УДК 004.891

к.т.н. **Гришин С.П.** (НМЦКП МОУ)
Коврига Є.О. (ХмНУ)
Березовська Ю.В. (ВІКНУ)

АНАЛІЗ МЕТОДІВ ВПРОВАДЖЕННЯ ІНФОРМАЦІЇ В ЗВУКОВІ ФАЙЛИ

В статті проведено аналіз існуючих методів впровадження інформації в звукові файли. Наведено аналіз існуючих програм впровадження інформації в звукові файли, виявлено їх переваги та недоліки. Розглянуті можливі області застосування стеганографії, зокрема-стеганографія може бути використана для зберігання і розподілення ключів в мережах. Виявлені недоліки методів впровадження інформації в звукові файли, їх програмні реалізації не дозволяють в повній мірі використовувати їх для безпечної передачі інформації.

Розглянуті методи впровадження інформації в файли формату MIDI не можуть застосовуватися для захисту авторських прав, зважаючи на відсутність секретного ключа, тому необхідно вирішити задачу захисту авторських прав і забезпечити секретність впровадження за допомогою ключа розподілу.

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

Вступ. Зростаючі можливості сучасних засобів зв'язку вимагають розробки спеціальних засобів безпечного зберігання та передачі інформації. Мережева безпека стає все більш актуальною з огляду зростаючих обсягів даних, що пересилаються по локальних і глобальних мережах. Для захисту інформації від несанкціонованого доступу та використання необхідно забезпечити конфіденційність і цілісність даних. Захист інформації може бути забезпечено криптографією, стеганографією, або одночасно криптографією і стеганографією. При використанні криптографії інформація модифікується, перетворюється. В результаті перетворень приховується зміст повідомлення. Стеганографія, в свою чергу, приховує сам факт передачі або зберігання інформації. Це досягається шляхом впровадження інформації, що захищається, в різні мультимедійні об'єкти (контейнери), які не втрачають від цього своїх споживчих властивостей. Відносно обчислювальної техніки виділився окремий напрямок стеганографії - комп'ютерна стеганографія. Як контейнери тут використовуються файли різних форматів, мережеві пакети і т.д. Наприклад, інформацію можна впровадити в звуковий сигнал, який згодом відтворюється практично точно так (з тією ж якістю), як вхідний сигнал без впровадження. Найпоширенішим методом впровадження інформації в звукові сигнали є метод заміни найменшого значущого біта (LSB - Least Significant Bit). В даний час більшість реально працюючих програм, які використовують як контейнери дискретизовані звукові сигнали, впроваджують інформацію тільки простим 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 ехо-сигналу) і малим об'ємом секретної інформації, що пересилається по таємному каналу зв'язку, організованому на основі зазначених методів.

З іншого боку, стеганографія стала доступна для більшості користувачів і може застосовуватися в протизаконних цілях, наприклад, для несанкціонованої передачі комерційних або державних секретів; переписки терористичних угруповань. Тому з'являється необхідність у розробці ефективних методів виявлення прихованих вкладень, в мультимедійних об'єктах, переданих в комп'ютерних мережах.

Модель каналу з прихованою передачею інформації. Стеганографія, як наука, визначається наступним чином - це науковий напрям, що вивчає способи прихованої передачі або зберігання інформації, при цьому прихований канал зв'язку організується на основі відкритого каналу зв'язку з урахуванням особливостей сприйняття інформації. Існують три напрямки стеганографії для організації прихованого каналу передачі інформації: класичне - приховування інформації в потоках даних так, щоб неможливо було виділити або виявити якусь приховану складову частину; комп'ютерне - приховування інформації, в різних комп'ютерних об'єктах, що представляють собою різні файли, програми, пакети

мережевих протоколів і т.д .; цифрове - приховування інформації в цифрових даних, мають аналогову природу (зображення, аудіо дані і відеодані).

