**УДК 004.932**

**Грицик І. В, Земляков А.В.**

Національний університет «Львівська політехніка»

Кафедра електронних обчислювальних машин

Методи та засоби цифрової стеганографії для звукових сигналів

*© Грицик І. В, Земляков А. В., 2020*

**Проаналізовано існуючі засоби стеганографії. Проведено аналіз щодо переваг та недоліків кожного з методів кодування звуку. Показано перспективність застосування метода фозового кодування. Досліджено ефективність метода фазового кодування.**

**Ключові слова: криптографія, стеганографія, методи стеганографії.**

Вступ

У сучасному інформаційному суспільстві велика кількість послуг забезпечується за допомогою комп’ютерних мереж та інформаційних технологій. Інформація, що представлена в цифровому вигляді, має бути надійно захищена від багатьох загроз: несанкціонованого доступу та використання, знищення, підробки, витоку, порушення ліцензійних угод, відмови від авторства та ін. Захист інформації є вкрай важливим як в комерційній, так і в державній сферах.

Виклад основного матеріалу

 Сучасні комп’ютерні технології обробки даних істотно підвищили рівень інформаційної безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. Як відомо, на відміну від криптографічного захисту інформації стеганографічні програмні засоби намагаються насамперед приховати сам факт існування конфіденційної інформації. Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на основі комп’ютерної техніки і програмного забезпечення, становлять предмет вивчення цифрової стеганографії. Актуальність дослідження методів стеганографії невпинно зростає, адже з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу великої кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних.

Актуальність стеганографії

Щодо актуальності стеганографії в теперішній час, можна сказати, що комп'ютерна стеганографія розвивається доволі інтенсивно, застосовуються відомі і розробляються нові методи стеганографії, засновані на різноманітних областях науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стегоконтейнеру, що зберігає дані.

Таким чином, до теперішнього часу для цілого кола фахівців з'явилася необхідність ознайомлення з основами сучасної комп'ютерної стеганографії, завданням яких є не тільки розробка, аналіз або протидія засобам стеганографії, а й кваліфікований вибір існуючих засобів і їх вміле використання для вирішення конкретних прикладних завдань захисту інформації.

Види стеганографічних методів

 Залежно від виду спеціальних властивостей форматів розрізняють такі стеганографічні методи:

- Засновані на використанні зарезервованих для розширення полів комп'ютерних форматів файлів. Поля для розширення є в багатьох мультимедійних форматах і призначені для вдосконалення, оновлення і сумісності нових версій форматів зі старими. Як правило, ці поля заповнюються нульовою інформацією і не враховуються програмами, і тому можуть бути використані для передачі додаткової інформації. Недоліком цих методів є низький ступінь скритності і передача невеликих обсягів інформації, що приховується.

- Засновані на спеціальному форматуванні текстових файлів, відомі вже давно, використовувалися задовго до появи комп'ютерних технологій і включають в себе методи:

* використовують заздалегідь відоме зміщення слів, речень, абзаців в текстовому файлі, засновані на зміні положення рядків і розстановки слів в реченні, що виробляється вставкою додаткових пробілів між словами, збільшень проміжків непомітно візуально, але фактично передає приховану інформацію;
* засновані на виборі певних позицій букв (нульовий шифр). Наприклад, вибір п'ятої літери кожного останнього слова в рядку в межах однієї сторінки. Сюди ж відносяться художні прийоми тайнопису - акростих, добре відомий знавцям поезії, це така організація віршованого тексту, при якій, наприклад, початкові літери кожного рядки утворюють приховуване повідомлення;
* використовують спеціальні властивості полів форматів, які не відображаються на екрані. Наприклад, використання чорного шрифту на чорному тлі спеціальних «невидимих», прихованих полів для організації виносок і посилань.
* Засновані на приховуванні в невикористовуваних місцях гнучких дисків. Назва цієї групи говорить сама за себе і має ті ж переваги і недоліки, що і методи, засновані на використанні зарезервованих для розширення полів форматів.
* Засновані на імітуючій функції (мнемосхема-функція) - цей вид стеганографії заснований на генерації текстів і є узагальненням акровірша. Для заданого приховуваного повідомлення генерується осмислений текст, який містить приховуване повідомлення. При цьому текст є граматично і синтаксично правильним і статистично еквівалентним до текстів на подібну тему. Такі тексти можуть не бути підозрілими для систем моніторингу мережі, але все ж людина може швидко визначити відсутність будь-якого сенсу в змісті тексту.
* Засновані на використанні кодів, що виправляють помилки; приховування даних в додатковій інформації, використовуваної перешкодозахищеними кодами при виправленні випадкових помилок і забезпеченні точності передачі цифрового інформації. Якщо інформація захована, а на стороні прицмача код знятий, то спостерігач не буде навіть знати, що було відправлено повідомлення.
* Засновані на видаленні заголовка файлу. У цьому методі приховуване повідомлення шифрується і у результаті видаляється ідентифікація заголовку, залишаючи тільки шифровані дані, які видаються за випадкові, можливо, як спотворена інформація. Одержувач заздалегідь знає про передачу секретних даних і має недостатньо інформації. При цьому проблема приховування вирішується тільки частково. Цей метод не є повністю стеганографічним методом, а служить скоріше доповненням до них, хоча багато програмні засоби (White Noise Storm) забезпечують цю додаткову ступінь захисту з використанням алгоритму шифрування PGP.

