Міністерство освіти і науки України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Худьо Володимир Дмитрович

Моделювання стійкої стегофонічної системи із заданими характеристиками мережі / Modeling of stehophonical stable system with desired characteristics of networks

Спеціальність 8.091501 – Комп'ютерні системи та мережі

Дипломна робота за освітньо-кваліфікаційним рівнем «магістр»

Науковий керівник
к.ф.-м..н., доцент Касянчук М.М.
_____

Дипломну роботу допущено до захисту
«___»_____ 20 __ р.
Зав. кафедри КІ
Березький О.М. _____

Тернопіль – 2017

РЕЗЮМЕ

Дипломна робота на тему “Моделювання стійкої стеганофонічної системи із заданими характеристиками мережі” на здобуття освітньо-кваліфікаційного рівня “Магістр” зі спеціальності “Комп’ютерні системи та мережі” написана обсягом 103 сторінка і містить 13 ілюстрацій, 3 таблиці, 3 додатки та 64 джерела за переліком посилань.

Метою роботи є моделювання параметрів стійких стегосистем для підвищення стійкості стеганофонічних систем в моделі пасивного супротивника.

Методи досліджень. Базуються на основі теорії інформації, теорії цифрових автоматів, теорії кодування, моделюванні алгоритмів і апаратних засобів комп’ютерів та експериментальних досліджень, теорії цифрової обробки сигналів та зображень.

Результати дослідження: розроблено програмне забезпечення для вибору оптимальних параметрів стеганофонічної системи при заданих мережевих характеристиках.

Результати роботи можуть бути використані в правоохоронних та військових структурах, на підприємствах, а також можуть використовуватись в навчальному процесі.

Орієнтовні напрямки розвитку досліджень: захист конфіденційної інформації від несанкціонованого доступу; протидія системам моніторингу і управління мережевими ресурсами, прихована анотація повідомлень, які повинні бути доступні тільки фахівцям.

КЛЮЧОВІ СЛОВА: IP-ТЕЛЕФОНІЯ, СТЕГАНОФОНІЯ, ПРИХОВУВАННЯ ДАНИХ, МОВНІ СИГНАЛИ, СТЕГОСИСТЕМА, МОДЕЛЮВАННЯ ПАРАМЕТРІВ, СТІЙКІСТЬ, ТРАФІК IP-ТЕЛЕФОНІЇ.

RESUME

Diploma work: "Modeling steganophonic stable system with specified characteristics of network" to education and qualification of "Master" specialty "Computer systems and networks" written 103 pages volume and contains 13 illustrations, 3 tables, 3 applications and 64 sources for references.

The aim is sustainable stegosystem modeling parameters to improve the sustainability of the model steganophonic passive opponent.

Research Methods. Based on information theory, the theory of digital automata, coding theory, simulation algorithms and computer hardware and experimental studies, the theory of digital signal processing and imaging

The results: developed software to select the optimal parameters for a given stehanofonic system network performance.

The results can be used in law enforcement and military structures, enterprises, and can be used in the classroom.

The estimated direction of research: protecting confidential information from unauthorized access; opposition to systems monitoring and management of network resources, hidden abstract messages that should be accessible only to experts.

KEY WORDS: IP-TELEPHONY, STEGANOPHONY, DATA HIDING, SPEECH SIGNALS, STEGOSYSTEM, MODELING PARAMETERS, STABILITY, TRAFFIC IP TELEPHONY THESIS.

ЗМІСТ

ВСТУП

Актуальність теми. Проблема інформаційної безпеки вирішується на протязі всієї історії людства. Ще в давнину виділилося два основні напрямки захисту інформаційних ресурсів: криптографія та стеганографія. Криптографія блокує несанкціонований доступ до даних шляхом їх шифрування. Стеганографія ж іде принципово далі – її мета приховати сам факт існування конфіденційної інформації.

Хоча стеганографія має дуже довгу і багату історію, однак тільки останнім часом у зв'язку з бурхливим розвитком інформаційних технологій, зокрема з появою комп'ютерних мереж, а також через наявність обмежень на використання криптозасобів та надзвичайну актуальність проблеми захисту інтелектуальної власності, стеганографія стає предметом зростаючого інтересу й активних наукових досліджень. Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на базі комп'ютерної техніки і програмного забезпечення в рамках окремих обчислювальних систем, корпоративних чи глобальних мереж, складають предмет вивчення цифрової стеганографії. Одним із видів стеганографії є стеганофонічні системи – це системи в яких приховується факт передачі таємного повідомлення, а саме повідомлення інкапсулюється у стек мережевих протоколів та передається у реальному масштабі часу [1]. Вперше принципи та визначення комп'ютерної стеганофонії були сформовані польськими спеціалістами з Варшавського університету технологій у 2008 році, які запропонували декілька методів приховування даних у трафіку IP-телефонії [1]. Структура та принципи роботи систем комп'ютерної стеганофонії аналогічні до стеганографічних систем, тому часто про ці галузі захисту даних порівнюють між собою.

Актуальність досліджень у галузі комп'ютерної стеганофонії витікає з обмежень на використання криптографічних засобів та з необхідності розв'язування задач захисту прав власності на інформацію, яка представлена у цифровому вигляді. На сьогодні в якості інструментів для розвитку цієї галузі широко використовуються методи теорії ймовірностей та математичної статистики, теорії швидких ортогональних перетворень, теорії апроксимації, теорії кодування, теорії складності, теорії похибок, цифрової обробки сигналів та зображень тощо. Тобто, як бачимо, це вже досить наукоємна дисципліна.

Незважаючи на молодість комп'ютерної стеганофонії, основні її поняття та принципи не аналогічні стеганографії. Так в роботах [1-5] наведено базову систему означень та математичні моделі стеганографічних систем. Велика кількість вітчизняних та зарубіжних публікацій присвячена аналізу головної характеристики стегосистеми – її стійкості.

Значний вклад у розвиток стеганофонії внесли такі вчені як: Задірака В.К., Кошкіна Н.В., Олексюк О.С., а також польські вчені Wojciech Mazurczyk, Krzysztof Szczypiorski,Zbigniew Kotulski.

В роботах [1], [3] наведено комплексний огляд теоретико-інформаційного, теоретико-складнісного та теоретико-ігрового підходу до оцінки стійкості стеганографічних систем.

Разом з тим чимало проблем поки що знаходяться на початковій стадії свого вирішення. Наведемо основні з них:

- побудова стійких стеганофонічних систем в рамках моделей пасивного та активного противника;
- отримання оцінок стійкості стеганофонічних систем;
- отримання оцінок складності стеганофонічних алгоритмів та їх порівняльний аналіз;
- моделювання параметрів стійких стегосистем;
- побудова стеганоалгоритмів з мінімальною довжиною ключа при заданій стеганостійкості та інші.

Вирішення наведених вище проблем забезпечить підвищення стійкості стеганофонічних систем.

Зв'язок роботи з науковими програмами, планами, темами

Напрямок виконаних досліджень безпосередньо пов'язаний з науково-дослідним напрямком кафедри “комп’ютерної інженерії” Тернопільського національного економічного університету.

Мета і задачі дослідження. Метою досліджень ємоделювання параметрів стійких стегосистем для підвищення стійкості стеганофонічних систем в моделі пасивного супротивника.

Для досягнення поставленої мети потрібно розв’язати наступні взаємопов’язані завдання:

- проаналізувати особливості побудови стеганофонічних систем;
- дослідити атаки на стеганофонічні системи;
- проаналізувати комп’ютерні засоби реалізації стеганофонічних алгоритмів;
- дослідити підходи щодо оцінки стійкості стеганофонічних систем;
- дослідити критерії підвищення стійкості стеганофонічних систем;
- розробити програмне забезпечення для моделювання параметрів стеганофонічних систем при заданих мережевих характеристиках в моделі пасивного супротивника;

Об’єкт дослідження – приховування даних у трафіку IP-телефонії.

Предмет дослідження – методи та комп’ютерні засоби приховування даних у трафіку IP-телефонії.

Методи дослідження. Основні наукові результати і висновки, одержані на основі теорії інформації, теорії цифрових автоматів, теорії кодування, моделюванні алгоритмів і апаратних засобів комп’ютерів та експериментальних досліджень, теорії цифрової обробки сигналів та зображень.

Наукова новизна одержаних результатів. Досліджено вплив розміру контейнера з прихованими даними на стійкість стегостистеми до виявлення її зловмисником.Запропоновано підхід до вибору оптимальних параметрів

стегосистем при заданих мережевих характеристиках, який дає змогу підвищити ефективність та захищеність передачі прихованих даних каналами IP-телефонії.

Публікації та апробація ДР. Публікацію тез дипломної роботи на тему «Моделювання стійкої стеганофонічної системи із заданими характеристиками мережі» надруковано у виданні «VIВсеукраїнської школи-семінару молодих вчених і студентів» [64].

Впровадження результатів ДР. Дипломна роботана тему «Моделювання стійкої стеганофонічної системи із заданими характеристиками мережі» відповідає замовленню товариства, має певну практичну значимість і планується до впровадження у ТОВ «Микулинецький Бровар».

1 ОСОБЛИВОСТІ ПОБУДОВИ СТЕГАНОФОНІЧНИХ СИСТЕМ

1.1 Аналіз структури стеганофонічної системи

Задача захисту інформації від несанкціонованого доступу розв'язувалася у всі часи протягом історії людства. Вже в стародавньому світі виділилося два основні напрями рішення цієї задачі, що досі існують і по сьогоднішній день: криптографія і стеганографія.

Метою криптографії є приховання вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії ховається сам факт існування таємного повідомлення.

Отже слово “стеганографія” має грецькі корені і буквально означає “тайнопис”. Історично цей напрям з'явився першим, але потім багато в чому був витиснений криптографією. Тайнопис здійснюється самими різними способами. Загальною межею цих способів є те, що приховуване повідомлення вбудовується в деякий нешкідливий об'єкт, що не привертає до себе увагу[1]. Потім цей об'єкт відкрито транспортується адресату. При криптографії наявність шифрованого повідомлення сама по собі привертає увагу зловмисників, при стеганографії ж наявність прихованого зв'язку залишається непомітною.

Якщо розглядати інформацію окремо від її матеріального уявлення, то де ж її тоді можна заховати? Тут можна дати однозначну відповідь: тільки в ще більшому масиві інформації – як голку в стозі сіна. В цьому і полягає принцип дії стеганографії. Наприклад, ми відправляємо нашому кореспонденту по електронній пошті файл з растровою чорно-білою картинкою, в якому найменш значущий біт в коді яскравості кожної точки зображення буде елементом нашого таємного повідомлення. Одержувач листа витягне всі такі біти і складе

з них "істинне повідомлення". Картинка, присутня тут тільки щоб вас заплутати, і вона так і залишиться для непосвячених простою картинкою. Стеганографія корисна, коли необхідно не просто передати секретне повідомлення, а таємно передати секретне повідомлення і при цьому приховати сам факт його передачі. Проте такий спосіб ведення таємної комунікації має ряд недоліків:

- по-перше, важко обґрунтувати його стійкість – раптом зловмисникам стане відомий спосіб "підмішування" секретних даних до контейнера – масиву відкритих даних;

- по-друге, при його використанні об'єм передаваємих або збережених даних різко збільшиться, що негативно позначиться на продуктивності систем їх обробки.

Стеганофонічні системи – це системи в яких приховується факт передачі таємного повідомлення, а саме повідомлення інкапсулюється у стек мережевих протоколів та передається у реальному масштабі часу [1]. Вперше принципи та визначення комп’ютерної стеганофонії були сформовані польськими спеціалістами з Варшавського університету технологій у 2008 році, які запропонували декілька методів приховування даних у трафіку IP-телефонії. Структура та принципи роботи систем комп’ютерної стеганофонії аналогічні до стеганографічних систем, тому часто про ці галузі захисту даних порівнюють між собою.

Виділяють такі основні області застосування стеганофонічних систем:

- захист авторського права;
- ідентифікація та аутентифікація користувачів;
- прихована передача даних.

Для кожної з областей існують свої особливості побудови стеганофонічних систем, проте всі вони мають ряд спільних принципів [1].

При використанні комп’ютерної стеганофонії потрібно дотримуватися наступних принципів:

- в якості носія прихованої інформації повинен виступати аудіо сигнал, який допускає спотворення власної інформації, що суттєво на вплинуть на його якість та внутрішню структуру;

- внесені спотворення повинні бути нижчі рівня чутливості засобів розпізнавання.

Перший принцип полягає в тому, що аудіо сигнали, які містять оцифрований звуковий чи мовний сигнал, можуть бути до деякої міри видозмінені без втрати функціональності, на відміну від інших типів даних, які вимагають абсолютної точності.

Другий принцип полягає в неспроможності органів слуху людини розрізнити незначні зміни в якості аудіо сигналу, при цьому враховується область звукового сприйняття [1] (рисунок 1.1).

Рисунок 1.1 – Область звукового сприйняття людини

З рисунка 1.1 видно, що органи слуху людини по-різному сприймають звукові частоти. Верхня межа області відповідає оглушливому звуку, що межує з больовим відчуттям. Нижня межа визначається порогом чутливості. Крім того, людина практично не може однозначно реєструвати на слух зміни інтенсивності звуку, якщо вони є незначними.

Базовим поняттям в стеганофонії є поняття контейнера. Контейнер – це блок даних, основним завданням якого є приховування таємної інформації [2]. Де фактор контейнер в стеганографії представляється файлом, однак у стеганофонії контейнером може бути будь-яке поле протоколу передачі даних Дані контейнера повинні бути достатньо шумними, щоб невелика зміна в них не була помітною. Біти контейнера, хоча і є шумом з точки зору точності вимірювань, можуть мати деякі спеціальні статистичні характеристики. Тому кодування таємного повідомлення повинно відтворювати характеристики шуму контейнера.

Існують декілька варіантів вибору контейнера:

- контейнер генерується стегосистемою;
- контейнер вибирається з деякої підмножини контейнерів за критерієм ефективності приховування даних;
- контейнер поступає ззовні;
- контейнер створюється шляхом моделювання шумових характеристик;
- контейнер вибирається із числа зарезервованих полів протоколу, які не використовуються в процесі передачі даних.

На практиці найчастіше застосовується така процедура вибору контейнера: спочатку вибирається клас достатньо шумних контейнерів і ідентифікуються біти шуму. Потім визначається, яку частину шумових бітів контейнера можна замінити псевдовипадковими даними без значних змін в його статистичних характеристиках. Для забезпечення додаткового рівня захисту вбудовані дані зашифровують криптоалгоритмом [2].

За протяжністю розрізняють неперервні (потокові) і обмежені (фіксовані контейнери). Потоковий контейнер представляє собою неперервну послідовність біт. Повідомлення вбудовується в нього в режимі реального часу, тому невідомо заздалегідь, чи вистачить розміру контейнера для передачі всього повідомлення. Якщо розмір контейнера достатньо великий, є можливість вкладення декількох повідомлень. Інтервали між вбудовуваними бітами визначаються генератором псевдовипадкової послідовності з рівномірним

розподілом інтервалів між відліками. Основна складність полягає в здійсненні синхронізації, визначенні початку і кінця повідомлення.

У фіксованого контейнера розміри і характеристики відомі наперед [2]. Це дозволяє вибрати оптимальний шлях для вкладення приховуваної інформації.

Вбудоване повідомлення, яке знаходиться в стегоконтейнері, передається від відправника до отримувача по каналу передачі, який називається стеганофонічним каналом або просто стеганоканалом.

В процесі передачі повідомлення може піддаватися різного роду трансформаціям: зменшуватися або збільшуватися, перетворюватись в інший формат і т.д. Крім того, воно може бути стиснуте, в тому числі з використанням алгоритмів стиснення з втратою даних. Саме тому стегоповідомлення повинно бути стійким до спотворень такого роду.

Задачу вбудовування і виділення повідомлення з контейнера виконує стегосистема [2]. Стегосистема складається з наступних основних елементів (рисунок 1.2):

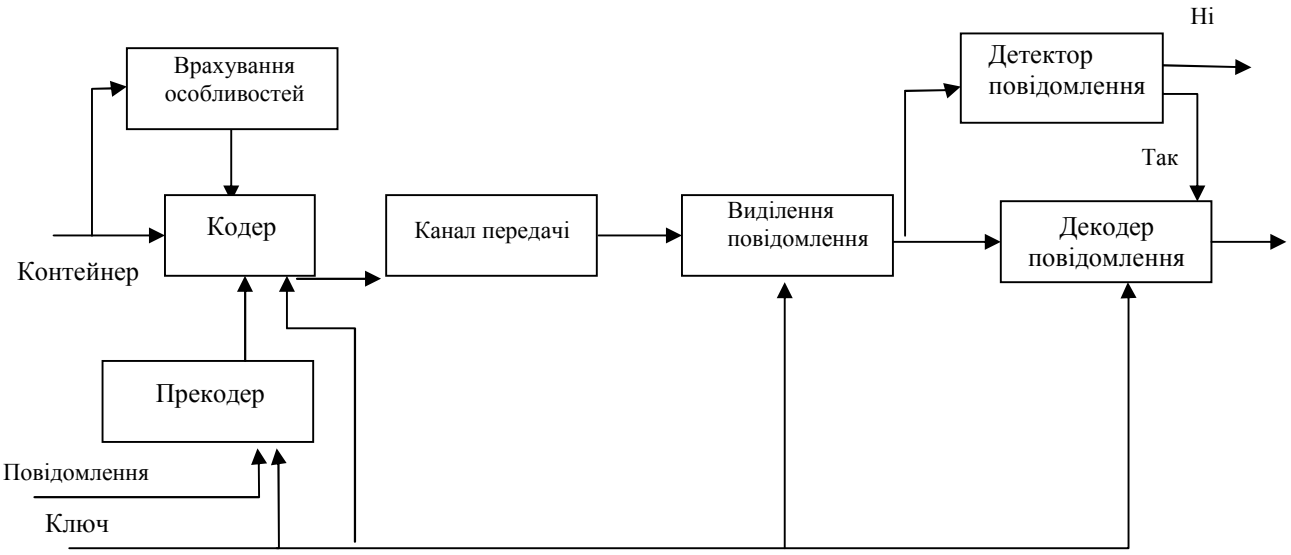

Рисунок 1.2 – Структурна схема типової стегосистеми

Вбудовування повідомлень в контейнер проходить з використанням спеціального стегоключа. Ключ – псевдовипадкова послідовність біт, яку створює генератор, що задовольняє певним вимогам (криптографічно

безпечний генератор). Цей ключ визначає порядок вбудовування повідомлення в контейнер. В якості основи генератора може використовуватися, наприклад, лінійний рекурентний регістр. Тоді адресатам для забезпечення зв'язку може повідомлятися початкове значення цього регістра [3].

Таємна інформація вбудовується у відповідності до ключа в ті відліки, спотворення яких не призводить до суттєвих спотворень контейнера. Ці біти утворюють стегошлях. Під суттєвим спотворення можна розуміти спотворення, яке призводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення факту наявності таємного повідомлення після стегоаналізу.

За типом стегоключа виділяють системи з таємним ключем і системи з відкритим ключем. В стегосистемі з таємним ключем використовується один ключ, який має бути визначений або до початку обміну даними, або ж переданий по захищеному каналу зв'язку.

В стегосистемі з відкритим ключем для вбудовування і виділення таємного повідомлення використовуються різні ключі, які вибираються таким чином, що вивести один ключ з іншого неможливо. Тому один ключ (відкритий) може передаватися вільно по незахищеному каналу зв'язку, а інший (таємний) – по захищеному каналу. Дана схема добре працює при взаємній недовірі відправника і отримувача.

В залежності від кількості рівнів захисту інформації в стегосистемі може бути один або декілька стегоключів.

Враховуючи всю різноманітність стеганофонічних систем, їх можна звести до 4 основних типів:

- безключеві стегосистеми;
- системи з таємним ключем;
- системи з відкритим ключем;
- змішані стегосистеми [3].