Стеганографічна система (стегосистеми) - це сукупність засобів і методів, за допомогою яких створюється прихований канал передачі інформації. Контейнер - будь який файл, призначений для впровадження приховуваного повідомлення. Приховуване повідомлення - повідомлення, впроваджуване в контейнер.

Повідомленням може бути секретний текст, зображення, фотографія, мітка, водяний знак. Стеганографічний канал (стегоканала) - канал передачі заповненого контейнера (Стего). Стегоключ (ключ) - секретні дані, використовувані в процесі впровадження приховуваного повідомлення в контейнері. На рисунку 1 представлена узагальнена модель стегосистеми і проілюстровані наведені визначення.

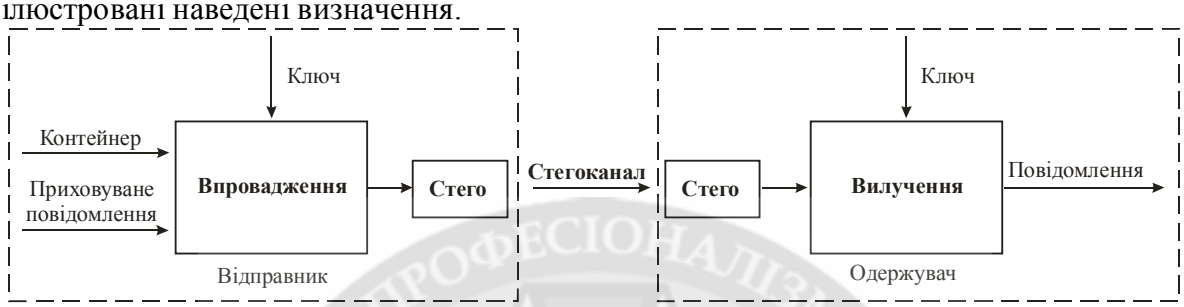

Рис. 1. Узагальнена модель стегосистеми

Відповідно до даної моделі, на стороні відправника приховуване повідомлення впроваджується в контейнер за спеціальним алгоритмом впровадження та ключем. Заповнений контейнер передається по відкритим каналам передачі даних одержувачу. На стороні одержувача із заповненого контейнера витягується вхідне повідомлення за алгоритмом витягування і ключем.

Комп'ютерна та цифрова стеганографія. Широке поширення мультимедійних технологій дало імпульс розвитку нових і вдосконаленню існуючих методів приховування інформації, а також сприяло виникненню більш складних методів організації прихованих каналів зв'язку, в основу яких були покладені особливості подання інформації в комп'ютерних файлах, пристроях, обчислювальних мережах і т.п. Комп'ютерна стеганографія застосовується для захисту ліцензійного програмного забезпечення, маскування мережевого трафіку, прихованого зберігання інформації. Основними положеннями організації прихованого каналу зв'язку з використанням комп'ютерної стеганографії є наступні: методи впровадження інформації повинні забезпечити автентичність та цілісність файлу; передбачається, що противнику повністю відомі можливі методи впровадження інформації; методи впровадження інформації повинні зберігати основні властивості відкритого переданого контейнера; безпека методів впровадження грунтується на деякій невідомій противнику інформації - ключі; витяг вкладеного повідомлення повинен представляти собою складну обчислювальну задачу, навіть якщо факт приховування повідомлення став відомий противнику.

Методи комп'ютерної стеганографії розділяються на два класи:

- методи, засновані на надмірності інформації, (цифрова стеганографія);
- методи, засновані на використанні різних властивостей комп'ютерних форматів (форматна стеганографія).

До першого класу відносяться методи, які використовують молодші розряди цифрових відліків і методи, засновані на цифровій обробці сигналу. До другого класу відносяться методи видалення - ідентифікують заголовок файлу; методи впровадження інформації в невикористовувані області гнучких і жорстких дисків; методи впровадження інформації в текстові файли; методи, які використовують зарезервовані поля різних комп'ютерних форматів файлів.