Це лише деякі методи, що ілюструють евристичний підхід в стеганографії. Недоліками відомих методів, заснованих на використанні спеціальних властивостей форматів файлів, є:

* низький ступінь скритності (скритність грунтується на незнанні противником самого алгоритму приховування);
* передача невеликих обсягів інформації, що приховується.

Методи стеганографії аудіофайлів

 Особливий розвиток отримали стеганографічні методи приховування інформації у аудіосередовищі. Це охарактеризовано тим, що ССЛ працює у надширокому динамічному діапазоні і має доволі малий різницевий діапазон. Виходячи із цього, можна зробити висновок, що у аудіофайлах присутній широкий простір для приховування даних. Також ССЛ не здатна розрізняти абсолютну фазу, вирізняє лише відносну. Крім того, існують деякі види спотворень, викликаних зовнішнім середовищем, які можна використати для приховування даних.

Приховування даних в аудіо файлах особливо складне через його великий діапазон частот. Аудіосигнали також чутливі до випадкових шумів. Шум може бути виявлений, якщо він знаходиться в діапазоні від одного до мільйону у звукових файлах.

При приховуванні звуку користувач повинен скористатися перевагами слабкості людського слухового апарату, але також слід подбати про його високу чутливість.

**LSB кодування.** Дуже популярною методологією є LSB (найменший значущий біт) алгоритм, який замінює найменш значущий біт в деяких байтах файлу обкладинки, щоб приховати послідовність байтів, що містять приховані дані. Це, як правило, ефективна методика у випадках, коли заміни LSB не викликають значне погіршення якості.

У обчисленні, найменш значний біт (LSB) - це бітна позиція у двійковому цільовому числу, що дає одичні значення, тобто визначає чи є число парним або непарним. Іноді згадується LSB як найправильніший біт, завдяки конвенції в позиційному позначенні писати менш значущі цифри далі вправо. Він аналогічний найменш значущому знаку десяткового цілого числа, тобто цифра у крайній (праворуч) позиції.



Рисунок. 1. – Метод LSB для аудіо стеганографії

**Паритетне кодування.** Паритетне кодування - це один з надійних звукових стеганографічних методів. Замість того, щоб розбити сигнал на окремі зразки, цей метод розбиває сигнал на окремі зразки і вставляє кожен біт секретного повідомлення в біт парності. Якщо бітності обраної області не збігається з секретним бітом, який буде кодуватися, процес інвертує LSB одного з зразків у регіоні. Отже, відправник має більше вибору при кодуванні секретного біта.



Рисунок. 2. – Метод паритетного кодування

**Фазове кодування.** До методу фазового кодування закладено заміну фази первинного звукового сегмента на опорну фазу, що представляє собою дані, які необхідно приховати. Для того, щоб зберегти різницеву фазу між сегментами, фази останніх відповідним чином узгоджуються.

Фазове кодування, коли воно може бути використане, є одним з найефективніших методів кодування за критерієм відношення сигнал/сприйманий шум. Суттєва зміна співвід- ношення фаз між кожною частотною складовою призводить до значного розсіювання фази. Тим не менш, до тих пір, поки модифікація фази є в достатній мірі малою (звичайно, достатньо малою в залежності від спостерігача; фахівці зі спектрального аналізу здатні виявити видозміни, що здаються незначними пересічному спостерігачеві), може бути досягнуте приховання, невідчутне на слух.