Для функціонування безключевих стегосистем не потрібно ніяких додаткових даних у вигляді стегоключа крім алгоритму стеганофонічного перетворення.

Безключовою системою будемо називати сукупність:

$$F=<C, M, D, E>, \qquad (1.1)$$

де C – множина можливих контейнерів,

M – множина таємних повідомлень, причому $|C|\geq|M|$;

$E: C\times M\rightarrow C$ і $D: C\rightarrow M$ – функції приховування і виділення повідомлення з контейнера, причому $D(E(c, m)) = m$ для будь-яких $m\in M$ і $c\in C$.

З цього визначення слідує, що безпечність безключевих стегосистем базується на таємності використовуваних стеганофонічних перетворень E і D, що суперечить основному принципу Кергхоффа для систем захисту інформації.

Зазвичай для підвищення надійності безключевих систем, перед початком процесу стеганофонічного перетворення попередньо виконується шифрування приховуваної інформації. Такий підхід збільшує захищеність всього процесу зв'язку, оскільки це ускладнює виявлення таємного повідомлення. Однак, «сильні» стеганофонічні системи, як правило, не потребують попереднього шифрування таємних повідомлень [3].

Слідуючи закону Кергхоффа, безпека система повинна базуватися на деякій таємній інформації, без знання якої неможливо отримати з контейнера таємну інформацію. В стегосистемах така інформація називається стегоключем. Відправник, вбудовуючи таємне повідомлення в вибраний контейнер c, використовує таємний стегоключ k. Якщо використовуваний в стегоперетвореннi ключ k відомий адресату, то він зможе витягти таємне

повідомлення з контейнера. Без знання такого ключа будь-який інший користувач цього зробити не зможе.

Стегосистемою з таємним ключем називається сукупність:

$$F = <C, M, K, D, E>, \tag{1.2}$$

де C – множина можливих контейнерів,

M – множина таємних повідомлень, причому $|C| \geq |M|$;

K – множина таємних ключів;

E_K: $C \times M \times K \rightarrow C$ і D_K: $C \times K \rightarrow M$ – стеганофонічне перетворення з властивістю $D_K(E_K(c, m, k), k) = m$ для будь-яких $m \in M$, $c \in C$ і $k \in K$. Даний тип стегосистем передбачає наявність безпечного каналу для обміну стегоключами.

Інколи стегоключ k обчислюють з допомогою таємної хеш-функції. Якщо стеганофонічне перетворення E не змінює в результуючому повідомленні вибрані особливості контейнера, то отримувач також зможе підрахувати стегоключ (хоча і в цьому випадку захист залежить від таємності хеш-функції, і таким чином, знову порушується принцип Кергхоффа). Очевидно, що для досягнення адекватного рівня захисту, таку особливість в контейнері необхідно вибирати дуже ретельно[3].

Стеганофонічні системи з відкритим ключем не потребують додаткового каналу обміну ключами. Для їх функціонування необхідно мати два стегоключа: один таємний, а інший – відкритий, який зберігається в доступному для всіх місці. При цьому відкритий ключ використовується в процесі приховування інформації, а таємний – для її виділення.

Стегосистемою з відкритим ключем називається сукупність:

$$F = <C, M, K, D, E>, \tag{1.3}$$

де C – множина можливих контейнерів,

M – множина таємних повідомлень, причому $|C| \geq |M|$;

$K(k_1, k_2)$ – множина пар стегоключів;

E_K: $C \times M \times k_1 \rightarrow C$ і D_K: $C \times k_2 \rightarrow M$ – стеганофонічне перетворення з властивістю $D_K(E_K(c, m, k_1), k_2) = m$ для будь-яких $m \in M$, $c \in C$.

Простим методом реалізації подібних стегосистем є використання криптосистем з відкритим ключем. Стегосистеми з відкритими ключами використовують той факт, що функція отримання таємної інформації D може бути застосована до будь-якого контейнера незалежно від того, знаходиться в ньому таємне повідомлення чи ні.[3] Якщо в контейнері відсутнє таємне повідомлення, то завжди буде відновлюватися деяка випадкова послідовність.

В більшості реальних систем віддають перевагу застосуванню безключевих стегосистем, хоча такі системи можуть бути зовсім неефективними, якщо противник дізнається, яке стеганофонічне перетворення застосовується [3]. У зв'язку з цим в безключових стегосистемах часто використовують криптографічні системи з відкритим і (або) таємним ключем.

1.2Аналіз стеганофонічних алгоритмів

На сьогоднішній день існує досить багато комп'ютерних методів вбудовування прихованих повідомлень в контейнер стеганофонічної системи. Потрібно зазначити, що більшість з них розвиваються в таких основних напрямках:

- методи, що базуються на використанні спеціальних властивостей форматів кадрів із аудіо сигналами;
- методи, що базуються на надмірності представлення цифрових аудіо сигналів;
- методи, що базуються на функціональних особливостях протоколів передачі даних;

- методи, що базуються на часових інтервалах передачі аудіо сигналів по каналах зв’язку [4].

Перша категорія методів використовує зарезервовані для розширення поля форматів даних. Вони заповнюються нульовою інформацією і не враховуються програмою, яка їх прослуховує.

Друга категорія методів використовує надмірність аудіо інформації. Цифровий звук – це матриця чисел, які представляють інтенсивність аудіо сигналу в послідовні моменти часу. Всі ці числа неточні, тому що неточні пристрої, які цифрують аналоговий сигнал. Похибку вимірювань зазвичай вимірюють в процентах або в кількості молодших значень розрядів і називають шумом квантування. Молодші розряди містять дуже мало корисної інформації про поточні параметри звуку, що дозволяє використовувати їх для приховування додаткової інформації [4].

Третя категорія методів враховує особливості передачі аудіо даних різними протоколами передачі, при цьому резервні поля протоколів можуть бути заповнені таємним повідомленням.

Четверта категорія методів базується на особливостях сприйняття аудіо сигналів приймачем повідомлення та мережевими характеристиками середовища передачі даних. Для прикладу, можна сказати, що хороша якість аудіо сигналу гарантується при затримці від відправника до одержувача в межах 400 мс, у той же час якщо аудіо пакети йдуть з часом 200 мс, то кожен другий пакет можна використати у якості стегоконтейнера. Використання такого алгоритму дозволяє досить ефективно передавати приховані дані.

Стеганофонічні алгоритми будуються з таким розрахунком, щоб максимально використовувати область звукового сприйняття і інші властивості мовних сигналів (тембр, швидкість і т.д.), незначні зміни яких людина не може почути [4].

Особливості сприйняття людиною звукових коливань дозволяють приховано передавати інформацію через мовне повідомлення. Серед всіх відомих психоакустичних ефектів найчастіше для вирішення цієї задачі

застосовують ефект маскування. Суть цього ефекту в наступному: більш інтенсивні мовні відрізки роблять нечутними сигналі, які з’являються до них («маскування вперед») і після них («маскування назад»). Часовий діапазон маскування вперед складає до 20 мс, а назад – до 150 мс. Крім того, існує ще частотне маскування, коли в момент появи більш інтенсивного низькочастотного сигналу стає нечутним більш високочастотних сигнал з меншою амплітудою. Необхідно зазначити, що підйом високих частот зменшує діапазон частотного маскування.

Розглянемо обмеження, які пов’язані з обмеженими можливостями нашої слухової системи, які дозволяють вбудовувати додаткову приховану інформацію.

Перше обмеження пов’язано з нечутливістю нашої слуховою системи до провалів спектру в шумовому сигналі. Таким чином, використовуючи режекторну фільтрацію, можна на звуках мовного повідомлення, які породжені турбулентним джерелом, передавати додаткову інформацію. Ці частоти для звука [х] розташовані в діапазоні частот нижче 800 Гц, для звука [ш] – в діапазоні частот від 2кГц до 4кГц, а для звука [с] – на частотах вище 5 кГц. Імовірність зустріти перераховані звуки в українській мові ≈ 0,08, отже за одну секунду мови можна передати 80 мс прихованої інформації і кількість квантів прихованої інформації складе 1, 2 на одну секунду мови [5].

Друге обмеження пов’язане з чутливістю нашої слухової системи до змін значень ширини резонансів, які виникають в мовному тракті. Така відносна чутливість складає 30%. Це означає, що мовний сигнал можна корегувати, змінюючи добротність резонансів голосних звуків. В цьому випадку є можливість передати до 200-300 мс прихованої інформації на одну секунду мови з кількістю квантів прихованої інформації 2-3 за одну секунду мови [5].

Третє обмеження пов’язано з можливістю регулювання мовного сигналу на інтервалах вимушених (моменти часу, коли прискорення повітряного потоку, породжене роботою голосових зв'язок, максимальні) і вільних (коли вплив голосових зв'язок відсутній) коливань. Регулювати тривалість цих

інтервалів не можна, оскільки наше слухове сприйняття дуже чутливе до цих змін. Але збільшити амплітуду на інтервалах вимушених коливань можна. Але робити це потрібно дуже акуратно, корегуючи діапазон змін миттєвої частоти для кожного резонансу мовного тракту. Інтервал вимушених коливань не перевищує половини періоду низькочастотного резонансу в мовному тракті, тобто частоту 300-600 Гц. З врахуванням частоти основного тону 100-200 Гц і тривалістю голосних звуків української мови 200-300 мс на одну секунду мови, отримуємо загальну тривалість кодування до 45 мс. Варто зазначити, що цей вид кодування є найбільш складним для виявлення з допомогою сучасних методів аналізу і розпізнавання мовних сигналів. Кількість квантів прихованої інформації при цьому складає від 15 до 40 на одну секунду мови [5].

Перейдемо до можливості вбудовування специфічних сигналів і завад, які не заважають сприйняттю мовного сигналу. В якості таких сигналів можуть розглядатися збудження на додаткових резонансних частотах. Збудження здійснюють імпульсами тонального джерела, виділеними з самого вихідного мовного сигналу. Цей механізм можна рекомендувати для тих інтервалів, на яких породжуються голосні звуки. Нові резонанси не заважають розумінню вихідного мовного сигналу і на слух сприймаються як деяке покращення тембру вихідного мовного повідомлення. Тривалість таких адитивних сигналів складає 500-600 мс, а кількість квантів прихованого повідомлення – від 2 до 4 на одну секунду мови.

Таким чином, максимальна швидкість передачі прихованої інформації на мовному сигналі може бути 52,2 кванта за одну секунду. Найпростіший спосіб кодування – це режекція звуків, породжених турбулентним джерелом, з швидкістю передачі 1 квант в секунду. Найскладнішим для виявлення ефекту кодування є метод корекції мовного сигналу на часових ділянках вимушених коливань з мінімальною швидкістю передачі інформації 12 квантів. Інформаційна ємність кожного кванта в середньому може складати 2 біти (приблизно 4 стани), так що максимальна швидкість передачі інформації може скласти приблизно 100 біт в секунду.

На практиці стеганофонічні системи, які побудовані по другому принципу, використовуються найчастіше, не дивлячись на багато недоліків, які притаманні цьому методу. Найбільш простим і популярним методом в комп'ютерній стеганофонії є метод, який базується на використанні молодшого біту аудіо (або будь-яких інших мультимедійних) даних – LBS-метод (Least Significant Bits)[5]. Розглянемо цей метод більш детально. Більша частина комп'ютерної інформації «шумить». Шумить все те, що зберігається, передається і обробляється. Оскільки мовний сигнал записується з мікрофона, то в записі присутній деякий рівень шуму, який залежить від якості мікрофона, рівня зовнішніх акустичних завад і похибок пристроїв перетворення каналового сигналу в цифровий. В якості шумових біт зазвичай розглядаються молодші розряди значень відліків, які є шумом з точки зору точності вимірів і несуть найменшу кількість інформації, яка міститься у відліку. При кодуванні стеганофонічного сигналу змінюється останній (молодший) біт сигналу в певні моменти часу з заданим кроком. Для людського вуха це залишається непомітним і сприймається як шум. Але такий метод використовується все рідше, тому що існує ряд властивостей, за якими можна визначити факт приховування інформації в молодших розрядах даних.

Найбільш популярними при побудові стеганофонічних систем є наступні методи:

- метод найменших значущих бітів – застосовується при цифровому представленні аудіо сигналу і придатний для використанні при будь-якій швидкості зв'язку. При перетворенні аудіо сигналу в цифрову форму завжди присутній шум дискретизації, який не вносить суттєвих спотворень. «Шумовим» бітам відповідають молодші біти цифрового представлення сигналу, які можна замінити приховуваними даними. В якості стегоключа зазвичай використовується вказівників на місце розташування бітів, в яких містяться таємні дані;
- методи широкосмугового кодування – використовують ті самі принципи, що й методи приховування даних в зображеннях. Їх суть полягає в незначній

одночасній модифікації цілого ряду певних бітів контейнера при приховуванні одного біта інформації. Існує декілька різновидів методу. В найбільш поширеному з них вихідних сигнал модулюється високошвидкісною псевдовипадковою послідовністю *w(t)*, яка визначена на області значень {-1; 1}. В результаті цього для передачі результату необхідна більша (інколи більше ніж в 100 разів) полоса пропускання. Зазвичай послідовності *w(t)* вибирають ортогональними до сигналу контейнера. Результуючий стегосигнал *s(t)* являє собою сумарний сигнал контейнера *c(t)* і прихованих даних *d(t)*:

$$s(t) = v(t) + \alpha \times d(t) \times w(t), \qquad (1.4)$$

де коефіцієнт затухання α призначений для вибору оптимального рівня шуму, який вноситься вбудовуваними даними;

- метод приховування в ехо-сигналі – приховування даних шляхом вбудовування еха в аудіо сигнал. Відомо, що при невеликих часових зсувах ехо-сигнал майже не розрізняється на слух. Тому, якщо ввести додаткові часові затримки, величина яких не перевищує поріг, коли їх можуть виявити, то, розбиваючи звуковий сигнал на сегменти, в кожен з них можна ввести відповідний ехо-сигнал. Для виділення ехо-сигналу і відновлення таємних даних застосовується автокореляційний аналіз. В якості стегоключа тут зазвичай використовують значення величин затримок з врахування вибраних меж для відрізків;

- фазові методи приховування – застосовуються як для аналогового, так і для цифрового сигналу. Вони використовують той факт, що плавну зміну фази на слух визначити неможливо. В таких методах таємні дані кодуються або певним значенням фази, або зміною фаз в спектрі. Якщо розбити звуковий сигнал на сегменти, то дані зазвичай приховують тільки в першому сегменті при дотриманні двох умов: потрібно зберігати відносні фази між послідовними сегментами і результуючий фазовий спектр стегосиогнала повинен бути гладким, оскільки різкі скачки фази є демаскуючим фактором.

До побудови стеганофонічних систем висуваються наступні вимоги:

- слухове сприйняття мовних і акустичних сигналів з закладеною в них приховуваною інформацією не повинно різнитися від сприйняття вихідної, відкритої мови або звуку;
- конфіденційні дані, які передаються по відкритих каналах зв'язку і камуфлюються мовними або акустичними сигналами або в неявному вигляді містяться в їх параметрах, не повинні бути легко виявлені в цих сигналах-носіях широко поширеними методами і технічними засобами аналізу звуку і мови, які є в наявності на даний час;
- постановка і виявлення стеганофонічних маркерів не повинні залежати від синхронізації цих процесів і від наявності якихось акустичних еталонів;
- спеціальні методи постановки і виявлення стеганофонічних маркерів повинні реалізовуватися на основі стандартної обчислювальної техніки або спеціальних програмно-апаратних засобів на її основі;
- повинна забезпечуватися можливість закладки і виявлення ознак автентичності в акустичний (мовний) сигнал, які б проявлялися при незаконному його копіювання або модифікації незалежно від виду представлення і передачі цього сигналу (аналового чи цифрового);
- повинна забезпечуватися можливість приховування конфіденційної інформації в акустичному (мовному) сигналі незалежно від виду його представлення (аналового чи цифрового) і передачі в відкритих каналах зв'язку[6].

У більшості випадків ці вимоги можна задовільнити, використовуючи новий підхід до побудови спеціальних стеганофонічних програмно-апаратних засобів аудіо обробки. Цей підхід поєднує ідею переводу аудіо сигналу у вигляд графічних образів (зображень сонограм і фазограм) і назад без втрати інформації.

Сліди фонооб'єктів різноманітної природи в вигляді параметрів складових їх сигналів проявляються на зображеннях динамічних спектрограм у вигляді сукупності контурів (ліній) перепаду яскравості або треків (ланцюжків)

локальних і глобальних екстремумів кольорової насиченості в рівнях одного кольору. З допомогою спеціального програмного забезпечення такі сліди, а точніше амплітуди і фази вузькосмугових сигналів, контури або треки яких і видно на частотно-часовій сітці динамічних спектрограм, можна реконструювати, модифікувати, знищувати, створювати знову для вирішення конкретної стеганофонічної задачі. Так, в ряді програмних продуктів, реалізована можливість вибірки і обробки вузькосмугових складових ділянки зображення спектрограми досліджуваного фонооб'єкта.

Акуратно затираючи або домальовуючи з потрібним нажимом (амплітудою) окремі обертони мови на ділянках зображень динамічних сонограм, можна залишати тільки їх парну або непарну кількість, відповідно приймаючих їх за одиничні або нульові біти конфіденціальної інформації в процесі її передачі-збереження в мовному сигналі [6]. Крім цього, якщо взяти один з обертонів за опорний, можна просинтезувати всі інші обертони з певним фазовим зсувом по відношенню до нього. Задаючи вектори приведених початкових фаз, можна досягнути достатньо великої місткості вбудованих біт прихованої інформації на одиницю часу. Просинтезована мова буде звучати аналогічно вихідній, оскільки фазові відхилення практично не впливають на слухове сприйняття. Можна також встановити певну шкалу умовних відрізків на часовій осі. При повному вміщенні в ці відрізки просинтезованих окремих слів або фраз будемо вважати, що передати одиничний біт інформації, а в протилежному випадку – що переданий нульовий біт. Також можна ввести шкалу умовних відрізків і на частотній осі. Невеликі (до 20 %) відхилення темпу і тембру нової мови по відношенню до вихідної також практично непомітні на слух.

Крім того, мовний сигнал можна непомітно для слуху передавати і зберігати в іншій ділянці мовного повідомлення, а також поєднувати технології стеганофонії з технологіями стеганографії, «розчиняючи» зображення динамічних акустичних спектрограм в заданих зображеннях, з наступним їх проявленням і синтезом на прийомному кінці каналу зв'язку. Самі зображення

сонограм можуть бути використані для передачі і збереження мови на паперових носіях. При реалізації такої технології «мовного підпису», пов’язаних з захищуваним документом по смислу і змісту приблизно таке ж, як і електронно-цифровий підпис, на стандартний лист паперу може бути нанесено в вигляді різноманітних малюнків від 2 до 4 хвилин мови телефонної якості звучання.

На основі запропонованої технології можна здійснити і такий спосіб постановки стеганофонічних маркерів, який полягає в синтезі звукового сигналу по заданому відомому зображенню для наступного збереження на носію або передачі в загальнодоступний канал зв’язку[6].

Для того, щоб перейти до обговорення питань вбудовування інформації в аудіо сигнали, необхідно визначити вимоги, які можуть бути пред'явлені до стего-систем, що використовуються для внесення інформації в аудіо сигнали:

- приховувана інформація повинна бути по можливості стійкою до наявності різних забарвлених шумів, стиснень з втратами, фільтрування, аналогово-цифровому і цифро-аналоговому перетворень;
- приховувана інформація не повинна вносити в сигнал спотворення, що сприймаються слуховою системою людини;
- спроба видалення приховуваної інформації повинна приводити до помітного пошкодження контейнера (для ЦВЗ);
- приховувана інформація не повинна вносити помітних змін у властивості та статистику контейнера.