З використанням цифрової стеганографії вирішують наступні завдання: вбудовування прихованої інформації; вбудовування цифрових водяних знаків; вбудовування ідентифікаційних номерів; вбудовування заголовків.
Класифікація існуючих методів стеганографії представлена на рисунку 2.

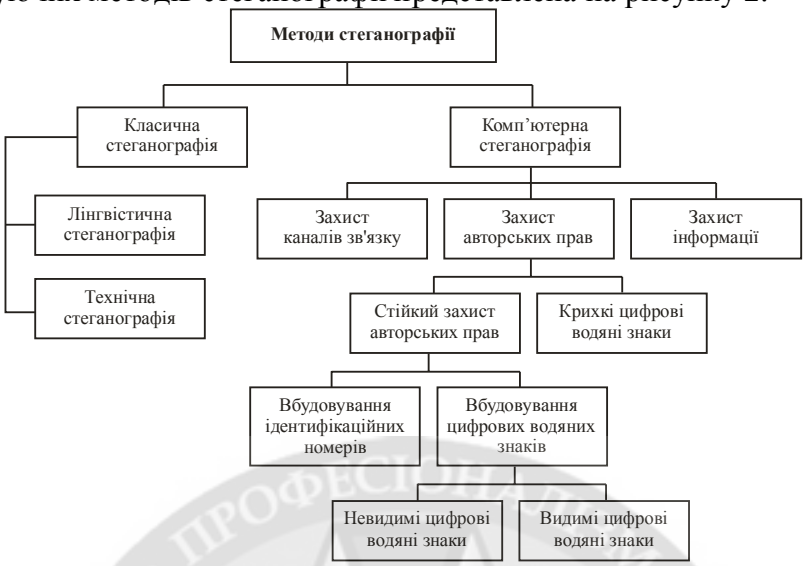

Рис. 2. Класифікація методів стеганографії

Цифрова стеганографія застосовується для захисту від копіювання і несанкціонованого використання, дозволяє захищати авторські права і інтелектуальну власність в області цифрової аудіо та відеоіндустрії. Для цього використовують вбудовування цифрових водяних знаків і ідентифікаційних номерів. Вбудовування невидимих заголовків застосовується для підпису медичних знімків та фотографій; нанесення легенди на карту, швидкого пошуку в базі даних по впровадженим в цифрові об'єкти ключовим словам, синхронізації відеопотоку зі звуком.

До методів організації прихованого каналу зв'язку засобами цифрової стеганографії пред'являються наступні вимоги:

- прозорість - відсутність помітних відмінностей між пустим контейнером і заповненим контейнером;
- стійкість до спотворень - впроваджена інформація повинна бути стійкою до різних перетворень, що відбуваються в процесі передачі інформації (вимога прозорості завжди конфліктує з вимогою стійкості до спотворень) ;
- стійкість до атак - впроваджена інформація може піддаватися взлому, видаленню або атакам (вимога стійкості до атак є головною вимогою пропонованою до будь-яких стеганографічних методів, однак досягти абсолютної стійкості впровадженої інформації до різного роду атак практично неможливо);
- можливість впровадження певного обсягу інформації - при істотному збільшенні обсягу впроваджуваної інформації знижується прозорість і стійкість до спотворень;
- секретність впровадження - у більшості випадків потрібно забезпечити секретність вбудованої інформації, її захист секретним ключем.

