УДК 004.056.5:004.7

ОСОБЛИВОСТІ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Потєхін М.В. – гр.БЧКІ-1-17, бакалавр, *marson75@mail.ru*
Захарова М.В – к.т.н., доцент, *z.maria@ukr.net*
Люта М.В. – старший викладач, *lyuta.mv@knutd.com.ua*
Київський національний університет технологій та дизайну

В роботі досліджено та проаналізовано види стеганографічних систем, розглянуто модель стеногосистеми, особливості механізмів стенографічного захисту, визначено схожості і відмінності різних видів стенографічного захисту інформації. Описані базові значення для розуміння загального поняття стенографії, декілька способів використання її механізмів.

The types of steganographic systems are investigated and analyzed in the work, the model of steno - system, features of mechanisms of stenographic protection are considered, similarities and differences of different types of stenographic protection of information are defined. The basic values for understanding the general concept of shorthand, several ways of using its mechanisms are described.

Вступ. Задача захисту інформації во всі часи стояла перед багатьма людьми. Основою захисту інформації стали два шляхи: криптографія - захист інформації, основою якого стає приховання лише в місту послання та її прямий конкурент – стенографія, яка приховує сам факт існування повідомлення. Актуальність досліджень у галузі комп'ютерної стеганографії витікає з обмежень на використання криптографічних засобів та з необхідності розв'язування задач захисту прав власності на інформацію, яка представлена у цифровому вигляді.

Постановка задачі. В даній роботі необхідно дослідити та проаналізувати види стеганографічних систем, розглянути узагальнену модель стеногосистеми , виявити типи та особливості застосування механізмів стеганографії. Стеганографія - наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі [1]. Методи стеганографії дозволяють не тільки приховано передавати дані, але і вирішувати завдання перешкодостійкою аутентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації з мереж зв'язку, пошуку інформації в мультимедійних базах даних. На відміну від криптографії, яка приховує вміст секретного

повідомлення, стеганографія приховує факт передачі інформації, який сам по собі може мати вирішальне значення.

Стенографування, як спосіб документування розвивалося на протязі декількох століть, переслідуючи головну мету: створення компактної і зручної стенографічною системи, яка змогла б задовольнити потреби багатьох мов. На даний момент існує кілька популярних систем стенографування.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту [3-5].

Розрозглянемо узагальнену модель стеногосистеми (рис.1). В якості повідомлення може використовуватись будь-яка інформація, яка підлягає прихованій передачі. Як повідомлення може використовуватися будь-який вид інформації: текст, зображення, звук. Контейнер - це будь-яка інформація, призначена для приховування повідомлення. Вибір виду контейнера має суттєвий вплив на надійність стегосистеми і можливість виявлення факту передачі прихованого повідомлення. Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер або стеганоконтейнер, що містить вбудовану інформацію. Стегосистеми утворює стегоканала, за яким передається або в якому зберігається заповнений контейнер. По суті контейнер в стеганографічної системі є не чим іншим, як носієм прихованої інформації, У стеганографії як контейнери можуть бути використані різні оцифровані дані: растрові графічні зображення, цифровий звук, цифрове відео, всілякі носії цифрової інформації, а також текстові та інші електронні документи. Стеганоключ або просто ключ – секретний ключ, необхідний для приховування інформації. У стегосистеми з секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу. У стегосистеми з відкритим ключем для вбудовування і вилучення повідомлення використовуються різні ключі, відмінність яких полягає в тому, що за допомогою обчислень неможливо визначити один ключ з іншого. Тому один ключ (відкритий) може передаватися вільно по незахищених каналу зв'язку.

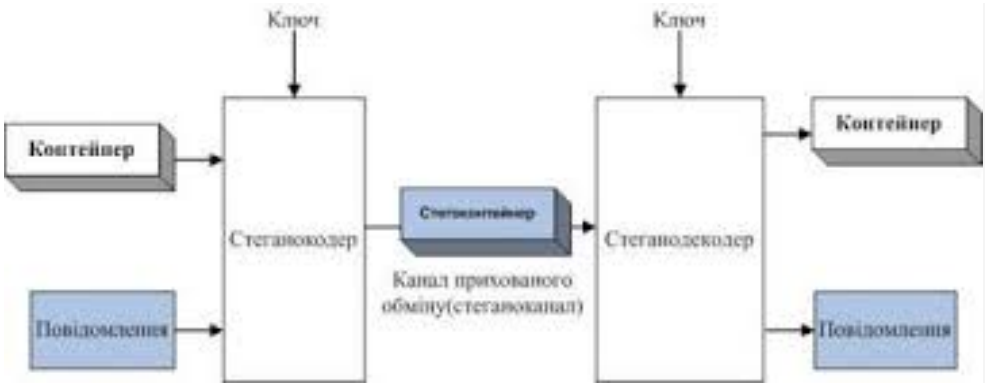

Рисунок 1 – Схема стегосистеми

В кінці 90 років стеганографію поділили на 3 види: класична, комп’ютерна та цифрова [3]. В наш час додалась мережева стенографія оскільки користувачем інтернету стала майже кожна людина.

Класична стеганографія. В часи другої світової війни використовували такий тип стенографії як мікроточки (мікроскопічні фотографії наклеєні в текст посилання). Також прикладом класичної стеганографії можна назвати надписи на бокових колодах карт та будь-який тип жаргонного шифру, де слова мають обговорені значення, семаграми [1].

Одним з найпоширеніших методів класичної стеганографії є використання симпатичних чорнил (невидимих). Зазвичай процес запису здійснюється наступним чином: перший шар — наноситься важливий запис невидимим чорнилом, другий шар — запис видимими чорнилом, що нічого не значить. Текст, записаний такими чорнилом, проявляється лише за певних умов (нагрівання, освітлення, хімічний проявник і т.ін.). Існує також чорнило з хімічно нестабільним пігментом. Написане цими чорнилами виглядає як написане звичайною ручкою, але через певний час нестабільний пігмент розкладається, і від тексту не залишається і сліду.