Отож для впровадження приховуваної інформації в аудіо сигнали можна використовувати методи, застосовні в інших видах стеганографії. Наприклад, можна вбудовувати інформацію, ґрунтуючись на особливостях аудіо сигналів і системи слуху людини, чи будувати стегосистеми, що заміщають найменш значущі біти (всі або деякі) [7].

Систему слуху людини можна представити, як аналізатор частотного спектру, який може знаходити і розпізнавати сигнали в діапазоні 10 - 20000 Гц.

Система слуху людини розрізняє зміни фази сигналу слабкіше, ніж зміни амплітуди або частоти.

Тому аудіо сигнали можна розділити на три класи:

- розмова телефонної якості, діапазон 300 - 3400 Гц;
- широкополосна мова в діапазоні частот 50 - 7000 Гц;
- широкополосні аудіо сигнали в діапазоні частот 20 - 20000 Гц.

До того ж практично всі аудіо сигнали мають характерну особливість. Будь-який аудіо файл є достатньо великим об'ємом даних, для того, щоб використовувати статистичні методи впровадження інформації [7].

Аналоговий звуковий сигнал, як відомо, представляється синусоїдними хвилями різних частот. Людське вухо може чути частоти номінально від 20 до 20 000 Герц (рисунок 1.3). Запам'ятовування звуку в цифровому вигляді вимагає, щоб безперервна звукова хвиля була перетворена на набір нулів і одиниць.

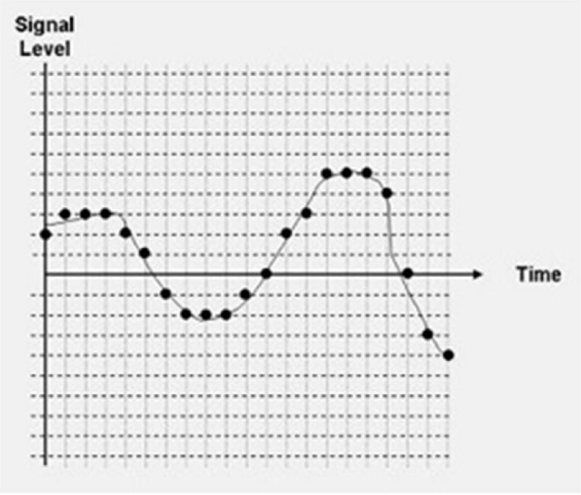

Рисунок 1.3 – Проста імпульсно-кодова модуляція сигналу

Оскільки не стиснений звук, є досить надмірним двійковим потоком, то в простому випадку використовують декілька молодших біт для передачі повідомлень. Більш цікавим є приховання повідомлень в стисненому звуці,

наприклад MP3, оскільки цей формат сьогодні дуже широко поширений в Інтернет. Найпоширеніші типи звукових форматів:

– WAV (з 16-bit WAV, приховуються дані з використанням широкосмугових методів);

– MP3 (використовуються особливості стиснення Mpeg Layer 3);

Суб'єктивне тестування на слух звукового потоку показує, що в середньому максимальна кількість найменш значущих бітів, яка може використовуватися для вбудовування повідомлення без явного спотворення та звернення уваги слухача – це 2-3 останні біти, якщо використовуються 16 бітна послідовність звукових даних.

Таблиця 1.1– Деякі основні формати звукових файлів

Тип	Розширення	Кодек
AIFF (Mac)	.aif, .aiff	Імпульсно-кодова модуляція
MP3	.mp3	MPEG Audio Layer III
Windows Media Audio	.wma	Microsoft proprietary
QuickTime	.qt	Apple Computer proprietary
RealAudio	.ra, .ram	Real Networks proprietary
WAV	.wav	Імпульсно-кодова модуляція

Для зображень таке значення – біля чотирьох останніх біт [8]. Такі випробування виконувалися з великою колекцією звукових файлів та файлів зображень різного напрямку. Жодна з перевірених звукових послідовностей після такого кодування не мала “персептивних артефактів” (або відчутних на слух спотворень).

Розглянемо більш детально формат файлу WAV. Формат файлу WAV – це підмножина специфікації Microsoft RIFF файлів, може включити велику кількість різних видів даних. Він був розроблений для мультимедійних файлів, але відкрита специфікація формату дозволяє досить багато чого для розміщення в таких файлах. Файл RIFF починається з заголовку за яким слідує набір

фрагментів даних [8]. Файл WAV є часто просто RIFF-файлом з єдиним фрагментом "WAVE", який складається з двох під-фрагментів – "fmt " фрагменту, що конкретизує формат даних і фрагменту "data", що містить фактично двійкові дані. Це приблизно і є канонічна форма звукового файлу WAV (рисунок 1.4).

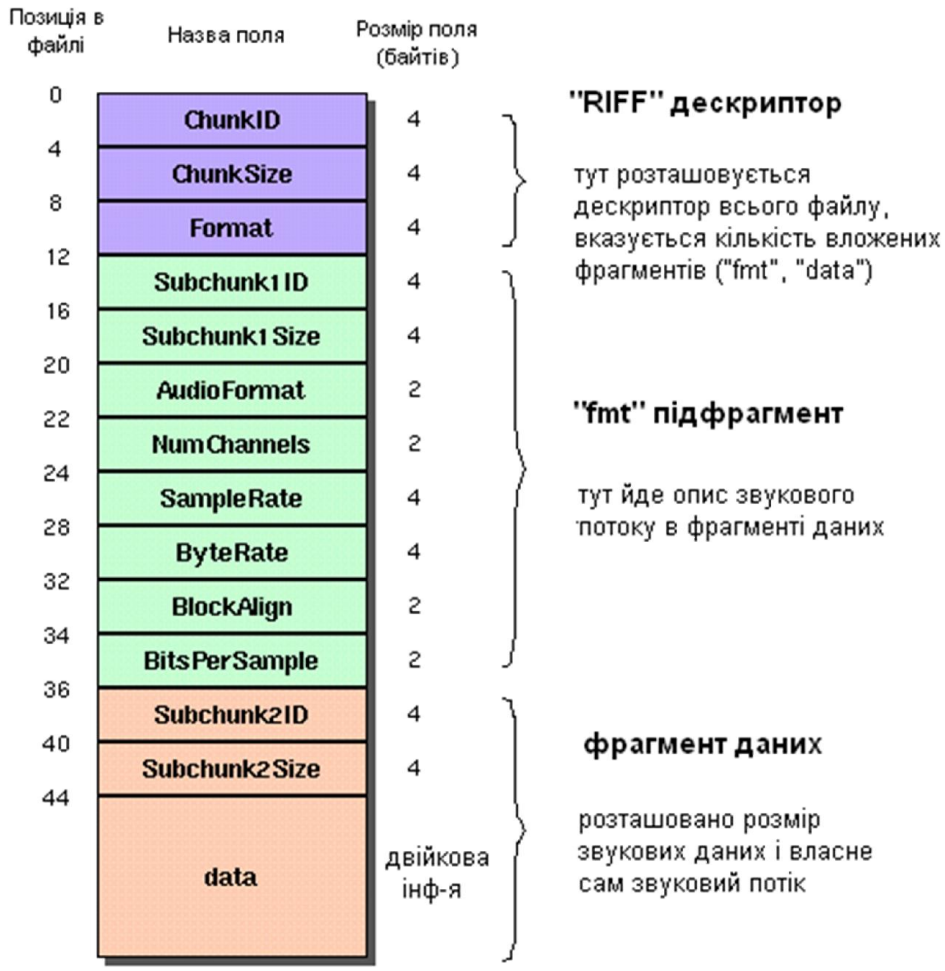

Рисунок 1.4 – Канонічна форма формату файлу WAV

Канонічний WAVE формат починається з RIFF заголовку:

Таблиця 1.2 – Структура формату файлу WAV

Позиція	Розмір	Назва	Опис
0	4	ChunkID	Містить значення "RIFF" в формі ASCII (0x52494646 big-endian).

4	4	ChunkSize	приблизний розмір: 4 + (8 + SubChunk1Size) + (8 + SubChunk2Size)

Продовження таблиці 1.2

			Це розмір поточного файлу в байтах мінус 8 байтів для двох полів не включених в цей підрахунок: ChunkID і ChunkSize.
8	4	Format	Містить значення "WAVE" (0x57415645 big-endian form).
Позиція	Розмір	Назва	Опис
12	4	Subchunk1ID	Містить значення "fmt" (0x666d7420 big-endian).
16	4	Subchunk1Size	16 для PCM (pulse code modulation). Це розмір інших під блоків фрагменту, що слідують за поточним.
20	2	AudioFormat	PCM = 1 (для Linear quantization). Значення, що не рівні 1 означають іншу форму аудіо формату.
22	2	NumChannels	Кількість звукових каналів: Mono = 1, Stereo = 2, і т.д.
24	4	SampleRate	Глубина звуку: 8000, 44100, і т.д.
28	4	ByteRate	Бітрейт: SampleRate * NumChannels * BitsPerSample/8
32	2	BlockAlign	NumChannels * BitsPerSample/8 Кількість байт на один блок (семпл) включаючи всі канали.

34	2	BitsPerSample	8 bits = 8, 16 bits = 16, і т.д.
	2	ExtraParamSize	в PCM, не використовується, місця для додаткових параметрів.
	x	ExtraParams	

Продовження таблиці 1.2

Позиція	Розмір	Назва	Опис
36	4	Subchunk2ID	Містить значення "data" (0x64617461 big-endian).
40	4	Subchunk2Size	NumSamples * NumChannels * BitsPerSample/8 Це кількість байтів у фрагменті даних.
44	*	Data	Звуковий потік (двійкові дані)

- фрагмент "fmt" описує звуковий формат файлу;
- фрагмент "data" містить розмір даних, що містить фактичні двійкові дані[8].

Тому приблизна інтерпретація цих даних звукового файлу наведена на рисунку 1.5.

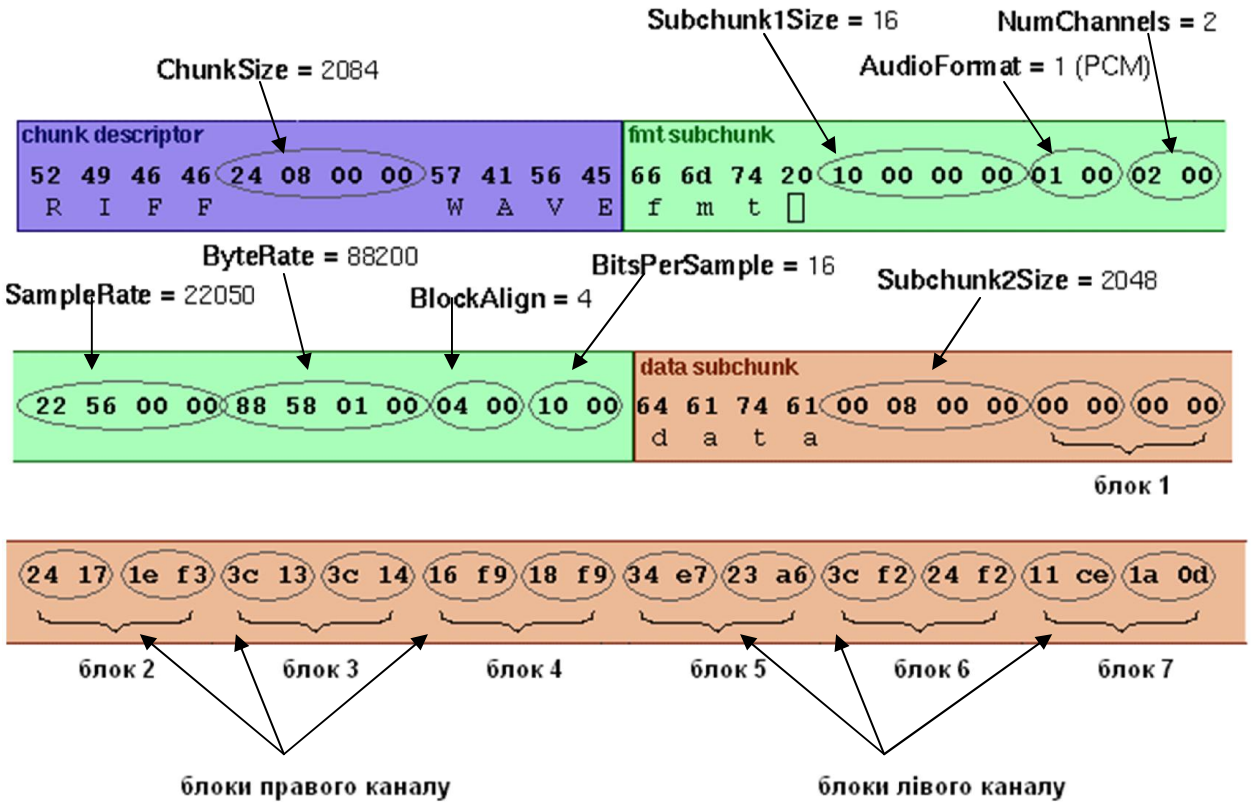

Рисунок 1.5 – Канонічна форма формату файлу WAV

Також в результаті аналізу можна виділити наступні методи побудови стеганофонічних алгоритмів, які наведені на рисунку 1.6.

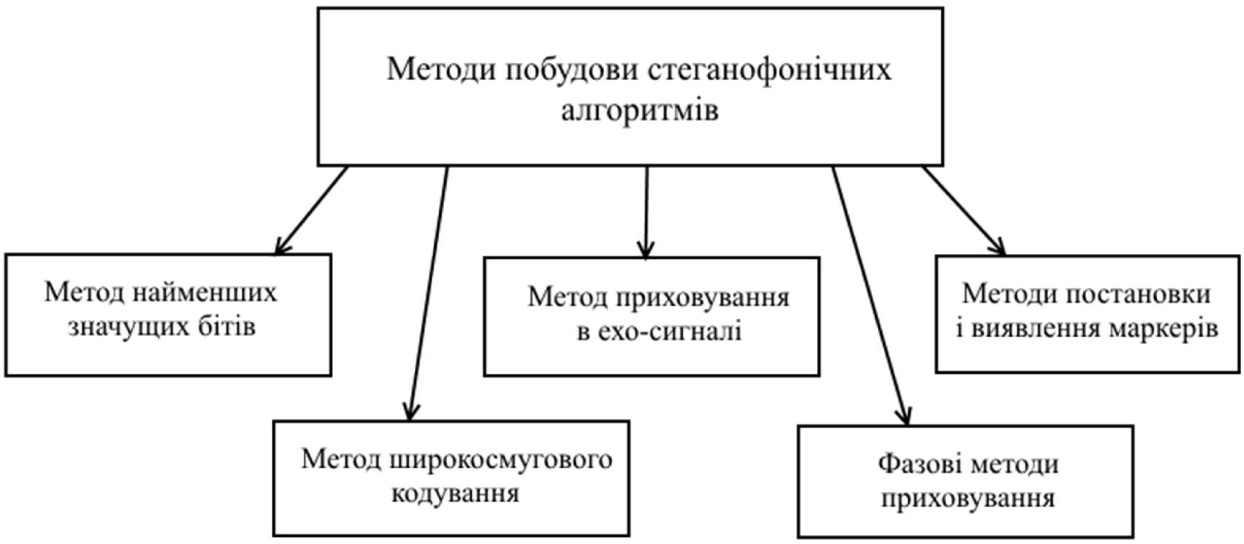

Рисунок 1.6 – Методи побудови стеганофонічних алгоритмів

1.3. Види атак на стеганофонічні системи

При розгляді проблеми атак на стегосистеми постановка задачі розглядається як «проблема в'язнів». Двоє в'язнів, Аліса і Боб, хочуть конфіденційно обмінюватися повідомленнями, не дивлячись на те, що канал зв'язку між ними контролює охоронець Віллі. Для того, щоб таємний обмін повідомленнями був можливий, допускається, що Аліса і Боб мають певний відомий обом таємний ключ [9]. Дії Віллі можуть полягати не тільки в спробі виявлення таємного каналу зв'язку, але і в знищенні повідомлень, які передаються, а також їх модифікації і створенні нових, хибних повідомлень.

Отже, можна виділити три типи порушників, яким повинна протистояти стегосистема: пасивний, активний і зловмисний порушники.

Пасивний порушник може тільки виявити факт наявності стегоканалу і (можливо) читати повідомлення. Чи зможе він прочитати повідомлення після його виявлення залежиться від стійкості системи шифрування, і це питання, як правило, не розглядається в стеганофонії. Якщо в зловмисника є можливість виявити факт передачі таємного повідомлення, то така система вважається нестійкою. Виявлення стегоканалу є найбільш трудомісткою задачею, а захист від цього вважається основною задачею стеганофонії.

Діапазон дій активного порушника значно ширший. Таємне повідомлення може бути ним видалене або знищене. В цьому випадку відправник і адресат мають можливість дізнатися про факт порушення.

Дії зловмисного порушника найбільш небезпечні. Він може не тільки зруйнувати, а й створити хибне стего. Історія протистояння розвідки і контррозвідки знає немало прикладів, коли реалізація цієї загрози приводила до катастрофічних наслідків.

Оскільки пасивний порушник може бути тільки в стегосистемах таємної передачі даних, то атаки саме на такі системи будуть розглянуті більш детально.

Для здійснення тої чи іншої загрози порушник використовує атаки. Найбільш проста атака – суб'єктивна. При цьому порушник детально вивчає підозрілий контейнер і з суб'єктивних міркувань пробує визначити, чи не несе він якоїсь прихованої інформації. Даних тип атак може дати результат тільки при зовсім незахищених стегосистемах. Однак, вона найбільш поширена на початковому етапі виявлення стегосистеми. Первинний аналіз може включати в себе наступні етапи:

- первинне сортування стего по зовнішнім ознакам;
- виділення стего з відомим алгоритмом вбудовування;
- виділення використовуваних стегоалгоритмів;
- перевірка достатності об'єму матеріалу для стегоаналізу;
- перевірка можливості проведення аналізу для часткових випадків;
- аналітична розробка стегоматеріалів, розробка методів розкриття стегосистеми;
- виділення стего з відомим алгоритмами вбудовування, але невідомим ключами і т.д.

У стегоаналізі можна виділити наступні типи атак:

- Атака на основі відомого заповненого контейнера. В цьому випадку в порушника є один або декілька стего. В останньому випадку вважається, що вбудовування повідомлень здійснювалось одним і тим самим методом. Знаючи ключ, порушник отримає можливість аналізу інших стегоповідомлень.

- Атака на основі відомого вбудованого повідомлення. Цей тип атаки в більшій мірі характерний для систем захисту інтелектуальної власності, коли зловмисник знає про спеціальні маркування, які використовує власник для своїх аудіо. Задачею аналізу є отримання ключа. Якщо відповідний прихованому повідомленню заповнений контейнер невідомий, то цю задачу досить важко вирішити.

- Атака на основі вибраного таємного повідомлення. В цьому випадку зловмисник має можливість пропонувати відправнику для повідомлення для передачі і аналізувати отримані стего.

- Адаптивна атака на основі вибраного таємного повідомлення. Ця атака є частковим випадком попередньої. В даному випадку зловмисник має можливість вибрати повідомлення для нав'язування відправнику адаптивно, в залежності від результатів аналізу попередніх стего.

- Атака на основі відомого пустого контейнера. Якщо він відомий зловмиснику, то він завжди може порівняти його з можливим стего і визначити факт наявності стегоканалу.

- Атака на основі відомої математичної моделі контейнера або його частини. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі [9].

Розглянуті вище атаки мають одну особливість: вони не змінюють стегоповідомлення, які відправляються адресату, а також не направлені на протидію роботи декодера. Але такі атаки мають перевагу: адресату і відправнику важко здогадатися про факт виявлення стегоканалу.

Для визначення факту наявності таємного повідомлення в контейнері, використовують статистичний стегоаналіз – вивчають статистичні властивості сигналу [9]. Наприклад, розподілення молодших бітів сигналу має, як правило, шумовий характер (помилки квантування). Вони несуть найменшу кількість інформації про сигнал і можуть використовуватися для вбудовування таємного повідомлення. При цьому, можливо, зміниться їх статистика, що і стане для атакуючого ознакою наявності прихованого каналу.