Методи впровадженні інформації в звукові сигнали. Метод заміни найменшого значущого біта. Формат файла WAV містить в собі дискретний, квантований, звуковий сигнал або абсолютні значення амплітуди в кожній точці дискретизації. Чим більше розрядність двійкового числа, використовуваного для представлення відліку, тим точніше відображається значення амплітуди. Заміна молодших розрядів цифрових сигналів є найпростішим способом впровадження конфіденційних даних. Метод має прийнятну стійкість до злому, дозволяє приховувати досить великий обсяг інформації в одному звуковому файлі, і якщо замінювати один останній біт, то спотворення звукового файлу будуть незначними. Наприклад, при довжині файлу 16 Мбайт і розмірі відліку 16 біт в ньому можна розмістити 1 Мбайт інформації. Для звукового файлу формату WAV з двома

звуковими каналами (стерео) і розміром відліку 16 біт найменшим значущим бітом є кожен шістнадцятий біт в кожному звуковому каналі. Аналогічно для звукового файлу з одним звуковим каналом; (моно) і розміром відліку 8 біт найменшим значущим бітом є кожен восьмий біт (рисунок 3).

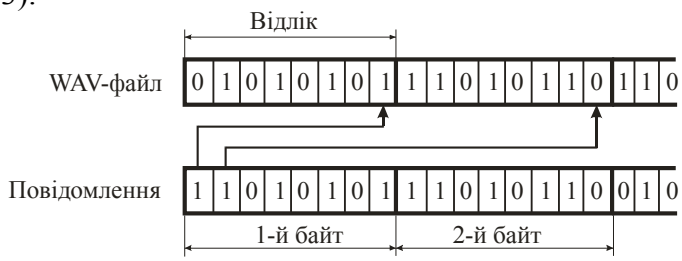

Рис. 3. Впровадження даних методом LSB

Зміна останнього біта у відліку призводить до незначної зміни амплітуди сигналу. Ці зміни в амплітуді сигналу неможливо визначити на слух. Недоліком вказаного методу є низька стійкість до виявлення прихованої інформації статистичними методами і до різних перетворень. Для підвищення стійкості впровадженої інформації необхідне застосування методів нормалізації локальних статистик молодших біт (модифікація молодших біт сусідніх відліків, таким чином, щоб статистики порожнього і заповненого контейнера не відрізнялися) і розподілення впроваджуваного секретного повідомлення по всьому контейнеру.

Метод модифікації фази. Існують різні варіації методів впровадження інформації на основі фазового кодування. Суть методів модифікації фази полягає в зміні фази кожної частотної складової дискретного сигналу. Для цього вихідний сигнал розбивають на серію коротких сегментів, що містять однакову кількість елементів (відліків). Кількість елементів повинна бути більше ніж кількість біт в переданому повідомленні. До кожного сегмента застосовують дискретне перетворення Фур'є. В результаті для кожного сегмента створюються масиви фаз і амплітуд, кількість елементів масиву рівна кількості елементів в сегментах. Для збереження скритності повідомлення необхідно зберігати різницю фаз між сусідніми сегментами, так як слухова система людини більш чутлива до різниці фаз, ніж до абсолютних значень фази. Модифікацію фаз формують в масиві фаз першого сегмента. Вбудовування інформації здійснюють шляхом заміни вихідного значення фази на значення, рівне $-\pi/2$, якщо біт повідомлення дорівнює 0, і значення $\pi/2$, якщо біт повідомлення дорівнює 1. Щоб зберегти існуючу різницю фаз, необхідно отриманий масив фаз першого сегмента скласти з обчисленою раніше різницею між першим і другим масивом фаз, і так далі для кожного масиву фаз. Для відновлення звукового сигналу необхідно виконати зворотне дискретне перетворення Фур'є для масивів амплітуд і модифікованих масивів фаз. Недоліком даного методу є низька пропускна здатність.

