одиниця. Якщо в слові присутні букви, схожі з латинськими, і перша з них не замінена на латинську, то в даному слові приховано логічний нуль. Для збільшення обсягу впроваджуваної інформації можна використовувати кожну кириличну букву, схожу за написанням з латинської. Якщо така буква замінена, то це є закодована одиниця, інакше - закодований нуль.

Для файлів формату MIDI, що містять послідовні записи подій, найбільш відповідним є ключ, який показує наскільки подій вліво або вправо від поточного положення необхідно переміститися для зчитування півбайта (чотири біта) впровадженої інформації. Алгоритм добування інформації з події визначається типом самої події і її параметрами. Довжина ключа залежить від кількості подій в MIDI-файлі. Для того щоб ключ не мав обмежень по кількості подій, що визначають інтервал, між напівбайтами впровадженої інформації, необхідно використовувати запис числа, у вигляді величини змінної довжини. Такий підхід застосовується в SMF для кодування інтервалу часу між записаними подіями. В даному методі представлення цілих чисел під саме число не треба відводити фіксовану кількість байт. Початкове число записується в кілька байт, по сім біт. У перший байт записується сім біт, тому що старший розряд визначає напрямок переміщення по файлу (0- вперед, 1 - назад). В другому і подальших байтах перший біт позначає перший і останній байти в

послідовності. Другий і наступні байти повинні містити в першому розряді одиницю, останній байт – нуль.

Наприклад, ключ призначений для зчитування півбайта інформації з MIDI -файла переміститься вперед на 16383 подій в двійковому виді буде виглядати наступним чином: 10000000111111101111111. Число 16383 в двійковому виді записується як 11111111111111, в ньому чотирнадцять значущих біт, отже для його зберігання в вигляді величини змінної довжини необхідно використовувати три байти. Останній, третій байт, як завершальний в першому розряді містить 0, в. інших розрядах сім останніх одиниць вихідного числа. Другий байт в першому розряді містить одиницю, показуючи, що цей байт не є завершальним у серії. В решті розрядах містить сім передостанніх одиниць вихідного числа. Перший байт в першому розряді містить одиницю, приписуючи відлік подій вести вправо, наступні розряди цього байта містять нулі, так як всі значущі байти вихідного числа вмістилися в двох останніх байтах. Таким чином, стійкість ключа визначається загальною кількістю подій в MIDI-файлі і кількістю подій, на які необхідно переміститися вперед або назад для читання наступного півбайта прихованої інформації. У загальному випадку число можливих ключів становить $K = 2 \cdot n$, де n - кількість вбудованих байт. Об'єм інформації (в бітах), який можливо впровадити в один MIDI-.файл, оцінюється за наступною формулою:

$$P = \frac{R + T + N_N + N_V + N_L}{K} \cdot 4, \qquad (3)$$

де R - кількість подій, що дозволяють впровадити інформацію шляхом зміни часу портаменто, T - кількість подій, що дозволяють впровадити інформацію в текст, N_N - кількість подій, що дозволяють впровадити інформацію шляхом заміни номера ноти, N_V - кількість подій, що дозволяють впровадити інформацію шляхом заміни гучності звучання ноти, N_L - кількість подій, що дозволяють впровадити інформацію шляхом заміни тривалості звучання ноти, K – загальна кількість подій в MIDI-файлі, четвірка у формулі (3) вказує на кількість біт, які можна впровадити в одній події.

Висновки. Наведено опис розроблених методів організації прихованого каналу зв'язку на основі WAV і MIDI-файлів і методу статистичного стегоаналізу звукового файлу. Дана характеристика стійкості до злому описаних методів і наведено оцінку пропускної спроможності прихованого каналу передачі інформації, організованого на основі зазначених методів. Для методу стегоаналізу наведена оцінка кількості вірно прийнятих рішень.

Література

1. Грибунин В.Г. Цифровая стеганография. /В.Г.Грибунин, И.Н.,Оков И.В.,Туринцев // М.: СОЛОН-Пресс; 2002. - 261 с.

2. Конахович Т.Ф. Компьютерная стеганография / Т.Ф Конахович, А.Ю Пузыренко // Теория и практика. Киев: МК-Пресс, 2006. -288с.

3. Мамаев М. Технологии защиты информации:в Интернете/ Мамаев М., Петренко С. //: Специальный;справочник..СИб::Иитер 2002. -848 с.

4. Хайкин С. Нейронные сети. / Хайкин С. //Полный курс: пер. с англ. / 2-е изд. М.: Издательский дом «Вильяме», 2006. -1104 с.

References

1. Hrybunyn VG Tsyfrovaya steganography. /V.H.Hrybunyn, IN, shackles IV, Turyntsev // .: SOLON M-Press; 2002 - 261 p.

2. Konahovych TF Kompyuternaya steganography / T.F Konahovych, A.YU Puzыrenko // Theory and Practice. Kiev: MK-Press, 2006 -288s.

3. Mamaev M. Technologies of protection of information: on the Internet / M. Mamaev, S. Petrenko //: Spetsyalnыy; spravochnyk..SYb :: Yyter 2002 -848 p.

4. Haykyn S. neural network. / Haykyn S. // Polnыy course: Lane. with the English. / 2nd ed. M .: Yzdatelskyy home "Vylyame" 2006. -1104 p.

Рецензія/Peer review : 19.12.2014 р. Надрукована/Printed :2.1.2015 р.