Для непомітного вбудовування даних стегокодер повинен вирішити три задачі: виділити підмножину біт, модифікація яких мало впливає на якість (незначущі біти), вибрати з цієї підмножини потрібну кількість біт у відповідності з розміром прихованого повідомлення і виконати їх зміну[9]. Якщо статистичні властивості контейнера не змінились, то вбудовування інформації можна вважати успішним. Оскільки розподіл незначущих біт

найчастіше близький до білого шуму, вбудовані дані повинні мати той самий характер. Це досягається за рахунок попереднього шифрування повідомлення або його стиснення.

Стегоаналітик на основі вивчення сигналу завжди може виділити підмножину незначущих біт, виконуючи ті самі припущення, що й стенограф. Далі він повинен перевірити відповідність їх статистики тій, яка мала би бути. При цьому якщо аналітик має кращу модель даних, ніж стенограф, вкладення буде виявлено.

При побудові моделі потрібно враховувати:

- неоднорідність послідовностей відліків;
- залежність між бітами в відліках (кореляцію);
- залежність між відліками;
- неоднакову імовірність умовних розподілів в послідовності відліків;
- статистику довжин серій (послідовностей з однакових біт)[10].

Відповідність реально спостережуваної статистику очікуваній зазвичай перевіряється за допомогою критерію хі-квадрат. Перевірка може здійснюватися на рівні монобітів, дибітів і т.д. Можливі і більш складні тести, аналогічні тим, які застосовуються при тестуванні криптографічно безпечних програмних датчиків випадкових чисел.

Таким чином, протидія статистичному стегоаналізу повинна полягати в побудові математичних моделей сигналів-контейнерів, пошуку на їх основі «дозволених» для модифікації областей і вбудовуванні в них таємної інформації, статистика якої не буде відрізнятися від статистики контейнера. Саме ця характеристика визначає стійкість стегосистеми.

1.4 Комп’ютерні засоби реалізації стеганофонічних алгоритмів

Для VoIP систем існує чотири можливих сценарії передачі прихованих даних [11] (рисунок 1.7). Перший сценарій є найбільш вживаним: відправник і отримувач здійснюють VoIP розмову і в цей час синхронно передають контейнери зі стего. В цьому випадку канал, по якому здійснюється власне розмова такий самий, як і прихований канал передачі даних. меВ цьому випадку відправник і отримувач VoIP пакетів можуть навіть не підозрювати про те, що відбувається обмін стеганофонічними даними.

Засоби реалізації стеганофонічних алгоритмів в комп'ютерних мережах можуть бути поділені на три групи [11] (рисунок 1.8).

Методи першої групи модифікують самі пакети – заголовки мережевих протоколів або поля з корисним навантаженням. Засоби реалізації цих методів включають модифікацію вільних (надлишкових) полів в заголовках IP, UDP або RTP протоколів під час фази розмови і модифікацію самих повідомлень в, наприклад, SIP (Session Initiation Protocol).

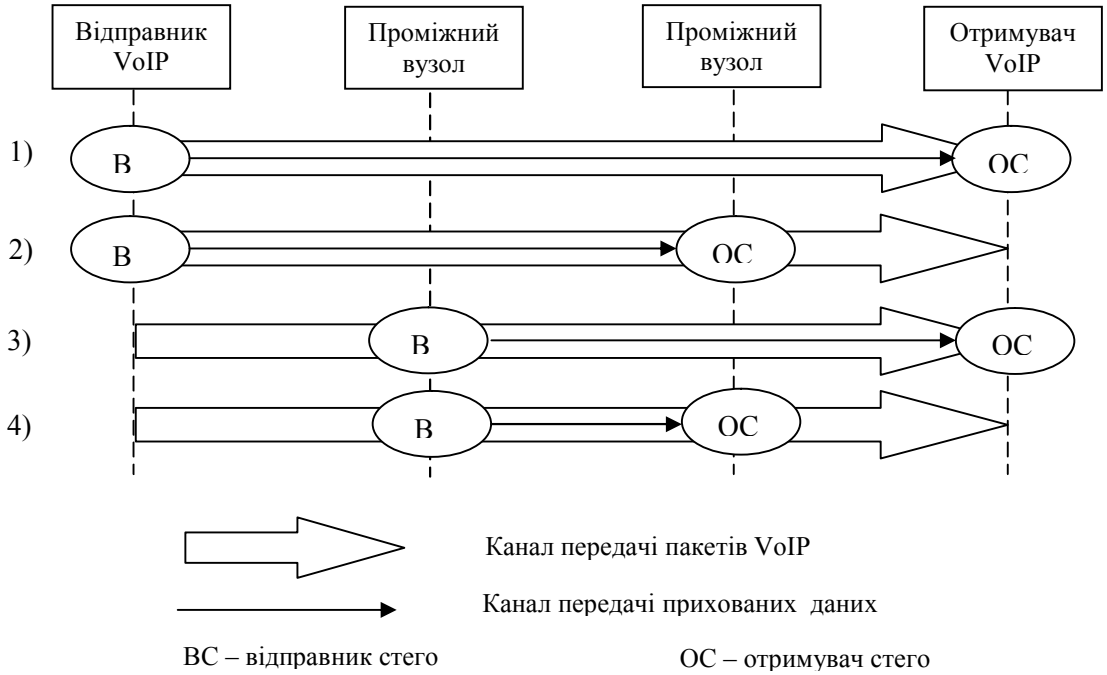

Рисунок 1.7 – Сценарії прихованої комунікації для VoIP

Приховування інформації, яке базується на модифікації бітів пакетів зазвичай застосовує алгоритми створення цифрових водяних знаків, такі як DSSS і QIM.

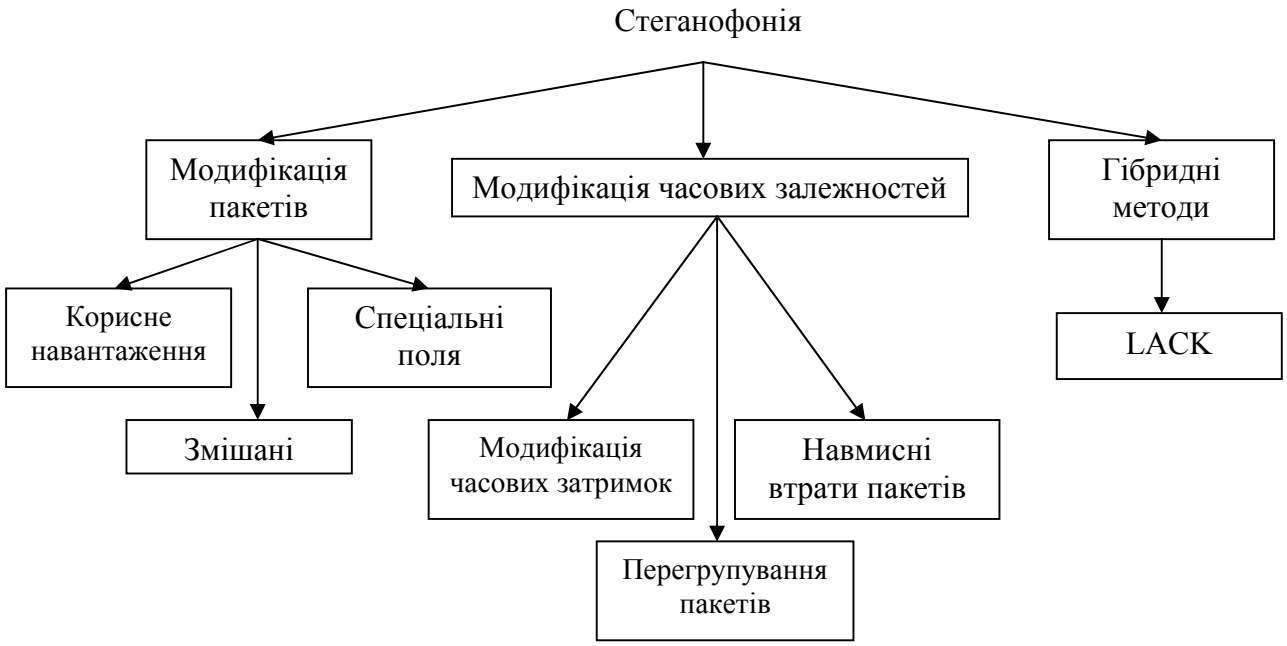

Рисунок 1.8 – Класифікація стеганофонічних методів

Прикладами стеганофонічних методів з цієї групи є:

- методи, які модифікують спеціальні поля протоколів – SIP, SDP, RTP, RTCP (VoIP протоколи) і IP, TCP, UDP (мережеві протоколи);
- методи, які модифікують НЗБ пакетів – алгоритми створення цифрових водяних знаків, техніки кодування мовного сигналу;
- змішані техніки – HICCUPS (Hidden Communication System for Corrupted Networks).

Характеристики даних методів:

Стеганофонічні методи, які використовують спеціальні поля протоколів зазвичай забезпечують високу ємність прихованих даних. Реалізація і виявлення порівняно прості. Недолік: потенційна втрата деякої функціональності протоколів.

Стеганофонічні методи, які модифікують НЗБ пакетів в загальному забезпечують нижчу ємність прихованих даних і їх важче реалізувати та виявити. Недолік: потенційне погіршення якості мови [13].

Змішані техніки забезпечують високу ємність прихованих даних, але їх реалізація є значно важчою, оскільки реалізовується на низькому рівні доступу до апаратного забезпечення. Для таких алгоритмів важко провести стегоаналіз, тому можна сказати, що вони є достатньо стійкими до виявлення. Недолік: збільшений показник помилок в кадрах.

Розглянемо більш детально алгоритм HICCUPS. HICCUPS застосовується для передачі даних в безпровідних LAN[6]. Обмін таємними даними проходить шляхом вбудовування їх в НЗБ кадрів, для яких навмисно створюються неправильні контрольні суми. Зазвичай, станція, яка не належить до якоїсь прихованої групи, відхиляє спотворені кадри з некоректними контрольними сумами. В HICCUPS ці кадри несуть приховані дані і таким чином створюється додатковий канал передачі для цілей стеганофонії.

Сама процедура HICCUPS базується на двох режимах: базовий режим і режим пошкодженого кадру. Це рішення може застосовуватися в прихованих групах користувачів, які повідомлені про передачу таємних даних. Крім того, існує певний ключ, відомий всім членам групи, який служить для перемикання між цими двома режимами.

В базовому режимі обмін даними проходить в полях протоколів. Такий спосіб дозволяє передавати досить незначну кількість даних – менше 1% від доступного простору в кадрах. Коли по каналу передачі передачі передається ключ, вся група користувачів переходить в режим пошкодженого кадру. Цей режим дозволяє майже 100% використання пропускної здатності каналу на певний період часу. Зазвичай, станції, які не входять до прихованої мережі, відхиляють кадри з некоректними контрольними сумами і тому не можуть перехопити таємні повідомлення. Наступна передача ключа по прихованих каналах групи знову повертає їх в базовий режим роботи.

Методи другої групи змінюють часові залежності між пакетами, наприклад, впливаючи на порядок слідування пакетів, модифікуючи затримки пакетів або створюючи навмисні втрати пакетів [4-8].

Прикладами методів з цієї групи є:

- методи, які впливають на порядок слідування пакетів (в VoIP реалізація можлива тільки для RTP);

- методи, які модифікують часові затримки пакетів (в VoIP реалізація можлива для RTP і RTCP; для деяких протоколів, наприклад SIP, неможливе застосування через малу кількість повідомлень);

- методи, які створюють навмисні втрати, пропускаючи послідовність даних від відправника (реалізація можлива для RTP і RTCP протоколів)[11].

Характеристики даних методів:

Потрібна синхронізація між відправником і отримувачем.

Нижча ємність прихованих даних і стегосистема є стійкішою до виявлення в порівнянні з методами реалізації, які використовують спеціальні поля протоколів.

Проста реалізація.

Недолік: потенційне погіршення якості мовного сигналу.

Гібридні методи модифікують і вміст пакетів, і їхні часові залежності. Прикладом засобу реалізації таких методів є LACK (Lost Audio Packets Steganography), запропонований польськими спеціалістами з Варшавського університету [12]. Зупинимося на цьому методі більш детально.

В загальному LACK придатний для широкого класу мультимедійних додатків, які виконуються в режимі реального часу. Але на даний час в більшості він застосовується для VoIP. Цей метод використає той факт, що для звичайних протоколів передачі даних, таких як RTP пакети з надмірною затримкою не використовуються для відновлення переданих даних на отримувачі. Ці пакети вважаються непотрібними і відхиляються [12].

Основна ідея методу полягає в наступному: відправник даних для деяких вибраних аудіо пакетів навмисно створює затримки перед передачею. Якщо отримувач вважає, що затримки цих пакетів є надмірними, він їх відхиляє. НЗБ пакетів з надмірними затримками використовуються для передачі таємних даних. При цьому, якщо отримувач не знає про передачу цих даних, то вони для нього є невидимими.

Ефективність LACK залежить від багатьох факторів, таких як параметри передачі аудіо даних (який тип кодування використовується, розмір кадру, розмір буферу на отримувачі і т.д.) і характеристики мережі (затримки пакетів і можливі втрати пакетів).

LACK є менш складним для реалізації, ніж більшість алгоритмів стеганофонії. При цьому ємність прихованих даних є порівняно такою ж, або навіть вищою.

Стегоаналіз LACK провести важче, ніж для інших стеганофонічних методів, які згадувались вище [12]. Це, в основному, через те, що в IP мережах втрата пакетів відбувається завжди. І якщо кількість втрачених пакетів коливається в межах середньої, тоді важко виявити, чи проходить в даний час прихована передача даних.

1.5. Постановка завдання на дипломну роботу

Можна виділити дві причини популярності досліджень в області стеганофонії в даний час: обмеження на використання крипто-засобів у ряді країн світу і появу проблеми захисту прав власності на інформацію, представлену в цифровому вигляді. Перша причина спричинила за собою велику кількість досліджень у дусі класичної стеганографії (тобто приховування факту передачі інформації), друга – ще більш численні праці в області так званих цифрових водяних знаків (ЦВЗ), спеціальна мітка, непомітно впроваджувана в зображення або інший сигнал з метою тим або іншим чином контролювати його використання.

Останніми роками у зв'язку з широким розповсюдженням мережевих засобів передачі мультимедійної інформації, зокрема, голосового трафіку і відео потоків актуальним є побудова на їх основі потокових стегосистем. Проте, застосування стегосистем, що використовують модифіковані методи,

наприклад, найменш значущих бітів початкові мультимедіа дані обмежується тим, що передача практично всіх потоків цих даних ведеться із застосуванням того або іншого методу стиснення, часто заснованого на психофізіологічній моделі сприйняття людини. Зокрема якщо розглядати оцифровану мову як одне з найпоширеніших джерел мультимедіа трафіку, то залежно від області застосування використовується або один з варіантів диференціальної модуляції або спеціалізовані мовні кодеки. Використання безлічі НЗБ методів стеганографії у такому разі виявляється неефективним і особливу значущість набувають методи стеганографії, що дозволяють проводити вбудовування повідомлень в перцептивно значущі області, які не піддаються істотних спотворенням при обробці сучасними кодеками.

Принципи побудови стеганофонічних алгоритмів показують, що на сьогоднішній день розроблено достатньо багато методів для приховування повідомлень у аудіо сигналах. Зокрема тільки у класичній стеганографії для роботи з аудіо файлами розроблено декілька десятків методів. У зв'язку з цим, та, враховуючи стрімкий розвиток IP-телефонії, комп'ютерної телефонії, мультимедійних конференцій та інших галузей, у яких аудіо сигнал є основним типом даних для передачі, постає питання стійкості стеганофонічних систем.

Аналізуючи ринок відповідних програмних продуктів, легко побачити, що більшість з них для приховування повідомлень використовують різні модифікації методу найменшого значущого біта (НЗБ) [13,14]. Користувач обирає довільний контейнер, розміри якого дозволяють розмістити в ньому повідомлення, і в результаті отримає стего, яке візуально нічим не відрізняється від оригіналу.

Раніше вважалося, що НЗБ аудіо сигналу незалежні між собою та незалежні від усіх інших бітів елемента контейнера. Але насправді між молодшими бітами сусідніх елементів природних контейнерів та між молодшим бітом і іншими бітами елемента контейнера існують суттєві кореляційні зв'язки, які можуть бути порушені «вкрапленням» повідомлення.

Для розпізнавання стего, сформованих з таких контейнерів, достатньо найпростішого аналізу – візуальної атаки на найменші значущі біти.

Отже, для побудови абсолютно стійкої в рамках моделі пасивного супротивника стеганофонічної системи приховане повідомлення не повинно змінювати статистику контейнера.

В стеганофонії є чимало проблем, які поки що знаходяться на початковій стадії свого вирішення [7, 13-15]. Наведемо основні з них:

- побудова стійких стеганофонічних систем в рамках моделей пасивного та активного супротивника;
- отримання оцінок стійкості стеганофонічних систем;
- отримання оцінок складності стеганофонічних алгоритмів та їх порівняльний аналіз;
- моделювання параметрів стійких стегосистем;
- побудова стеганоалгоритмів з мінімальною довжиною ключа при заданій стеганостійкості та інші.

Таким чином, актуальним є наукове завдання моделювання стійкої стеганофонічної системи при заданих характеристиках мережі.

Вирішення цього завдання дозволить підвищити ефективність та захищеність передачі прихованих даних каналами зв’язку.

2 ДОСЛІДЖЕННЯ АЛГОРИТМІВ І СТІЙКОСТІ СТЕГАНОФОНІЧНИХ СИСТЕМ

2.1 Дослідження існуючих стеганофонічних алгоритмів

Стеганофонічні алгоритми будуються з таким розрахунком, щоб максимально використовувати область звукового сприйняття і інші властивості мовних сигналів (тембр, швидкість і т.д.), незначні зміни яких людина не може почути.

Особливості сприйняття людиною звукових коливань дозволяють приховано передавати інформацію через мовне повідомлення. Серед всіх відомих психоакустичних ефектів найчастіше для вирішення цієї задачі застосовують ефект маскування. Суть цього ефекту в наступному: більш інтенсивні мовні відрізки роблять нечутними сигналі, які з’являються до них («маскування вперед») і після них («маскування назад»). Часовий діапазон маскування вперед складає до 20 мс, а назад – до 150 мс. Крім того, існує ще частотне маскування, коли в момент появи більш інтенсивного низькочастотного сигналу стає нечутним більш високочастотних сигнал з меншою амплітудою. Необхідно зазначити, що підйом високих частот зменшує діапазон частотного маскування [4].

Розглянемо обмеження, які пов’язані з обмеженими можливостями нашої слухової системи, які дозволяють вбудовувати додаткову приховану інформацію.

Перше обмеження пов’язано з нечутливістю нашої слуховою системи до провалів спектру в шумовому сигналі. Таким чином, використовуючи режекторну фільтрацію, можна на звуках мовного повідомлення, які породжені турбулентним джерелом, передавати додаткову інформацію. Ці частоти для звука [х] розташовані в діапазоні частот нижче 800 Гц, для звука [ш] – в діапазоні частот від 2кГц до 4кГц, а для звука [с] – на частотах вище 5 кГц. Імовірність зустріти перераховані звуки в українській мові ≈ 0,08, отже за одну

секунду мови можна передати 80 мс прихованої інформації і кількість квантів прихованої інформації складе 1, 2 на одну секунду мови.

Друге обмеження пов’язане з чутливістю нашої слухової системи до змін значень ширини резонансів, які виникають в мовному тракті. Така відносна чутливість складає 30%. Це означає, що мовний сигнал можна корегувати, змінюючи добротність резонансів голосних звуків. В цьому випадку є можливість передати до 200-300 мс прихованої інформації на одну секунду мови з кількістю квантів прихованої інформації 2-3 за одну секунду мови.