Метод розширення спектра. У даному методі інформацію вбудовують в звуковий сигнал незначною зміною амплітуди сигналу. Метод розширення спектра застосовується в радіозв'язку для забезпечення високої завадостійкості сигналу в каналах з високим рівнем шуму й ускладнення перехоплення сигналу. Завадостійкість забезпечується тим, що енергія сигналу розподіляється по широкому діапазону частот. Дана обставина ускладнює виділення сигналу на фоні шуму і, що більш важливо, робить сигнал стійким до внесення шуму. Застосування даного методу в стеганографії робить впроваджену інформацію стійкою до несанкціонованого вилучення і спотворення. В разі застосування даного методу для приховування інформації в звуковому сигналі, дані множать на псевдовипадкову послідовність і на основний несучий сигнал, в результаті отримують розширену послідовність. Щоб зробити отриманий послідовністю шум низьким, його необхідно ослабити. Рівень ослаблення вибирається залежно від вимог непомітності змін до несучого сигналу. В звуковому сигналі спотворення непомітні при ослабленні послідовності до рівня однієї сотої. Ослаблений сигнал послідовності підсумовують з основним несучим сигналом. Для вилучення впровадженої інформації одержувачу повинен бути відомий

немодифікований основний сигнал і псевдовипадкова послідовність, яка в даному випадку є ключем. Недоліком даного методу також є низька пропускна здатність.

Метод кодування з використанням ехо-сигналу. Метод впровадження інформації з використанням ехо-сигналу заснований на тому, що слухова система людини не може зафіксувати ехо-сигнал, якщо затримка між основним сигналом, і ехо-сигналом менше певного значення. Впровадження даних в звуковий сигнал виробляється шляхом підмішування до нього ехо-сигналу (рисунок 4).

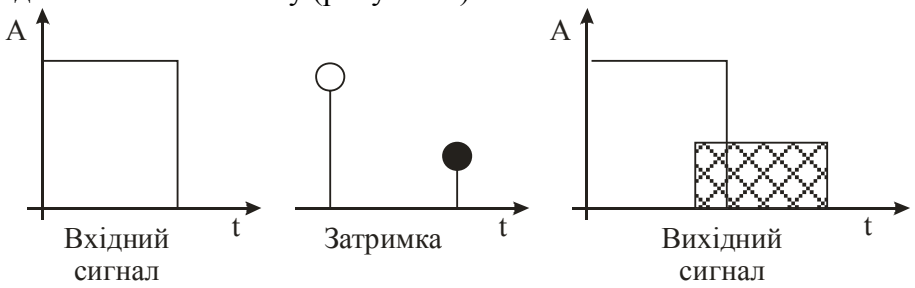

Рис. 4. Приклад ехо-кодування

Для вбудовування інформації в сигнал використовують дві часових затримки: одна для кодування нуля, інша для кодування одиниці. Щоб в звуковий сигнал можна було вбудувати декілька біт, його необхідно розбити на сегменти, що відповідають кількості біт в повідомленні. Кожен блок в цьому випадку розглядається, як окремий сигнал і використовується для кодування одного біта повідомлення. Для приховування інформації в звуковому сигналі необхідно створити одиничний і нульовий змішувані сигнали. Сума нульового змішуваного сигналу і одиничного змішуваного сигналу завжди має дорівнювати одиниці, щоб виключити різкі зміни в кінцевому сигналі. Недоліком методу є те, що для деяких звукових сигналів неможливо отримати достатню кількість правильно витягнутих біт впровадженого повідомлення.

Метод впровадження інформації варіацією різниці часу. Існує два підходи до впровадження інформації в MIDI-файли:

- використання подій MIDI;
- використання структури даних MIDI-файлу.

До першого підходу відноситься метод впровадження інформації в MIDI-файли шляхом варіації різниці часу між записаними в файл подіями, які не змінюють характеристики (налаштування) пристрою відтворення. Це відбувається, наприклад, коли поспіль слідують кілька однакових керуючих подій.

Для прихованої передачі інформації зазначеним методом використовується не тільки програмне регулювання гучності, а й інші керуючі події. Наприклад, здійснювати вимкнення неувімкненої ноти, підйом педалі, якщо вона не була натиснута, багаторазову установку стереобалансу на одне і те ж значення і т.д.