Процедура фазового кодування полягає в наступному:

Звукова послідовність ***S***[***i***], (1  ***i***  ***I***) розбивається на серію ***N*** коротких сегментів (блоків) ***Sn***[***i***], (1  ***n***  ***N***) – рисунок *а*, *б*.

До ***n***-го сегмента сигналу ***Sn***[***i***] застосовується ***K***-точкове ДПФ, де ***K*** = ***I***/***N***, та створюються масиви фаз ***n***(***k***) і амплітуд ***An***(***k***) для 1  ***k***  ***K*** (рис., *в*).

Запам’ятовується різниця фаз між кожними сусідніми сегментами для 1 < ***n***  ***N***

(рис. *г*):

***n***(***k*** )  ***n***(***k*** )***n***1(***k*** ) ; ****1(***k*** )  0 .

Двійкова послідовність даних представляється як ***data*** = ****/2 або ***data*** = –****/2,

відображуючи відповідно «1» або «0» (рис. *д*): ****1(***k*** )  ***data***.

**Метод розширення спектру.** У стандартному каналі зв’язку часто є бажаним зосередити інформацію у як можливо вужчій ділянці частотного спектру, для того щоб зберегти наявну смугу пропускання і зменшити потужність сигналу. З іншого боку, основний метод розширення спектру призначений для шифрування потоку інформації шляхом “розсіяння” кодованих даних по всьому можливому частотному спектру. Це робить можливим прийом сигналу навіть за наявності завад на певних частотах.

 Розглядається технологія розширення спектру сигналу прямою послідовністю (РСПП). Метод РСПП розширює сигнал даних (повідомлення), помножуючи його на елемен- тарну посилку – ПВП максимальної довжини, модульовану відомою частотою. Оскільки аудіосигнали, що використовуються в якості контейнерів, мають дискретний формат, то для кодування як частоту елементарної посилки можна використовувати частоту дискретизації. Як наслідок, дискретний характер сигналу усуває найскладнішу проблему, яка виникає при одержанні сигналу з розширеним прямою послідовністю спектром, – встановлення правильногопочатку і кінця квантів елементарної посилки з метою фазової синхронізації. Отже, існує можливість використання набагато вищої частоти елементарної посилки, а, отже, й одержання більш високої пов’язаної з нею швидкості передачі даних. За відсутності цього можуть застосовуватися різноманітні алгоритми блокування сигналу, але у обчислювальному від- ношенні вони є досить складними.

Метод РСПП при цьому полягає в наступному. Сигнал даних помножується на сигнал несучої і псевдовипадкову шумову послідовність, яка має широкий частотний спектр. В резуль- таті спектр даних розширюється на всю доступну смугу. Тоді послідовність розширених даних послаблюється і додається до первинного файлу як адитивний випадковий шум (рис.3.,4).



Рис. 3. – Кодування з розширенням спектру Рис. 4.– Інформація синтезована розширенням спектру

**Висновки**

Отже, 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. Захисті інформації може бути забезпечено криптографією, стеганографією, або одночасно криптографією і стеганографією. При використанні криптографії інформація модифікується, перетворюється. Також мною було розглянуто сучасні стеганографічні методи та здійснений їх аналіз, здійснено огляд та типи загроз на стеганографічні системи. Здійснено порівняння стеганографічних методів. Також було здійснено огляд та аналіз стеганографічних алгоритмів, огляд їх сильних та слабких сторін.

 Відповідно від отриманої інформації, було зроблено висновок, що рівень захищеності не відповідає сучасним вимогам, частина алгоритмів не є ефективними інша ж частина підлягає вдосконаленню.

**Список використаних джерел**

1. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. *Основи комп’ютерної стегано- графії* : Навч. посіб. для студентів і аспірантів. — Вінниця: ВДТУ, 2003.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография*. — М.: Солон-Пресс, 2002.
3. Інтернет ресурс: <https://library.kre.dp.ua/Books/2-4>
4. Інтернет ресурс: <http://tks.nau.edu.ua/wp-content/uploads/2016/05/Steganografiya.pdf>