Третє обмеження пов’язано з можливістю регулювання мовного сигналу на інтервалах вимушених (моменти часу, коли прискорення повітряного потоку, породжене роботою голосових зв'язок, максимальні) і вільних (коли вплив голосових зв'язок відсутній) коливань [4]. Регулювати тривалість цих інтервалів не можна, оскільки наше слухове сприйняття дуже чутливе до цих змін. Але збільшити амплітуду на інтервалах вимушених коливань можна. Але робити це потрібно дуже акуратно, корегуючи діапазон змін миттєвої частоти для кожного резонансу мовного тракту. Інтервал вимушених коливань не перевищує половини періоду низькочастотного резонансу в мовному тракті, тобто частоту 300-600 Гц. З врахуванням частоти основного тону 100-200 Гц і тривалістю голосних звуків української мови 200-300 мс на одну секунду мови, отримуємо загальну тривалість кодування до 45 мс. Варто зазначити, що цей вид кодування є найбільш складним для виявлення з допомогою сучасних методів аналізу і розпізнавання мовних сигналів. Кількість квантів прихованої інформації при цьому складає від 15 до 40 на одну секунду мови.

Перейдемо до можливості вбудовування специфічних сигналів і завад, які не заважають сприйняттю мовного сигналу. В якості таких сигналів можуть розглядатися збудження на додаткових резонансних частотах. Збудження здійснюють імпульсами тонального джерела, виділеними з самого вихідного мовного сигналу. Цей механізм можна рекомендувати для тих інтервалів, на яких породжуються голосні звуки. Нові резонанси не заважають розумінню вихідного мовного сигналу і на слух сприймаються як деяке покращення

тембру вихідного мовного повідомлення. Тривалість таких адитивних сигналів складає 500-600 мс, а кількість квантів прихованого повідомлення – від 2 до 4 на одну секунду мови [5].

Таким чином, максимальна швидкість передачі прихованої інформації на мовному сигналі може бути 52,2 кванта за одну секунду. Найпростіший спосіб кодування – це режекція звуків, породжених турбулентним джерелом, з швидкістю передачі 1 квант в секунду. Найскладнішим для виявлення ефекту кодування є метод корекції мовного сигналу на часових ділянках вимушених коливань з мінімальною швидкістю передачі інформації 12 квантів. Інформаційна ємність кожного кванта в середньому може складати 2 біти (приблизно 4 стани), так що максимальна швидкість передачі інформації може скласти приблизно 100 біт в секунду.

На практиці стеганофонічні системи, які побудовані по другому принципу, використовуються найчастіше, не дивлячись на багато недоліків, які притаманні цьому методу. Найбільш простим і популярним методом в комп'ютерній стеганофонії є метод, який базується на використанні молодшого біту аудіо (або будь-яких інших мультимедійних) даних – LBS-метод (LeastSignificantBits). Розглянемо цей метод більш детально. Більша частина комп'ютерної інформації «шумить». Шумить все те, що зберігається, передається і обробляється. Оскільки мовний сигнал записується з мікрофона, то в записі присутній деякий рівень шуму, який залежить від якості мікрофона, рівня зовнішніх акустичних завад і похибок пристроїв перетворення каналового сигналу в цифровий. В якості шумових біт зазвичай розглядаються молодші розряди значень відліків, які є шумом з точки зору точності вимірів і несуть найменшу кількість інформації, яка міститься у відліку. При кодуванні стеганофонічного сигналу змінюється останній (молодший) біт сигналу в певні моменти часу з заданим кроком. Для людського вуха це залишається непомітним і сприймається як шум. Але такий метод використовується все рідше, тому що існує ряд властивостей, за якими можна визначити факт приховування інформації в молодших розрядах даних [6].

Найбільш популярними при побудові стеганофонічних систем є наступні методи:

- метод найменших значущих бітів – застосовується при цифровому представленні аудіо сигналу і придатний для використанні при будь-якій швидкості зв'язку. При перетворенні аудіо сигналу в цифрову форму завжди присутній шум дискретизації, який не вносить суттєвих спотворень. «Шумовим» бітам відповідають молодші біти цифрового представлення сигналу, які можна замінити приховуваними даними. В якості стегоключа зазвичай використовується вказівників на місце розташування бітів, в яких містяться таємні дані;

- методи широкосмугового кодування – використовують ті самі принципи, що й методи приховування даних в зображеннях. Їх суть полягає в незначній одночасній модифікації цілого ряду певних бітів контейнера при приховуванні одного біта інформації. Існує декілька різновидів методу. В найбільш поширеному з них вихідних сигнал модулюється високошвидкісною псевдовипадковою послідовністю *w(t)*, яка визначена на області значень {-1; 1}. В результаті цього для передачі результату необхідна більша (інколи більше ніж в 100 разів) полоса пропускання. Зазвичай послідовності *w(t)* вибирають ортогональними до сигналу контейнера. Результуючий стегосигнал*s(t)* являє собою сумарний сигнал контейнера *c(t)* і прихованих даних *d(t)*:

$$s(t) = v(t) + \alpha \times d(t) \times w(t), \qquad (2.1)$$

де коефіцієнт затухання α призначений для вибору оптимального рівня шуму, який вноситься вбудовуваними даними;

- метод приховування в ехо-сигналі – приховування даних шляхом вбудовування еха в аудіо сигнал. Відомо, що при невеликих часових зсувах ехо-сигнал майже не розрізняється на слух. Тому, якщо ввести додаткові часові затримки, величина яких не перевищує поріг, коли їх можуть виявити, то, розбиваючи звуковий сигнал на сегменти, в кожен з них можна ввести

відповідний ехо-сигнал. Для виділення ехо-сигналу і відновлення таємних даних застосовується автокореляційний аналіз. В якості стегоключа тут зазвичай використовують значення величин затримок з врахування вибраних меж для відрізків [5];

- фазові методи приховування – застосовуються як для аналогового, так і для цифрового сигналу. Вони використовують той факт, що плавну зміну фази на слух визначити неможливо. В таких методах таємні дані кодуються або певним значенням фази, або зміною фаз в спектрі. Якщо розбити звуковий сигнал на сегменти, то дані зазвичай приховують тільки в першому сегменті при дотриманні двох умов: потрібно зберігати відносні фази між послідовними сегментами і результуючий фазовий спектр стегосиогнала повинен бути гладким, оскільки різкі скачки фази є демаскуючим фактором.

До побудови стеганофонічних систем висуваються наступні вимоги:

- слухове сприйняття мовних і акустичних сигналів з закладеною в них приховуваною інформацією не повинно різнитися від сприйняття вихідної, відкритої мови або звуку;

- конфіденційні дані, які передаються по відкритих каналах зв’язку і камуфлюютьсямовними або акустичними сигналами або в неявному вигляді містяться в їх параметрах, не повинні бути легко виявлені в цих сигналах-носіях широко поширеними методами і технічними засобами аналізу звуку і мови, які є в наявності на даний час;

- постановка і виявлення стеганофонічних маркерів не повинні залежати від синхронізації цих процесів і від наявності якихось акустичних еталонів;

- спеціальні методи постановки і виявлення стеганофонічних маркерів повинні реалізовуватися на основі стандартної обчислювальної техніки або спеціальних програмно-апаратних засобів на її основі;

- повинна забезпечуватися можливість закладки і виявлення ознак автентичності в акустичний (мовний) сигнал, які б проявлялися при незаконному його копіювання або модифікації незалежно від виду представлення і передачі цього сигналу (аналового чи цифрового);

- повинна забезпечуватися можливість приховування конфіденційної інформації в акустичному (мовному) сигналі незалежно від виду його представлення (аналового чи цифрового) і передачі в відкритих каналах зв'язку.

У більшості випадків ці вимоги можна задовільнити, використовуючи новий підхід до побудови спеціальних стеганофонічних програмно-апаратних засобів аудіо обробки. Цей підхід поєднує ідею переводу аудіо сигналу у вигляд графічних образів (зображень сонограм і фазограм) і назад без втрати інформації [7].

Сліди фонооб'єктів різноманітної природи в вигляді параметрів складових їх сигналів проявляються на зображеннях динамічних спектрограм у вигляді сукупності контурів (ліній) перепаду яскравості або треків (ланцюжків) локальних і глобальних екстремумів кольорової насиченості в рівнях одного кольору. З допомогою спеціального програмного забезпечення такі сліди, а точніше амплітуди і фази вузькосмугових сигналів, контури або треки яких і видно на частотно-часовій сітці динамічних спектрограм, можна реконструювати, модифікувати, знищувати, створювати знову для вирішення конкретної стеганофонічної задачі. Так, в ряді програмних продуктів, реалізована можливість вибірки і обробки вузькосмугових складових ділянки зображення спектрограми досліджуваного фонооб'єкта.

Акуратно затираючи або домальовуючи з потрібним нажимом (амплітудою) окремі обертони мови на ділянках зображень динамічних сонограм, можна залишати тільки їх парну або непарну кількість, відповідно приймаючих їх за одиничні або нульові біти конфіденціальної інформації в процесі її передачі-збереження в мовному сигналі. Крім цього, якщо взяти один з обертонів за опорний, можна просинтезувати всі інші обертони з певним фазовим зсувом по відношенню до нього. Задаючи вектори приведених початкових фаз, можна досягнути достатньо великої місткості вбудованих біт прихованої інформації на одиницю часу. Просинтезована мова буде звучати аналогічно вихідній, оскільки фазові відхилення практично не впливають на слухове сприйняття. Можна також встановити певну шкалу умовних відрізків

на часовій осі. При повному вміщенні в ці відрізки просинтезованих окремих слів або фраз будемо вважати, що передати одиничний біт інформації, а в протилежному випадку – що переданий нульовий біт. Також можна ввести шкалу умовних відрізків і на частотній осі. Невеликі (до 20 %) відхилення темпу і тембру нової мови по відношенню до вихідної також практично непомітні на слух [8].

Крім того, мовний сигнал можна непомітно для слуху передавати і зберігати в іншій ділянці мовного повідомлення, а також поєднувати технології стеганофонії з технологіями стеганографії, «розчиняючи» зображення динамічних акустичних спектрограм в заданих зображеннях, з наступним їх проявленням і синтезом на прийомному кінці каналу зв’язку. Самі зображення сонограм можуть бути використані для передачі і збереження мови на паперових носіях. При реалізації такої технології «мовного підпису», пов’язаних з захищуваним документом по смислу і змісту приблизно таке ж, як і електронно-цифровий підпис, на стандартний лист паперу може бути нанесено в вигляді різноманітних малюнків від 2 до 4 хвилин мови телефонної якості звучання.

На основі запропонованої технології можна здійснити і такий спосіб постановки стеганофонічних маркерів, який полягає в синтезі звукового сигналу по заданому відомому зображенню для наступного збереження на носію або передачі в загальнодоступний канал зв’язку.

Для того, щоб перейти до обговорення питань вбудовування інформації в аудіо сигнали, необхідно визначити вимоги, які можуть бути пред'явлені до стегосистем, що використовуються для внесення інформації в аудіо сигнали:

- приховувана інформація повинна бути по можливості стійкою до наявності різних забарвлених шумів, стиснень з втратами, фільтрування, аналогово-цифровому і цифро-аналоговому перетворень;
- приховувана інформація не повинна вносити в сигнал спотворення, що сприймаються слуховою системою людини;
- спроба видалення приховуваної інформації повинна приводити до

помітного пошкодження контейнера (для ЦВЗ);

- приховувана інформація не повинна вносити помітних змін у властивості та статистику контейнера.

Отож для впровадження приховуваної інформації в аудіо сигнали можна використовувати методи, застосовні в інших видах стеганографії [9]. Наприклад, можна вбудовувати інформацію, ґрунтуючись на особливостях аудіо сигналів і системи слуху людини, чи будувати стегосистеми, що заміщають найменш значущі біти (всі або деякі).

2.2 Підходи щодо оцінки стійкості стеганофонічних систем

Ступінь захищеності стеганофонічних систем оцінюється їх стійкістю. Під стійкістю стегосистем розуміють їх здатність приховувати від кваліфікованого порушника факт таємної передачі повідомлень, можливість протистояти спробам порушника зруйнувати, спотворити, видалити таємні повідомлення, а також здатність підтвердити або спростувати достовірність інформації, яка передається.

В загальному випадку стегосистема є стійкою, якщо порушник, який спостерігає обмін інформацією між відправником і отримувачем, нездатний виявити, що під прикриттям контейнера передаються таємні повідомлення, і тим більше читати ці повідомлення. Відповідно нестійкою є стегосистема в тому випадку, коли зловмисник здатний виявити факт її використання [10].

Розрізняють такі види стійкості стегосистем:

- стійкість до виявлення факту передачі повідомлення;
- стійкість до вилучення прихованих даних з контейнера;
- стійкість до нав’язування хибних повідомлень по каналу таємного зв’язку (імітостійкість);
- стійкість до відновлення таємного ключа стегосистеми.

Якщо стегосистема є стійкою до виявлення факту передачі повідомлення, то вони при цьому є стійкою і до читання прихованої інформації. Протилежне твердження в загальному випадку невірне. Стегосистема може бути стійкою до читання прихованої інформації, але факт передачі деякої інформації під прикриттям контейнера може бути виявлений.

Стійкість стегосистеми до нав'язування хибних повідомлень по каналу таємної передачі характеризує її здатність виявляти і відкидати сформовані порушником повідомлення, які вводяться ним в канал передачі повідомлень з метою видати їх за істинні, тобто ті, які надходять від відправника.

Стійкість до відновлення таємного ключа стегосистеми характеризує її здатність протистояти спробам порушника вичислити таємну ключову інформацію даної стегосистеми. Якщо порушник спроможний визначити ключ симетричної стегосистеми, то він може однозначно виявляти факти передачі таємних повідомлень і читати їх або нав'язувати хибні повідомлення без будь-яких обмежень. Таку ситуацію можна назвати повною компрометацією стегосистеми.

Існують два основних підходи до оцінки стійкості стегосистем:

- оцінка в теоретико-інформаційній моделі системи;
- оцінка в теоретико-складнісній моделі.

Для аналізу стійкості стеганофонічних систем до виявлення факту передачі таємного повідомлення розглянемо модель стегосистем з пасивним супротивником. В даній моделі стегосистеми відомий імовірнісний розподіл пустих контейнерів (P_c) і імовірнісний розподіл стего(P_s). Порушник в контрольованому каналі зв'язку може спостерігати множину можливих пустих контейнерів і стегоконтейнерів. Позначимо цю множину можливих спостережень Q. Порушник, спостерігаючи передачу повідомлення $q \epsilon Q$, висуває дві гіпотези H_c і H_s. Якщо справедлива гіпотеза H_c, то повідомлення q породжене у відповідності з розподілом P_c, а якщо справедлива H_s, то q відповідає розподілу P_s. Правило вирішення полягає в розбитті множини Q на дві частини так, щоб призначити одну з двох гіпотез кожному можливому

повідомленню $q\epsilon Q$. В цій задачі визначення можливі два типи помилок: помилка першого типу, яка полягає у присвоєнні гіпотези H_s, коли вірною є гіпотеза H_cі помилка другого типу, коли прийняте рішення H_cпри правильній гіпотезі H_s. Імовірність помилки першого типу позначається α, імовірність помилки другого типу – β.

Метод знаходження оптимального вирішення задається теоремою Неймана-Пірсона. Правило вирішення залежить від порогу T. Змінні α і β залежать від T. Теорема встановлює, що для деякого заданого порогу T і допустимої максимальної імовірності β, імовірність α може бути мінімізована присвоєнням такої гіпотези H_c для спостереження $q\epsilon Q$, якщо і тільки якщо виконується

$$\log\frac{\mathrm{P_c(q)}}{\mathrm{P_s(q)}} \geq \mathrm{T}. \tag{2.2}$$

Основним інструментом для визначення гіпотез є відносна ентропія або розрізнення між двома розподілами імовірностей P_c і P_s, яка записується у вигляді:

$$D(P_c||P_s) = \sum_{q=Q} P_c(q) log \frac{P_c(q)}{P_s(q)}. \tag{2.3}$$

Відносна ентропія між двома розподілами завжди невід’ємна і дорівнює 0 тоді і тільки тоді вони співпадають.

Використаємо відносну ентропію $D(P_c||P_s)$між розподілами P_c і P_s для оцінки стійкості стегосистеми у випадку пасивного супротивника. Стегосистема називається ε-стійкою проти пасивного порушника, якщо $\mathrm{D(P_c||P_s)} \leq \varepsilon$.

Якщо $\varepsilon = 0$, то стегосистема є ідеальною.

Якщо розподіли контейнера і стего однакові, то $\mathrm{D(P_c||P_s)} = 0$ і така стегосистема є ідеальною. Це означає, що імовірність виявлення факту передачі таємної інформації не змінюється від того, чи спостерігає порушник

інформаційний обмін між адресатом і отримувачем, чи ні. Пасивник супротивник, який володіє довільно великими ресурсами і будь-якими методами стегоаналізами не спроможний виявити факт використання ідеальної стегосистеми [11].

Існує дещо інший підхід до оцінки стегосистеми в теоретико-інформаційній моделі. Стегосистема вважається стійкою, якщо порушник не спроможний отримати ніякої інформації про вбудоване повідомлення, аналізуючи перехоплені стего при умові, що він знає статистичні характеристики пустих контейнерів. В рамках цього визначення підраховується взаємна інформація *I(M;(S,C))* між прихованими повідомленнями *M* і множинами стего*S* і відповідним їм контейнерам *C*. В теоретико-інформаційній стійкій стегосистемі повинна виконуватися рівність *I(M;(S,C))=0*. Як відомо з теорії інформації, взаємна інформація може бути визначена через безумовну і умовну ентропію:

$$I(M;(S,C)) = H(M) - H(M/(S,C)) = 0. \quad (2.4)$$

Це дає фундаментальну умову стійкості стегосистеми вигляду

$$H(M/(S,C)) = H(M). \quad (2.5)$$

Визначення (2.4) означає, що невизначеність порушника відносно повідомлення *M* не повинна зменшуватися при знанні ним стего*S* і контейнера *C*, тобто *M* повинно бути незалежним від *S* і С. Дослідимо умови стійкості стегосистем. Припустимо, що не тільки *S* і *C*, але і їх ентропії *H(S)* і *H(C)* рівні. Розглянемо для випадки.

Нехай жодне повідомлення *M* не вбудоване в контейнер *C*. Очевидно, що в цьому випадку, оскільки *S* і *C* співпадають, то виконується *H(S/C) = H(C/S) = 0*.

В стего*S* поміщене повідомлення *M* з ентропією *H(M)>0*.Очевидно, що

при наявності цієї вбудованої інформації у порушника з'являється відмінна від нуля невизначеність відносно *S*, якщо відомо *C* і невизначеність відносно *C*, якщо відомо S: *H(S/C))>0, H(C/S)>0*. Отже, взаємна інформація між прихованими повідомленнями і відповідними контейнерами у стего вже не може бути рівною нулю: *I(M;(S,C)) = H(M) – H(M/(S,C)) > 0.*

Тому,

$$H(M/(S,C)) < H(M). \tag{2.6}$$

Це означає, що умова стійкості стегосистеми не задовольняється. Можна сказати, що необхідною і достатньою умовою стійкості є:

$$H(S/C) = H(C/S) = 0. \tag{2.7}$$

Отже, можна зробити висновок, що якщо порушнику відомі стего і відповідні їм контейнери, то стегосистема не може бути ідеальною. В рамках теоретико-інформаційної моделі дана стегосистема при атаці порушника з невідомим контейнером не може приховати факту передачі повідомлення [12]. А з виразу (2.5) випливає, що порушник також спроможний дізнатися якщо не повністю, то частково склад цього повідомлення: якщо *I(M;(S,C))>0,* то при відомих *S* і *C* невизначеність порушника про це повідомлення менша його ентропії.