Але такі типи як комп’ютерна і цифрова стенографія набагато популярніші.

Комп'ютерна стеганографія – напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи. Комп'ютерна стеганографія базується на двох основних принципах. Перший принцип полягає в тому, що файли, що містять оцифроване зображення або звук, можуть бути до певної міри видозмінені без втрати їх функціональності на відміну від інших типів даних, що вимагають абсолютної точності. Другий принцип полягає в нездатності органів почуттів людини розрізняти незначні зміни в кольорі зображення або якості звуку. Цей принцип

особливо легко застосовувати до зображення або звуку, який несе надлишкову інформацію.

Цифрова стеганографія – напрям класичної стеганографії, заснований на захованні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів [3]. Але, як правило, дані об'єкти є мультимедіа-об'єктами (зображення, відео, аудіо, текстури 3D-об'єктів) та внесення спотворень, які знаходяться нижче межі чутливості середньостатистичної людини, не призводить до помітних змін цих об'єктів.

Прикладом цифровой стенографії покажем метод LSB (Least Significant Bit, найменший значущий біт). Даний метод полягає у виділенні найменш значущих біт зображення-контейнера з подальшою їх заміною на біти повідомлення (рис. 2). Оскільки заміні піддаються лише найменш значущі біти, різниця між вихідним зображенням-контейнером і контейнером, що містить приховані дані невелика і зазвичай непомітна для людського ока [1]. Метод LSB можна застосовувати лише до зображень в форматах без стиснення (наприклад, BMP) або зі стисненням без втрат (наприклад, GIF), так як для зберігання прихованого повідомлення використовуються найменш значущі біти значень пікселів, при стисненні з втратами ця інформація може бути втрачена. Формати без стиснення мають дуже великий розмір і можуть викликати підозру, з цього для стеганографії частіше використовують інші формати.

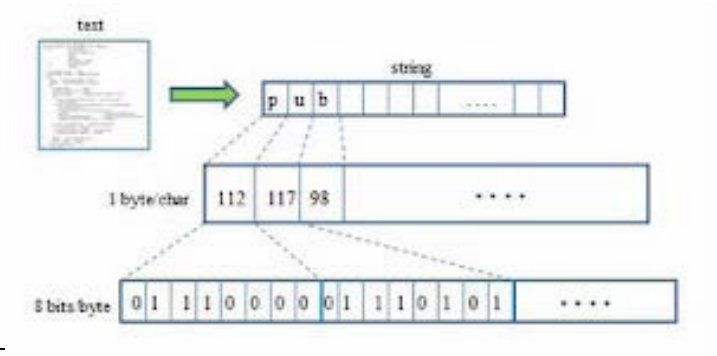

Рисунок 2 – Перетворення тексту в байтовую послідовність

Принцип цього методу полягає в наступному: Припустимо, є 8-бітне зображення в градаціях сірого. 00h (00000000b) позначає чорний колір, FFh (11111111b) – білий. Усього є 256 градацій (2 ^ 8). Також припустимо, що повідомлення складається з 1 байта – наприклад, 01101011b. При використанні 2 молодших біт в описах пікселів, нам буде потрібно 4 пікселя. Припустимо, вони чорного кольору. Тоді пікселі, що містять

приховане повідомлення, будуть виглядати наступним чином: 00000001 00000010 00000010 00000011. Тоді колір пікселів зміниться: першого – на 1/255, другого і третього – на 2/255 і четвертого – на 3/255. Такі градації, мало того що непомітні для людини, можуть взагалі не відобразитися при використанні низькоякісних пристроїв виведення. В ролі базового контейнера пропонується використовувати файли BMP-зображень високої роздільності з глибиною кольору 24 та 32 біти, таємне зображення може мати розширення .BMP, .GIF, .PNG, .JPEG.

Але методи LSB є нестійкими до всіх видів атак і можуть бути використані тільки при відсутності шуму в каналі передачі даних [5]. Виявлення LSB-кодованого «стего» здійснюється по аномальним характеристикам розподілу значень діапазону молодших бітів відліків цифрового сигналу.

Висновки. В результаті проведеного дослідження, було визначено можливості стеганографії, як технології яку можна використовувати в багатьох аспектах життя. В роботі було досліджено та проаналізовано види стеганографічних систем, розглянуто узагальнену модель стеногосистеми, виявлено особливості застосування механізмів стеганографії.

Список використаних джерел:

1. Стеганографія в зображеннях приклади. Двійкова тайнопис (за матеріалами відкритій пресі). Сучасні підходи до стеганографії. [Электронный ресурс]. – Режим доступа: https://maylohack.ru/uk/operacionnye-sistemy/steganografiya-v-izobrazheniyah-primery-dvoichnaya-tainopis-po.html
2. Стеганография, классификация видов и методов стеганографии [Электронный ресурс]. – Режим доступа: https://intellect.icu/steganografiya-klassifikatsiya-vidov-i-metodov-steganografii-5824
3. Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=330&lvl, 2020 – Назва з екрана.
4. Стеганографічні методи захисту документів / Б. В. Дурняк, Д. В. Музика,
В. І. Сабат. – Львів : Укр. акад. друкарства, 2014. – 159 с.
5. Konahovich, G.F. and Puzyirenko, A.Y. Kompyuternaya steganografiya. Teoriya i praktika, [Computer steganography. Theory and practice], MK-Press, Kyiv, Ukraine, 2006.
6. Стеганографія. [Электронный ресурс]. – Режим доступа: http://www.nestego.ru/2012/07/lsb.html