Недоліками даного методу прихованої передачі інформації є відсутність секретного ключа, який запобігав би можливості читання впровадженої інформації будь-яким користувачем. По суті, захист інформації утримується на секретності алгоритму, що суперечить правилу Керкхофа. Крім того, розглянутий метод має низьку стійкість до виявлення впровадженої інформації. Музикант, добре знайомий з форматом MIDI, легко виявить, що у файлі присутні «дивні» події. Звісно, що подібні події можна виявити автоматично спеціально розробленою програмою.

Метод впровадження інформації варіацією порядку запису подій. Впровадження інформації в MIDI-файл можна здійснити шляхом варіації порядку запису подій, що одночасно відбуваються. При використанні даного методу до файлу не додається нова інформація, і розмір файлу не змінюється. Даним методом зручно впроваджувати інформацію в одночасно виконувані ноти (акорди). Порядок запису нот в аркуші подій не має ніякого значення для відтворювальної апаратури, а варіація їх взаємного розташування при запису дозволяє кодувати переданий символ.

Висновки. На основі проведеного аналізу наведено поняття прихованого каналу передачі інформації, а також класифікація методів і завдань прихованої передачі інформації.

Проведено огляд існуючих методів впровадження інформації в звукові файли. Наведено аналіз існуючих програм впровадження інформації в звукові файли, виявлено їх переваги та недоліки. Розглянуті можливі області застосування стеганографії, зокрема-стеганографія може бути використана для зберігання і розподілення ключів в мережах зв'язку. Виявлені недоліки методів впровадження інформації в звукові файли і їх програмні реалізації не дозволяють в повній мірі використовувати їх для безпечної передачі інформації. Для організації прихованого каналу зв'язку, розподілу і передачі ключової інформації найбільш адекватним є метод впровадження інформації LSB, на відміну від інших розглянутих методів, він має високу пропускну здатність. Однак для його застосування в реальних задачах необхідно вирішити задачу підвищення стійкості до злому і спотворень. Розглянуті методи впровадження інформації в файли формату MIDI не можуть застосовуватися для захисту авторських прав зважаючи на відсутність секретного ключа, тому необхідно вирішити задачу захисту авторських прав і забезпечити секретність впровадження за допомогою ключа розподілу.

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.

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н., Гришин С.П., Коврига Є.О., Березовская Ю.В.

АНАЛИЗ МЕТОДОВ ВНЕДРЕНИЯ ИНФОРМАЦИИ В ЗВУКОВЫЕ ФАЙЛЫ

В статье проведен анализ существующих методов внедрения информации в звуковые файлы. Приведен анализ существующих программ внедрения информации в звуковые файлы, выявлены их преимущества и недостатки. Рассмотрены возможные области применения стеганографии, в частности - стеганография может быть использована для хранения и распределения ключей в сетях. Выявленные недостатки методов внедрения информации в звуковые файлы и их программные реализации не позволяют в полной мере использовать их для безопасной передачи информации. Рассмотренные методы внедрения информации в файлы формата MIDI не могут применяться для защиты авторских прав ввиду отсутствия секретного ключа, поэтому необходимо решить задачу защиты авторских прав и обеспечить секретность внедрения с помощью ключа распределения.

Ключевые слова: стеганография, контейнер, скрытый канал, секретный ключ.

Ph.D. Gryshin S.P., Kowryha E., Berezovskaya U.V.

ANALYSIS METHODS FOR INTRODUCING INFORMATION INTO SOUND FILES

The article analyzes the existing methods for the introduction of information into audio files. An analysis of existing programs to introduce information into audio files, identified their strengths and weaknesses. Possible fields of application of steganography, in particular - steganography can be used for storage and key distribution in networks. Identified disadvantages of introducing information into audio files and software implementations do not allow the full use of them for the secure transfer of information. The methods considered for the introduction of information in MIDI format files can not be used for copyright protection due to the lack of a secret key, so you need to solve the problem of copyright protection and to ensure the secrecy of the introduction to the key distribution.

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