Але розглянуті інформаційно-теоретичні моделі стійкості стеганофонічних систем мають суттєві недоліки:

На практиці неможливо реалізувати абсолютно стійку стегосистему.

Розподіл імовірностей контейнерів на практиці невідомий, або відомий з точністю до деякої дуже приблизної моделі.

Використовувані контейнери найчастіше є оцифрованими образами реальних фізичних процесів, а не результатом роботи генератора випадкових послідовностей.

В моделі не враховується те, що на практиці порушник зазвичай має в наявності лише обмежені обчислювальні ресурси.

Тому пропонується здійснювати оцінку стійкості стегосистеми в теоретико-складнісній моделі. Припустимо, що маємо множину можливих контейнерів *N*, елементи якої *n*ϵ*N* породжуються деяким поліноміальним алгоритмом. Таємне повідомлення *m*ϵ*M* вибирається з множини можливих повідомлень $\mathrm{M} = \{0,1\}^l$. Стегосистема визначається трійкою $< \mathrm{G}, \mathrm{E}, \mathrm{D} >$ поліноміальних алгоритмів.

Алгоритм *G* є процесом генерації ключа, який у відповідь на вхідну стрічку з одиниць породжує псевдовипадковий стегоключ $\mathrm{k} \in \{0,1\}$. Відповідно до принципу Керхгофа стійкість залежить від ключа, а його довжина є параметром таємності стегосистеми. Алгоритм *E* виконує вбудовування інформації, формуючи на основі $\mathrm{c} \in \mathrm{C}, \mathrm{m} \in \mathrm{M}$ і *k,* стегоs $\in$ C. Алгоритм *D* витягує з *s* з використанням ключа *k* повідомлення m'. У випадку, коли контейнер *s* дійсно містив вбудоване повідомлення, то $\mathrm{m}' = \mathrm{m}$. Для визначення присутності стегосистеми порушник повинен вирішити наступну задачу: на основі контейнера $\mathrm{s} \in$ Свизначити, чи існує ключ $\mathrm{k} \in \{0,1\}$, який породжується *G* і повідомлення$m \in M$такі, що *D(s,k) = m* [2].

Варто зазначити, що якщо на структуру прихованого повідомлення не накладаються ніякі обмеження, то для багатьох стегосистем ця задача не може бути вирішена. Справді, будь-яка комбінація біт може бути вкладенням, і навіть якщо порушник якимось чином запідозрить наявність прихованого зв’язку, він все рівно не зможе довести це третій стороні. Тому, накладемо обмеження на структуру прихованого повідомлення: воно повинно мати хоча б якийсь семантичний смисл [13].

Далі вважаємо, що в порушника є стегосистема у вигляді «чорного ящика», тобто він має можливість породжувати стего з вибраних ним контейнерів і таємних повідомлень, не знаючи при цьому ключа. Для цієї цілі у нього є два оракули: один для генерації пустих контейнерів (стеганофонічний

оракул), інший – для отримання з них стего, тобто імітації алгоритму вбудовування (оракул оцінки). Так як обидва оракули імовірнісні, то у випадку вибору першим оракулом декілька разів підряд одного і того ж контейнера, стего будуть отримуватися різні. Це допоможе порушнику виявити структуру алгоритму вбудовування повідомлень.

Атака полягає в наступному. Порушник має неодноразову можливість генерувати контейнери і відповідні їм стего, намагаючись вияснити структуру стегоалгоритму. При цьому існує обмеження, що вся процедура повинна бути поліноміальною по довжині ключа і розміру контейнера. Після того, як він закінчив роботу, йому надаються два випадково вибраних контейнери: один пустий, інший – заповнений. Стегосистема називається умовно стійкою, якщо у порушника нема можливості правильного визначення стего з імовірністю ~0,5. Умовно стійка стегосистема зберігає цю властивість для всіх можливий ключів і всіх можливих контейнерів. [14]

Очевидно, що поняття умовно стійкої стегосистеми більш слабке, ніж поняття стегосистеми, стійкої з інформаційно-теоретичної точки зору і включає її як частковий випадок. Безумовно стійка стегосистема в наведеній вище моделі буде отримана у випадку, якщо зняти обмеження поліноміальності в часі атаки.

2.3. Критерії стійкості стеганофонічних систем

В класичній стеганографії для оцінки стійкості стегосистеми проти атак пасивного зловмисника використовують такі методи [7]:

- за критерієм Хі-квадрат;
- по кількості переходів в потоці НЗБ;
- по групуванню серій в потоці НЗБ.

Існує ряд важливих ознак, які здійснюють вплив на безпечність методів

приховування інформації. Серед них варто виділити:

- неоднорідність послідовностей відліків;
- залежність між бітами в відліках;
- залежність між відліками;
- неоднакова імовірність умовних розподілів в послідовності відліків;
- наявність довгих серій однакових біт;
- кореляція між НЗБ і старшими бітами.

Ці властивості в різній мірі спостерігаються в більшості звукових файлів і можуть бути використані при побудові статистичних критеріїв, які визначають факт приховування інформації в НЗБ.

Критерій Хі-квадрат при восьми розрядному квантуванні визначається наступним чином:

$$\chi^2 = (\mathrm{n}\sum_{\mathrm{i}=0}^{1}\sum_{\mathrm{j}=0}^{127}\frac{\left(\mathrm{v_{ij}}-\lambda_{\mathrm{i}}\cdot\mu_{\mathrm{j}}/\mathrm{n}\right)^2}{\lambda_{\mathrm{i}}\cdot\mu_{\mathrm{j}}}-\mathrm{m})/\sqrt{2\cdot\mathrm{m}}, \qquad (2.8)$$

де v_{ij} - кількість спостережень пари *(i,j)*;

$\lambda_{\mathrm{i}} = \sum_{j=0}^{127} v_{ij}$;

$\mu_j = v_{0j} + v_{1j}$;

i=0,1;

j=0,1,2…127;

m – число ступенів свободи *Xi*-квадрат (m=127);

n – об’єм вибірки.

При проведенні досліджень автор виявив, що використання навіть на 10% НЗБ контейнера з великою імовірністю буде виявленим. Зміна значення статистики незалежності Хі-квадрат є демаскуючою ознакою і визначає наявність таємного каналу передачі інформації [15].

При оцінці стійкості за кількістю переходів в потоці НЗБ досліджується статистика потоку НЗБ контейнера. Даний потік має певне групування нулів і

одиниць, які слідують один за одним, і яке порушується при вбудовуванні додаткової інформації. При оцінці наявності прихованих даних за цим критерієм аналізується кількість переходів від 0 до 1 в початковому файлів і в сформованому стего. Якщо ці дані не мають істотної відмінності, то стегосистема є стійкою.

При оцінці стійкості за групуванням серій в потоці НЗБ досліджується статистика довжин однакових серій в потоці НЗБ контейнера. Визначається кількість переходів з 0 в 0, з 0 в 1, з 1 в 0 і з 1 в 1. Для стійкої системи різниця довжин однакових серій не повинна бути більшою 1% для порожнього і заповненого контейнерів.

Для оцінки рівня стійкості автор пропонує також використовувати критерій оцінки, який ґрунтується на коефіцієнті групування серій:

$$K^{гр} = (s^{ср}\text{-}1)/s^{ср}, \qquad (2.9)$$

де $s^{ср}$- середнє значення довжини серії.

Коефіцієнт групування $K^{гр}$, який змінюється в межах від 0 до 1, легко визначається і дозволяє здійснювати кількісну оцінку рівня прихованості стеганографічного каналу. В цьому випадку критерієм прихованості є коефіцієнт прихованості стегоканалу:

$$K^{пр} = K^{гр}_{вих}\text{-}K^{гр}_{зап}\ , \qquad (2.10)$$

де $K^{гр}_{вих}$ – коефіцієнт групування серій у вихідному файлі;

$K^{гр}_{зап}$ – коефіцієнт групування серій в заповненому контейнері.

Розглянуті критерії дозволяють проводити оцінку стійкості мультимедійних стеганографічних каналів збереження і передачі інформації, а також визначати факт «грубого» втручання в потік молодших розрядів. Найкращими характеристиками для цього володіє метод, що базується на

коефіцієнті групування серій бітів, які слідують один за одним. Більш точну оцінку можна проводити з використанням більш складних моделей, які описуються, наприклад, багатоосновною алгеброю (алгеброю скритності) [16].

Проте критерії стійкості, які використовують в класичній стеганографії, зазвичай не підходять для оцінки стійкості стеганофонічних систем, оскільки більшість цих критеріїв побудовані на статистичному аналізі змін в НЗБ контейнера, в які вбудовані приховані дані.

В роботі запропонований критерій стійкості при виконанні критерію Неймана-Пірсона. Коротко опишемо критерій Неймана-Пірсона. Розглянемо задачу виявлення наявності прихованої інформації як задачу перевірки основної гіпотези H_0– контейнер не містить прихованих даних, за умови, що для неї є всього одна альтернатива, гіпотеза H_1 – контейнер містить приховані дані.

Будь-яке правило виявлення характеризується імовірністю прийняти ту чи іншу гіпотезу в залежності від спостережуваного значення випадкової величини. Нехай $\pi(Z)$ є критичною імовірністю – імовірністю відкинути основну гіпотезу, якщо спостережуваним результатом є Z, тобто

$$\pi(Z) = P(H_1 \mid Z). \tag{2.11}$$

Якість правила визначається імовірностями прийняття і відкидання кожної з гіпотез в залежності від того, яка з гіпотез є вірною. Його характеризують ймовірностями помилок.

Помилка першого роду – відкинути істинну основну гіпотезу H_0, вона зазвичай позначається α:

$$\alpha = P(H_1 \mid H_0). \tag{2.12}$$

Помилка другого роду – прийняти основну гіпотезу, якщо вірною є її альтернатива. Її ймовірність позначається β:

$$\beta = P(H_0 \mid H_1). \tag{2.13}$$

де α – рівень значущості критерію, 1 – β – його потужність. Рівень значущості відповідає імовірності хибного виявлення стего, потужність – це імовірність виявлення стего. Як правило, рівень значущості вибирається заздалегідь, потужність критерію максимізують, тобто ймовірність помилки другого роду намагаються зробити мінімальною. Якщо вибрана критична імовірність, то

$$\alpha = \int \pi(Z) F_0(dZ)\,,\ \beta = \int \big(1 - \pi(Z)\big) F_1(dZ), \tag{2.14}$$

де $F_i(Z)$ – розподіл випадкової величини Z при гіпотезі $H_i(i=0,1)$.

Найбільш потужний критерій з заданим рівнем значущості – критерій Неймана-Пірсона. Він визначений для випадку, коли міра F_1 абсолютно неперервна відносно міри F_0: для всіх множин $C \epsilon R^m$

$$F_1(C) = \int_C^1 f(Z) F_0(dZ). \tag{2.15}$$

Розподіл $P_x(q)$ називають δ-наближеним відносно розподілу $P_0(q)$, якщо

$$\max_{q \in Q} \left| \frac{P_X(q) - P_0(q)}{P_0(q)} \right| \leq \delta < 1. \tag{2.16}$$

Тоді даний критерій формулюється так: якщо в стегосистемі розподіл стего є δ-наближеним відносно розподілу контейнерів і виконується критерій Неймана-Пірсона для заданого рівня значущості α, тоді виконується критерій стійкості

$$\mathrm{D}(\mathrm{P_C}//\mathrm{P_S}) < \frac{1}{\ln a}\left[(\mathrm{t}_\alpha\text{-}1) + \delta\alpha\right]. \tag{2.17}$$

В роботі [10] наводиться наступний критерій оцінки стійкості стегосистем. Нехай C і M – множини контейнерів і прихованих повідомлень відповідно. Під критичним коефіцієнтом приховування (коефіцієнт використовування контейнера під приховані дані) $K_{крит}$розуміють таке значення коефіцієнта приховування, при якому для $\forall q \in Q: q = c \oplus m \mid c \epsilon C, m \in M$, а також для $k = \frac{|m|}{|c|} < К_{крит}$ виконується нерівність $P_s(q) \leq T$, де $P_s(q)$ – результат застосування вибраного методу аналізу до контейнера $q \epsilon Q$.

Допустимим коефіцієнтом приховування $0 < K_{доп} < K_{крит}$ є такий коефіцієнт, що для $\forall q \in Q: q = c \oplus m \mid c \epsilon C, m \in M,\ k = \frac{|m|}{|c|} < К_{доп}$ виконується нерівність $P_s(q) \leq \alpha$, де $P_s(q)$ – імовірність наявності прихованого повідомлення в контейнері q, α – імовірність помилки першого роду для вибраного методу стегоаналізу.

Автор пропонує здійснювати оцінку стійкості по кінцевій множині методів аналізу L, які можуть бути застосовані проти вибраного методу приховування інформації. Допустимий коефіцієнт приховування для даного випадку позначимо як $К'_{доп}$. Для цілей практичної оцінки стійкості стегосистеми рекомендується використовувати граничний коефіцієнт приховування, який визначається як:

$$К_{гкп} = \min_{c \in C} \left(\frac{\max_{m \in M: |m| < |c| \cdot К'_{доп} | К'_{доп} = \min_L (К_{доп})} |m|}{|c|} \right). \qquad (2.18)$$

Стеганофонічну систему на стеганофонічному методі $h \epsilon H$ вважають Δ стійкою до атак пасивного зловмисника, якщо при розширенні множини L існує границя $lim(K_{гкп}) = \Delta$.

Якщо для деякої стеганофонічної системи значення $\Delta = 0$, то стегосистема не є ідеальною і факт її використання може бути виявленим. Якщо $\Delta > 0$, то виявити таємне повідомлення, а відповідно, і виявити стеганофонічний канал зв’язку неможливо.

Стеганофонічну система на стеганофонічному методі $h \epsilon H$ вважають Δ_L стійкою до множини методів аналізу L, де Δ_L визначається як $\Delta_L = 1$, якщо $\Delta_L > 0$.

Якщо стеганофонічна система є Δ_L стійкою до множини всіх відомих методів аналізу, то існуючими на даний момент часу засобами аналізу виявити таємний канал зв'язку неможливо [17]. Крім того, даний критерій може бути використаний при порівнянні різних стеганофонічних методів по заданій множині методів аналізу.

В роботі пропонується ще один критерій оцінки стійкості складних стегосистем, до яких відносяться і стеганофонічні системи. Для таких систем існує множина взаємозв'язаних параметрів, суттєве відхилення яких може мати вирішальне значення для даної системи і провокувати злом такої системи. Допустимо, що для стегосистеми ψ існує множина параметрів $T = \{T_1, T_2, \ldots, T_m\}$, які можуть бути аналізовані супротивником на наявність відхилень розподілів їх значень від очікуваних значень [18]. Ціллю розробника системи є:

- визначення всіх тих параметрів, які мають суттєві відхилення від середньостатистичних значень при створенні прихованого каналу;
- розробка методів приховування, при яких у супротивника, при відомому стегоаналізі контейнера, не з'явиться серйозних причин для припущення про існування прихованого каналу в системі.

Припустимо, що параметр T_i як випадкова величина має функцію щільності розподілу $f(T_i)$. Тоді розіб'ємо інтервал $(-\infty; +\infty)$ на k частин $(-\infty, a_{i1})$, (a_{i1}, a_{i2}), … , $(a_{i,k-1}, +\infty)$ таким чином, щоб мали місце наступні рівності:

$$\int_{-\infty}^{a_{i1}} f(T_i) = \int_{a_{i1}}^{a_{i2}} f(T_i) = \cdots = \int_{a_{i,k-1}}^{+\infty} f(T_i) = \frac{1}{k}.$$

В цьому випадку маємо справу з рівноімовірнісними категоріями і можемо використовувати спрощену формулу для визначення стійкості по параметру T_i.

Для того, щоб отримати оцінку, яка буде враховувати всі параметри T_i потрібно просумувати зважені значення стійкості по всіх параметрах, тобто:

$$V = \sum_{i=1}^{m} \lambda_i \left(\frac{k_i}{n} \sum_{s=1}^{k_i} \left(Y_{i,s}\right)^2 - n_i\right). \quad (2.19)$$

Враховуючи наступні залежності між коефіцієнтами λ_i: $\lambda_i \geq 0$ і $\sum_{i=1}^{m} \lambda i = m$, і, підставляючи в (2.15) отримаємо кінцевий вигляд формули оцінки стійкості для складних стегосистем:

$$V = \sum_{i=1}^{m} \lambda_i \left(\frac{k_i}{n_i} \sum_{s=1}^{k_i} \left(Y_{i,s}\right)^2 - \sum_{i=1}^{m} \lambda_i \, n_i\right). \quad (2.20)$$

Таким чином, ми отримали кінцеву формулу оцінки, котра враховує всі параметри для визначення стійкості стеганофонічної системи.

2.4. Методи підвищення стійкості стеганофонічних систем

Стійкість системи цілком визначається таємністю ключа, сторонній спостерігач не має можливості статистично довести факт існування прихованого повідомлення, знаходження повідомлення без знання ключа є обчислювально складною задачею та ін.

Основними характеристиками будь-якої стегосистеми ми вважаємо її стеганографічну стійкість, обчислювальну складність реалізації та пропускну здатність створюваного системою захищеного каналу зв’язку.

Як вже згадувалось раніше, вибір контейнера є дуже важливим при створенні стеганофонічної системи. Правильно підібраний контейнер дозволяє підвищити стійкість стегосистеми до виявлення порушником. За способом вибору контейнера розрізняють методи сурогатної стеганографії, селективної стеганографії і конструюючоїстеганографії [19].

В методах сурогатної (безальтернативної) стеганографії відсутня можливість вибору контейнера і для приховування повідомлення вибирають

перший-ліпший контейнер, який зазвичай не зовсім підходить для вбудовування даного повідомлення. В цьому випадку біти контейнера замінюються бітами таємного повідомлення таким чином, щоб ці зміни не були помітними. Основним недоліком методу є те, що він дозволяє приховувати тільки незначну кількість даних.

В методах селективної стеганографії припускають, що приховане повідомлення повинно відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів, щоб потім вибрати той, який найбільше підходить для конкретного повідомлення. Частковим випадком такого підходу є знаходження деякої хеш-функції для кожного контейнера. При цьому для приховування повідомлення вибирається той контейнер, значення хеш-функції якого співпадає з значенням хеш-функції повідомлення.

В методах конструюючоїстеганографії контейнер генерується самою стегосистемою. Тут може бути декілька варіантів реалізації. Так, наприклад, шум контейнера може моделюватися прихованим повідомленням. Це реалізується за допомогою процедур, які не тільки кодують приховане повідомлення під шум, але і зберігають модель початкового шуму. В граничному випадку по моделі шуму може будуватися ціле повідомлення. Прикладами такого підходу може бути метод, який реалізований в програмі MandelSteg, де в якості контейнера для вбудовування повідомлення генерується фрак тал Мандельброта, або ж апарат функції імітації (mumicfunction) [18].

Стегосистеми, які використовують принцип заміни молодших бітів елементів контейнерів на біти таємного повідомлення, є нестійкими до статистичних атак. Підвищити їх стійкість можна різними методами, наприклад, переходом до операцій вбудовування вигляду зваженої суми елементів контейнера з елементами прихованого повідомлення. Подібні операції не зберігають баланс імовірностей появи відповідних елементів контейнера і стего і тому володіють більш високою стійкістю до аналізу їх статистик.

Ще одним методом є зменшення степені заповнення контейнера бітами прихованого повідомлення, тобто зменшення пропускної здатності стегоканалу в обмін на підвищення його захищеності. Статистичні атаки на основі критерію Хі-квадрат в більшості випадків нездатні виявити стегоканал при заповненні контейнера на 50% і менше, особливо якщо вбудоване повідомлення розкидане по контейнеру.

Один з методів підвищення стійкості стегосистем з повідомленнями, які вбудовуються в найменш значущі біти контейнера пропонує поділити процес вкладення прихованої інформації на три етапи:

- визначення надлишкових біт, які можна змінювати без шкоди для контейнера;
- вибір найменш значущих бітів, в які буде вбудовуватися таємна інформація;
- корекція статистичних змін в сформованому стего.

На першому етапі оцінюється кількість найменш значущих бітів контейнера, які можна змінити на біти прихованого повідомлення без втрати якості контейнера [20]. Реально для вкладення повідомлення можна використовувати не більше половини знайдених бітів. Якщо знайдених надлишкових бітів не достатньо, необхідно змінити контейнер. Далі по таємному ключу визначаються рівноймовірно розподілені в межах контейнера найменш значущі біти, які замінюються на біти таємної інформації.

Потім сформоване стего оцінюється статистичними тестами і при виявленні відхилень від статистичних характеристик природніх контейнерів та надлишкові біти, які залишилися, використовуються для виправлення цих відхилень. Простим методом корекції є збереження взаємної кореляції і величини ентропії, яка визначається по тесту Маурера. Справді, якщо деякий молодший біт при вбудовуванні змінюється від 0 до 1, то доцільно змінити сусідній найменш значущий біт від 1 до 0 і т.п.

Коректуючі перетворення повинні задовольняти наступним вимогам:

- для будь-якого фрагменту аудіо-файлу розподіл характеристик стего

повинен бути аналогічний їх розподілу в порожньому контейнері;

- кількість виправлень, необхідних для корекції статистичних характеристик, повинна бути малою.

Вдосконалення стегосистем в загальному випадку може бути описано деяким ітеративним процесом. Стегосистеми розробляються і пропонуються їх авторами для використання. Вони досліджуються відомими методами стегоаналізу, при необхідності для них розробляються нові методи аналізу, і так до тих пір, поки не вдається їх зламати. Потім з врахуванням виявлений слабкостей принципи побудови стегосистеми вдосконалюється, але одночасно розвиваються і стегоатаки. Стегоатаки бувають різного рівня складності тому потрібно виділити процес захисту від цих атак.

Цей процес ітеративно продовжується, поки не вдається довести, що при поточному рівні розвитку стегоаналізу дана стегосистема є практично стійкою.

3 МОДЕЛЮВАННЯ ПАРАМЕТРІВ СТІЙКИХ СТЕГОСИСТЕМ

3.1. Математична модель стеганофонічної системи

Будь-яка стегосистема може бути розглянута як система зв'язку. Алгоритм вбудовування ЦВЗ складається з трьох основних етапів:

- генерації ЦВЗ;
- вбудовування ЦВЗ в кодері;
- виявлення ЦВЗ в детекторі.

$$W*, K*, I*, B* \tag{3.1}$$

1) Нехай (3.1) є безліч можливих ЦВЗ, ключів, контейнерів і приховуваних повідомлень, відповідно. Тоді генерація ЦВЗ може бути представлена у вигляді:

$$F: I* \times K* \times B* \rightarrow W*, W = F(I, K, B) \tag{3.2}$$

де W, K, I, B – представники відповідних множин.

Взагалі, функція F може бути довільною, але на практиці вимоги робастності (стійкості) ЦВЗ накладають на неї певні обмеження. Так, в більшості випадків,$F(I, K, B) \approx F(I + \varepsilon, K, B)$, тобто трохи змінений контейнер не приводить до зміни ЦВЗ. Функція F звичайно є складеною:

$$F = T \circ G, \text{ де } G: K* \times B* \rightarrow C* \text{ і } T: C* \times I* \rightarrow W*, \tag{3.3}$$

тобто ЦВЗ залежить від властивостей контейнера. Функція G може бути реалізована за допомогою криптографічно-безпечного генератора ПВП з K в якості початкового значення [21].

Для підвищення робастності ЦВЗ, можуть застосовуватися завадостійкі коди, наприклад, коди БЧХ, згортальні коди [9]. У ряді публікацій відмічені добрі результати, що досягаються при вбудовуванні ЦВЗ у області вейвлет-перетворення з використанням турбо-кодів. Відліки ЦВЗ приймають зазвичай значення з множини $\{-1,1\}$, при цьому для відображення $\{0,1\} \to \{-1,1\}$ може застосовуватися двійкова відносна фазова модуляція (BPSK).

Оператор T модифікує кодові слова, внаслідок чого отримується ЦВЗW^*. На цю функцію можна не накладати обмеження, оскільки відповідний вибір G вже гарантує безповоротність F. Функція T повинна бути вибрана так, щоб незаповнений контейнер I_0, заповнений контейнер I_W і трохи модифікований заповнений контейнер I'_W породжували б один і той же ЦВЗ:

$$T(C, I_0) = T(C, I_W) = T(C, I'_W), \tag{3.4}$$

тобто вона повинна бути стійкою до малих змін контейнера.

2) Процес вбудовування ЦВЗ $W(i,j)$ в початкове зображення $I_o(i,j)$ може бути описаний як суперпозиція двох сигналів:

$$\varepsilon: I^* \times W^* \times L^* \to I^*_w, I_w(i,j) = I_0(i,j) \oplus L(i,j)W(i,j)p(i,j) \tag{3.5}$$

де $I_w(i,j)$ – заповнений контейнер;

$I_o(i,j)$ – порожній контейнер;

$\oplus$ – позначений оператор суперпозиції, що включає, крім складання, усікання і квантування;

$L(i,j)$ – маска вбудовування ЦВЗ, служить для зменшення помітності ЦВЗ;

$W(i,j)$ – функція генерації ЦВЗ;

$p(i,j)$ – проектуюча функція, залежна від ключа.

Проектуюча функція здійснює “розподіл” ЦВЗ по області зображення. Її використання може розглядатися, як реалізація рознесення інформації по

паралельних каналах. Крім того, ця функція має певну просторову структуру і кореляційні властивості, що використовуються для протидії геометричним атакам.

Інший можливий опис процесу впровадження одержимо, представивши стегосистему як систему зв'язку з передачею додаткової інформації. У цій моделі кодер і декодер мають доступ, крім ключа, до інформації про канал (тобто про контейнер і про можливі атаки). Залежно від положення перемикачів А і Б виділяють чотири класи стегосистем (мається на увазі, що ключ завжди відомий кодеру і декодеру) [22].

І клас: додаткова інформація відсутня (перемикачі розімкнені) – "класичні" стегосистеми. У ранніх роботах по стеганографії вважалося, що інформація про канал недоступна кодеку. Виявлення ЦВЗ здійснювалося шляхом обчислення коефіцієнта кореляції між прийнятим стего і обчисленим по ключу ЦВЗ. Якщо коефіцієнт перевищував деякий поріг, виносилося рішення про присутність ЦВЗ. Відомо, що кореляційний приймач оптимальний лише у разі адитивної гауссовой перешкоди. При інших атаках (наприклад, геометричних спотвореннях) ці стегосистеми показували кепські результати.

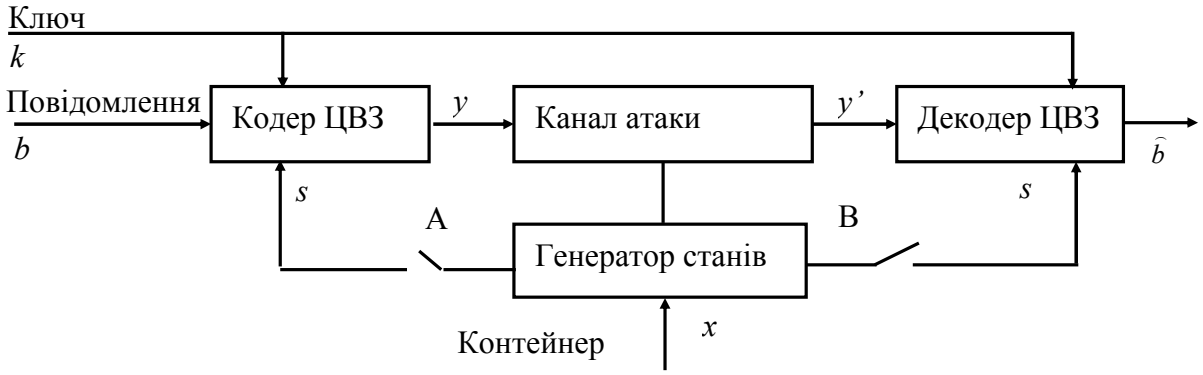

Рисунок 3.1 – Представлення стегосистеми, як системи зв'язку з передачею додаткової інформації

ІІ клас: інформація про канал відома тільки кодеру (А замкнутий, Б розімкнений). Цікавою особливістю схеми є те, що, будучи сліпою, вона має ту ж теоретичну пропускну спроможність, що і схема з наявністю початкового

контейнера в декодері. До недоліків стегосистем II класу можна віднести високу складність кодера (необхідність побудови кодової книги для кожного зображення), а також відсутність адаптації схеми до можливих атак. Останнім часом запропонований ряд практичних підходів, що долають ці недоліки. Зокрема, для зниження складності кодера пропонується використовувати структуровані кодові книги, а декодер розраховувати на випадок як найгіршої атаки.

III клас: додаткова інформація відома тільки декодеру (А розімкнений, Б замкнутий). У цих схемах декодер будується з урахуванням можливих атак. В результаті виходять до геометричних атак системи. Одним з методів досягнення цієї мети є використання так званого опорного ЦВЗ (аналог пілот-сигналу у радіозв'язку). Опорний ЦВЗ – невелике число біт, вбудовуванні в інваріантні до перетворень коефіцієнти сигналу. Наприклад, можна виконати вбудовування в амплітудні коефіцієнти перетворення Фур'є, які інваріантні до афінних перетворень. Тоді опорний ЦВЗ “покаже”, яке перетворення виконав із стего атакуємий. Іншим призначенням пілотного ЦВЗ є боротьба із завмираннями, по аналогії з радіозв'язком. Завмираннями в даному випадку можна вважати зміну значень відліків сигналу при вбудовуванні даних, атаках, додаванні негауссівського шуму і т.д. У радіозв'язку для боротьби із завмираннями використовується метод рознесеного прийому (по частоті, часу, простору, коду). У стеганографії ж використовується рознесення ЦВЗ по простору контейнера. Пілотний ЦВЗ генерується в декодері на основі ключа.

IV клас: додаткова інформація відома і в кодері і в декодері (обидва ключі замкнуті). Всі перспективні стегосистеми повинні будуватися за цим принципом. Оптимальність цієї схеми досягається шляхом оптимального узгодження кодера з сигналом-контейнером, а також адаптивним управлінням декодера в умовах спостереження каналу атак.

Так як в радіозв'язку найбільш важливим пристроєм є приймач, в стегосистемі головним є стегодетектор. Залежно від типу він може видавати двійкові рішення про наявність/відсутність ЦВЗ (у випадку детектора з м'якими

рішеннями) [23]. Розглянемо спочатку більш простий випадок “жорсткого” детектора стего. Позначимо операцію детектування через D. Тоді $D: I_W^* x K^* \rightarrow \{0,1\}$,

$$D(I_w, W) = D\big(I_w, F(I_w, K)\big) = \begin{Bmatrix} 1, \text{якщо } W \text{ є} \\ 0, \text{якщо } W \text{ немає} \end{Bmatrix}, \qquad (3.6)$$

де D– операція детектування;

I – вбудований ЦВЗ;

W– згенерований ЦВЗ.

В якості детектора ЦВЗ зазвичай використовують кореляційний приймач, зображений на рис. 3.2.

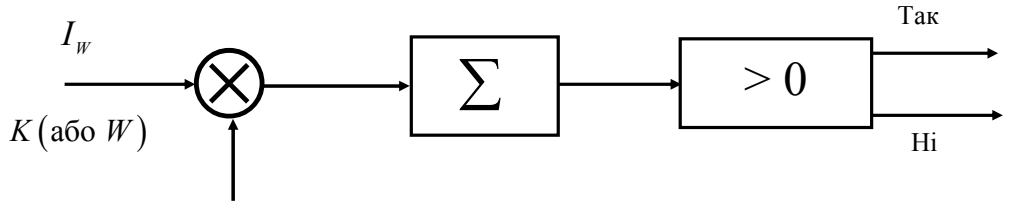

Рисунок 3.2– Кореляційний детектор ЦВЗ

Нехай у половини пікселів зображення, значення яскравості збільшено на 1, а у інших – залишилося незмінним, або зменшено на 1. Тоді$I_w = I_0 + W$, де$F(I_0, K) = W$.Корелятор детектора ЦВЗ обчислює величину $I_w \cdot W = (I_0 + W) \cdot W = I_0 \cdot W + W \cdot W$. Оскільки W може приймати значення ”± 1”, то $I_0 \cdot W$ буде вельми мало, а $W \cdot W$ буде завжди позитивне. Тому $I_w \cdot W$ буде дуже близько до $W \cdot W$. Тоді можна скористатися результатами теорії зв’язку і записати ймовірність невірного виявлення стего, як додаткову (комплементарну) функцію помилок від кореня квадратного з відношення $W \cdot W$ (“енергії сигналу”) до дисперсії значень пікселів яскравості (“енергія шуму”).

Для випадку м’якого детектора і закритої стегосистеми маємо дві основні міри схожості:

$$\delta = \frac{I_0 I_w}{\|I_0\|\|I_w\|}, \tag{3.7}$$

нормований коефіцієнт взаємної кореляції івідстань по Хеммінгу.

$$\delta = N - \sum_{i=1}^{N} i_o i_w, \tag{3.8}$$

У детекторі можливе виникнення двох типів помилок. Існує ймовірність того, що детектор не виявить наявний ЦВЗ і ймовірність помилкового знаходження ЦВЗ в порожньому контейнері (ймовірність помилкової тривоги). Зниження однієї ймовірності приводить до збільшення іншої [25]. Надійність роботи детектора характеризують ймовірністю помилкового виявлення. Система ЦВЗ повинна бути побудована так, щоб мінімізувати ймовірність виникнення обох помилок, оскільки кожна з них може привести до відмови від обслуговування.

3.2. Обґрунтування вибору засобів для розробки програмного забезпечення

Microsoft .NET Framework – це програмна платформа, розроблена компанією Microsoft. Вона може бути інстальована на комп'ютерах з операційною системою Microsoft Windows. Це програмна платформа для створення як звичайних програм, так і веб-програм. Багато в чому є продовженням ідей та принципів, покладених в технологію Java.

Одною з ідей .NET є сумісність служб, написаних різними мовами. Хоча ця можливість рекламується Microsoft як перевага .NET, платформа Java має таку саму можливість [26].

Кожна бібліотека (збірка) в .NET має свідчення про свою версію, що дозволяє усунути можливі конфлікти між різними версіями збірок.

.NET — кросплатформена технологія, на даний момент існує реалізація для платформи Microsoft Windows, FreeBSD (від Microsoft) і варіант технології для ОС Linux в проекті Mono (в рамках угоди між Microsoft з Novell), DotGNU.

Захист авторських прав відноситься до створення середовищ виконання (CLR — Common LanguageRuntime) для програм .NET. Компілятори для .NET випускаються багатьма фірмами для різних мов вільно.

.NET поділяється на дві основні частини — середовище виконання (по суті віртуальна машина) та інструментарій розробки.

Середовища розробки .NET-програм: Visual Studio .NET (C++, C#, J#), SharpDevelop, Borland Developer Studio (Delphi, C#) і т. д. Середовище Eclipse має додаток для розробки .NET-програм. Застосовні програми також можна розроблювати в текстовому редакторі та використовувати консольний компілятор.

Як і технологія Java, середовище розробки .NET створює байт-код, призначений для виконання віртуальною машиною. Вхідна мова цієї машини в .NET називається CIL (CommonIntermediateLanguage), також відома як MSIL (Microsoft IntermediateLanguage), або просто IL. Застосування байт-кода дозволяє отримати кроссплатформеність на рівні скомпільованого проекту (в термінах .NET: *збірка*), а не на рівні початкового тексту, як, наприклад, в C. Перед запуском збірки в середовищі виконання (CLR) байт-код перетворюється вбудованим в середовище JIT-компілятором (justintime, компіляція на льоту) в машинні коди цільового процесора.

Слід зазначити, що один з перших JIT-компіляторів для Java був також розроблений фірмою Microsoft (на даний момент в Java використовується більш досконала багаторівнева компіляція — SunHotSpot). Сучасна технологія динамічної компіляції дозволяє досягнути аналогічного рівня швидкодії з традиційними «статичними» компіляторами (наприклад, C++) і питання швидкодії часто залежить від якості того чи іншого компілятора [28].

Версії .NET Framework:

- .NET Framework 1.0 — випущений 2002 року;
- .NET Framework 1.1 — випущений 2003 року;
- .NET Framework 2.0 — випущений 27 жовтня 2005 року;
- .NET Framework 3.0 (кодове ім'я WinFX) — випущений 6 листопада 2006 року. Містить в собі CLR і компілятори від .NET Framework 2.0, плюс низка нових API: Windows PresentationFoundation (WPF, кодове им'яAvalon), Windows CommunicationFoundation (WCF, кодове им'яIndigo), Windows WorkflowFoundation (WF) і Windows CardSpace(WCS, кодове ім'я InfoCard). Входить до складу Windows Vista;
- .NET Framework 3.5 — випущений 11 січня 2008 року — є розширенням .NET Framework 3.0, додатково реалізуючи інтеграцію з LINQ, підтримку ASP.NET AJAX, підтримку нових протоколів для Web, таких як AJAX, JSON, REST, POX, RSS, ATOM тощо;
- .NET Framework 4.0 — випущений 12 травня 2010 року.

Окрім повної версії .Net, компанією Microsoft також випускається так званий .Net Compact Framework. .Net Compact Framework є обрізаною версією повного фреймворка і несумісний з ним на рівні виконання (програми, написані для Compact Framework не можуть виконуватись виконавчим середовищем від повної версії фреймворка, для їх виконання необхідно встановити виконавче середовище саме від Compact Framework). Внутрішньо Compact Framework працює дещо інакше, ніж повний фреймворк, наприклад “збирач сміття” працює значно більш агресивно, не розділяючи об'єкти на покоління. Відмінності здебільшого обумовлені особливостями роботи компактних пристроїв: меншими розрахунковими можливостями, значно вищими вимогами до низьких енергозатрат, обмеженими графічними можливостями [29].

Основні принципи та переваги .NET

Взаємодія з іншими програмами. Оскільки часто необхідно пов’язати функціональність .NET із програмами, які виконуються поза середовищем .NET, платформа надає можливості для взаємодії з сторонніми компонентами:

COM-компонентами – за допомогою InteropServices, Native-кодом – за допомогою механізму P/Invoke.

Спільне середовище виконання (CommonLanguageRuntime, CLR). Всі .NET-програми виконуються у спеціальній віртуальній машині. Завдяки цьому можна очікувати від всіх програм однакової поведінки в плані керування пам'яттю, безпеки та обробки помилок.

Незалежність від мови програмування. Платформа .NET містить так звану спільну систему типів (CommonTypeSystem, CTS), яка специфікує всі допустимі типи даних, якими може оперувати CLR, і описує, яким чином вони можуть чи не можуть взаємодіяти один з одним. Завдяки цьому бібліотеки класів, написані для CLR однією з мов програмування, можуть бути використані в проектах, що розробляються на іншій мові.

Легкість в перенесенні. .NET Framework спроектовано таким чином, що вона теоретично незалежна від платформи, а отже, може бути крос-платформенний. Програми для .NET не компілюються відразу в машинний код, а тільки в проміжне представлення коду, яке називається CommonIntermediateLanguage (CIL). При запуску програми на цільовій платформі трансляцією проміжного коду в машинний код займається JIT(JustInTime)-компілятор. Тому .NET-програма може виконуватись на будь-якій архітектурі, для якої реалізовано середовище виконання .NET відповідної версії. В даний момент вже існує реалізація .NET для Unix-подібних платформ (проект Mono під керівництвом компанії Novell).

"Garbagecollection" – автоматичне звільнення пам'яті, зайнятої об'єктами, що більше не використовуються. Ця можливість звільняє програміста від відповідальності за виділення ділянок пам'яті та їх вивільнення.

Мови програмування в .NET:

- Вбудовані (постачаються разом з .NET Framework)
- C#;
- J#;
- VB.NET;

- JScript .NET;
- C++/CLI — нова версія C++ (Managed).

Для створення GUI додатків в Microsoft. NET, Microsoft пропонує використовувати технологію Windows Forms. Windows Forms - новий стиль побудови програми на базі класів. NET Framework classlibrary. Вони мають власну модель програмування, яка більш досконаліше, ніж моделі, засновані на Win32 API або MFC, і вони виконуються в керованої середовищі. NET CommonLanguageRuntime (CLR).

Windows Forms - одна з найбільш цікавих можливостей Microsoft. NET. Якщо ви знайомі з MFC (або Windows API), то Windows Forms гарний початок для роботи з . NET Framework classlibrary, тому що вона дозволяє писати традиційні GUI додатки з вікнами, формами і т.п. речами. Одного разу, почавши працювати з Windows Forms ви зможете швидко зрозуміти. NET Framework [30].

Головна вигода від написання Windows-додатків з використанням Windows Forms - це те, що Windows Forms гомогенізують (створюють однорідну (гомогенну) структуру) програмну модель і усувають багато помилок і протиріччя від використання Windows API. Наприклад, кожен досвідчений програміст під Windows знає, що деякі стилі вікна можуть застосовуватися тільки до вікна, коли воно вже створено. Windows Forms значною мірою усувають таке протиріччя. Якщо ви хочете існуючого вікна задати стиль, який може бути присвоєний тільки в момент створення вікна, то Windows Forms спокійно знищить вікно і знову створить його з вказаним стилем. Крім того,. NET Framework classlibrary набагато багатший, ніж Windows API, і коли ви будете писати програми, використовуючи Windows Forms, ви отримаєте в розпорядження більше можливостей. Написання програми з використанням Windows Forms потребують меншого кількості коду, ніж додатки, які використовують Windows API або MFC.

Незважаючи на дуже серйозні розбіжності між компонентною об'єктною моделлю COM (основного стандарту Microsoft для компонентного

проектування та реалізації програмного забезпечення) і моделлю JavaBeans, базовим стандартом SunMicrosystems для компонента, мова програмування C # має досить багато спільного з мовою Java . Природно, чимало рис мова програмування C# успадкувала і від свого попередника, створеного корпорацією Microsoft, мови VisualBasic.

Перелічимо найбільш характерні риси подібності мов програмування C # і Java. Перш за все, обидві мови належать до категорії об'єктно-орієнтованих і припускають єдиність наслідування. Іншими важливими особливостями, які зближують мови програмування C# і Java, є механізми інтерфейсів, обробки виняткових ситуацій, а також процесів або "ниток" (threads). "Збірка сміття" і простору імен реалізовані у цих двох мовах подібним чином. Обидві мови програмування характеризуються сильною (суворою) типізацією та динамічним завантаженням коду при виконанні програми.

Від свого прямого попередника, мови програмування C++, мовою C# успадковані наступні механізми: "перевантаження" операторів, небезпечні арифметичні операції з плаваючою точкою, а також ряд інших особливостей синтаксису. Але, незважаючи на те, що цілий ряд конструктивних синтаксичних механізмів і особливостей реалізації успадкований мовою програмування C # від прабатьків (C++, VisualBasic і Java), можливості цієї нової мови програмування не обмежуються сумою можливостей його історичних попередників.

До числа принципово важливих рішень, які реалізовані корпорацією Microsoft у мові програмування C#, можна віднести наступні:

- компонентно-орієнтований підхід до програмування (який характерний і для ідеології Microsoft. NET в цілому);
- властивості як засіб інкапсуляції даних (характерно також в цілому для ООП);
- обробка подій (наявні розширення, в тому числі в частині обробки виключень, зокрема, оператор try);
- обробка подій (наявні розширення, в тому числі в частині обробки

виключень, зокрема, оператор try);

- делегати (delegate - розвиток покажчика на функцію в мовах C і C++);
- індексатори (indexer - оператори індексу для звернення до елементів класу-контейнера);
- перевантажені оператори (розвиток ООП);
- оператор foreach (обробка всіх елементів класів-колекцій, аналог VisualBasic);
- механізми boxing і unboxing для перетворення типів;
- атрибути (засіб оперування метаданими в COM-моделі);
- прямокутні масиви (набір елементів з доступом за номером індексу і однаковою кількістю стовпців і рядків).

Перш за все, розглянемо узагальнену структуру програми на мові програмування C#. Програма на C# може складатися як з одного, так і з декількох файлів, що містять вихідний текст на мові програмування C#. Кожен такий файл має розширення CS.

Будь-який файл з вихідним текстом на мові програмування C# може як містити простір імен, так і не містити їх.

Нарешті, кожен простір імен може як містити опис класів (одного або декількох), так і не містити.

Розглянемо більш детально реалізацію двох основних сімейств типів даних, а саме, типів-посилань і типів-значень, стосовно мови програмування C#. Для визначеності візьмемо випадок одного з найпростіших об'єктів мови програмування C#, а саме, змінної.

Відповідно з назвами, змінна в разі застосування типів-значень містить власне значення, а при використанні типів-посилань - не саме значення, а лише посилання (покажчик) на нього.

Місцем зберігання змінної, визначеної як тип-значення, є стек, а визначеної як контрольний тип - "купа" (останнє необхідно для динамічного виділення та звільнення пам'яті для зберігання змінної довільним чином).

Значенням, яким значення, яким ініціалізується змінна за замовчуванням (необхідність виконання цієї вимоги диктується ідеологією безпеки Microsoft .NET) у разі використання типу-значення є 0 (для цілого або дійсного типу даних), false (для логічного типу даних), '\ 0' (для строкового типу даних), а у разі використання типу-посилання - значення порожнього посилання null.

У мові програмування C#, де об'єкти мають істотно більш складну структуру, вводиться поняття області опису, під якою розуміють фрагмент програми, до якого відноситься даний опис.

Проаналізувавши основні особливості мови програмування C #, а також дослідивши структуру та принципи побудови програм на цій мові, позначимо найбільш очевидні переваги досліджуваного мови програмування.

Перш за все, необхідно відзначити, що мова програмування C # претендує на справжню об'єктну орієнтованість.

Крім того, мова програмування C # покликана практично реалізувати компонентно-орієнтований підхід до програмування, який спричиняє меншу машинно-архітектурну залежність результуючого програмного коду, більш гнучку, переносимість та легкість повторного використання програм.

Принципово важливою відмінністю від попередників є початкова орієнтація на безпеку коду (що особливо помітно в порівнянні з мовами C і C++).

Уніфікована, максимально близька за масштабом і гнучкістю до CommonTypeSystem, прийнятої в Microsoft. NET, система типізації є важливою перевагою мови C#.

Розширена підтримка подійно-орієнтованого програмування вигідно відрізняє мову програмування C# від цілого ряду попередників.

Мова програмування C# є "рідною" для створення додатків в середовищі Microsoft. NET, оскільки найбільш тісно і ефективно інтегрована з нею.

Об'єднання кращих ідей сучасних мов програмування (Java, C++, VisualBasic та ін.) робить мову C# не просто сумою їх достоїнств, а мовою програмування нового покоління.

Для створення Windows додатку вибраний інструментальний засіб VisualStudio 2010. VisualStudio значно спрощує розробку додатків. Він дозволяє звести до нуля кількість помилок, які пов’язані з синтаксисом мови, оскільки перевіряє це ще на етапі компіляції проекту. Також є зручні можливості для роботи з WindowsForms. VisualStudio дозволяє без значних зусиль розробити зручний користувацький інтерфейс за допомогою стандартних елементів управління.

3.3 Програмне забезпечення для моделювання параметрів стійких стегосистем

Основним завданням розробленого програмного забезпечення є моделювання параметрів стеганофонічної системи за заданими критеріями, а саме: користувач, задаючи певні характеристики мережі, в якій відбувається передача мовного сигналу, має отримати рекомендації щодо того, який алгоритм стиснення мовного сигналу використовувати, скільки часу повинна тривати передача сигналу (тривалість дзвінка).

Для мереж в IP-телефонії важливими є такі характеристики:

-затримки пакетів;

- відсоток втрати пакетів;

- якість передачімовного сигналу.

При визначенні характеристик стеганофонічної мережі особливу увагу потрібно звернути на алгоритми стиснення, які використовуються для передачі мовного сигналу.

В роботі [12] проведено аналіз методів стиснення мовного сигналу, наведено порівняльну характеристику алгоритмів стиснення мовних сигналів.

До переліку основних характеристик алгоритмів стиснення мови включено:

- швидкість передачі мовних сигналів;

- довжина кадру – міра кількості часу, що визначає елементарний відрізок мовного сигналу, який обробляється алгоритмом стиснення;

- затримка – час, необхідний для стиснення мовного сигналу;

- завадостійкість – здатність алгоритму правильно функціонувати при наявності завад.

- MOS (mean opinion score) – суб'єктивна оцінка якості мовлення, яка одержується шляхом опрацювання оцінок, що даються групами слухачів.

Оцінки інтерпретуються наступним чином:

- 4-5 – висока якість мовлення,

- 3.5-4 – прийнятна якість мовлення,

- 3-3.5 – задовільна якість мовлення,

- 2.5-3 – незадовільна якість мовлення, потребує концентраціїуваги для розуміння.

В таблиці 3.1 наведена порівняльна характеристика алгоритмів стиснення мовного сигналу.

Таблиця 3.1 – Порівняння характеристик алгоритмів стиснення мовних сигналів

Стандарт	Алгоритм стиснення	Швид-кість, Кб/с	Кадр, мс	Затримка, мс	MOS	Завадо-стійкість
1	2	3	4	5	6	7
ITU G.711	PCM A-law / PCM u-law	64	0,125	0,125/0,75/ 5	4,15	10
ITU G.722	SB-ADPCM	64	40	5	4,1	9
		56	35			9
		48	30			8
ITU G.721	ADPCM	32		5	4,1	9
ITU G.726	ADPCM	40	25	5	3,91	9
		32	0,125/ 20	1/5		9
		24	15	5		8
		16	10	5		8
ITU G.728	LD-CELP	16	0,625/ 10	2,5/3 … 5	3,69	4
ITU G.729	CS- ACELP	8	10	10	3,96	
ITU G.729a	CS-ACELP	8	10	10	3,71	
ITU G.723.1	MP-MLQ	6,3	30/24	30/37,5	3,93	

Продовження таблиці 3.1

ITU G.723	ACELP	5,3	30/20	30/37,5	3,66	
INMAR-SAT-M	IMBE	6,4		80	3,1	
	IMBE	3,6				
ETSI GSM	RPE-LTP	13	20		3,3	
ETSI TETRA	ACELP	4,8			3,4	
США	MELP	2,4		45	3,5	
USFS 1015	LPC10e	2,4			2	
TIA IS-54	VSELP	5,6	20			
D-AMPS	VSELP	7,95	20		3,3	
TETRA	ACELP	4,57	30			
eXpressDSP	RCELP	3,6		30	3,5	
eXpressDSP	MMBE	2,4	30	45	3,5	
eXpressDSP	ICELP	4,8	30	60	3,7	
AudioCodes	NetCoder	6,4	20		3,85	
AudioCodes	NetCoder	8	20		4,1	
USFS 1016	CELP	4,8				
USFS 1015	LPC10e	2,4				

При визначенні коефіцієнту передачі прихованих даних в мережевих пакетах враховуються відсоток вбудовування для алгоритму стиснення мови [1].

Вхідними даними для створюваного додатку є:

- розмір прихованих даних;
- бажана якість мовного сигналу;
- затримка пакетів в мережі;
- відсоток втрати пакетів в мережі.

Після введення початкових даних відкидаються методи стиснення, які не забезпечують бажану якість мовного сигналу. Далі визначається метод стиснення, який є оптимальним при заданих параметрах. Для цього спочатку визначається розмір загальних даних, які слугують контейнером для передачі прихованих даних потрібного розміру:

$$S_1 = \frac{100 \cdot ds}{IR}, \tag{3.9}$$

де ds – розмір прихованих даних;

IR – можливий відсоток приховування даних в кадрах.

Крім цього, потрібно врахувати те, що в мережі постійно йде втрата пакетів. Тому загальний розмір контейнера для передачі прихованих даних буде мати розмір:

$$S = S_1 + \frac{S_1 \cdot LR}{100}, \tag{3.10}$$

де *LR* – відсоток втрати пакетів.

Далі, враховуючи розмір кадру для конкретного алгоритму, визначаємо кількість пакетів, необхідних для передачі контейнера:

$$PA = \frac{S}{fs}, \tag{3.11}$$

де *fz* – розмір кадру.

Для визначення часу, необхідного для передачі даних заданого розміру потрібно врахувати швидкість передачі даних для даного алгоритму стиснення:

$$T = \frac{PA}{sp} + PA \cdot d/60, \tag{3.12}$$

де *sp* – швидкість передачі даних,

d – затримка пакетів.

Метод стиснення, який при заданих параметрах забезпечує найшвидшу передачу даних по мережі і буде вважатися оптимальним для використання в стеганофонічній системі.

Для тестування розробленого програмного забезпечення введемо розмір прихованих даних 1 кВ, якість мовного сигналу «висока», затримки пакетів мережі 5 мс і втрати пакетів 2%. Бачимо, що оптимальним алгоритмом стиснення є G.722 і йому для передачі даних потрібно ~6 с. Збільшимо розмір прихованих даних до 10 кВ. Решту характеристик залишимо такими ж. Знову ж кращим алгоритмом є G.722. Змінимо відсоток втрати пакетів і затримки. Оптимальним алгоритмом знову є G.722 (рисунок 3.3-3.6). Це можна пояснити

тим, що для методів стиснення, які забезпечують високу якість мовного сигналу, G.722 має найвищу швидкість передачі пакетів при однакових величинах затримки пакетів.

При збільшенні прихованих даних більше 200 кВ значно збільшується тривалість розмови (більше 30 хв), що є небажаним через можливість обривів, збільшення втрати пакетів. При істотному збільшенні розміру прихованих даних потрібні додаткові дослідження алгоритмів стиснення.

Для прийнятної якості мовлення в більшості тестувань найкращим виявився метод G.726. Він також показує невеликий передачі даних (рисунок 3.4).

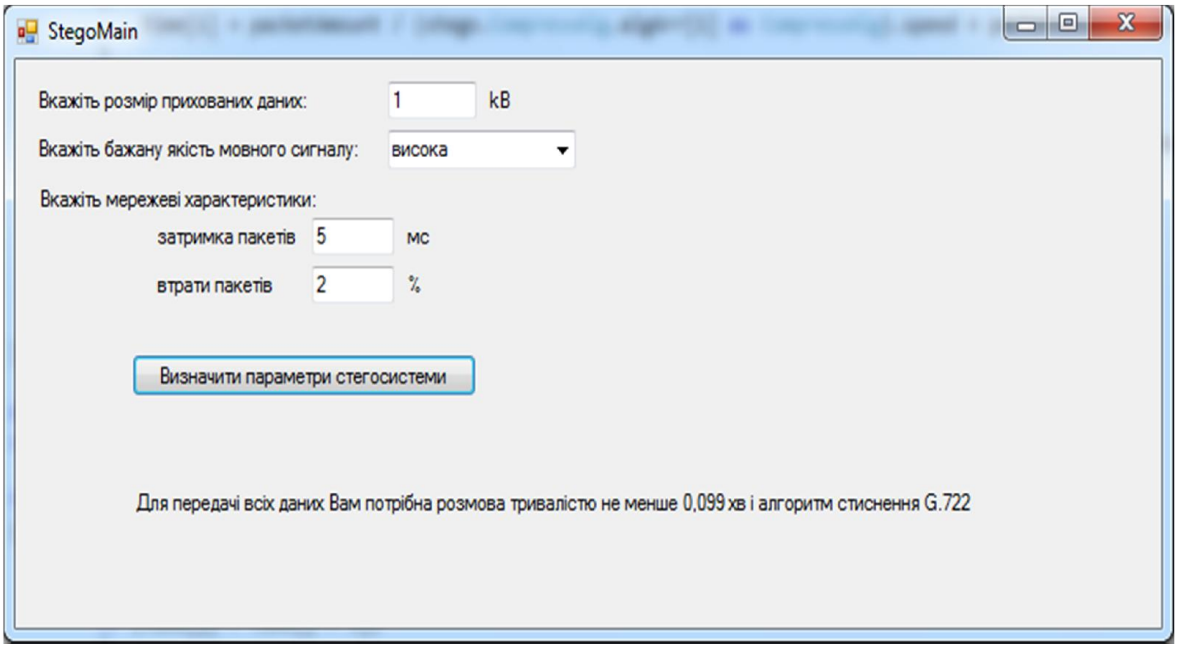

Рисунок 3.3 – Результатироботи програми при високій якості мовного сигналу

Для задовільної якості мовлення в більшості тестувань найкращим виявився метод GSM, але час передачі даних значно збільшується, в порівнянні з іншими алгоритмами (рисунок 3.5).

При виборі стеганофонічного методу потрібно також враховувати, що методи, які модифікують мережеві пакети, призводять до погіршення якості

мовлення, а гібридні та змішані методи при досить високій ємності вбудованих даних дають вищу стійкість стегосистеми в порівнянні з іншими методами [1].

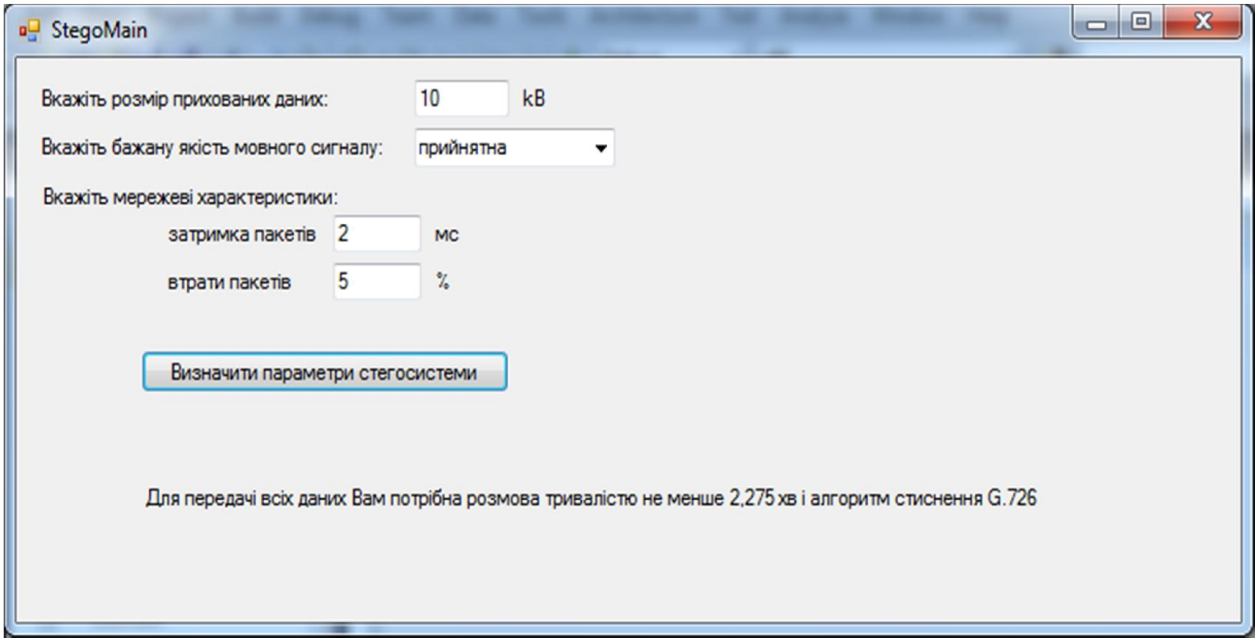

Рисунок 3.4 – Результатироботи програми при прийнятній якості мовного сигналу

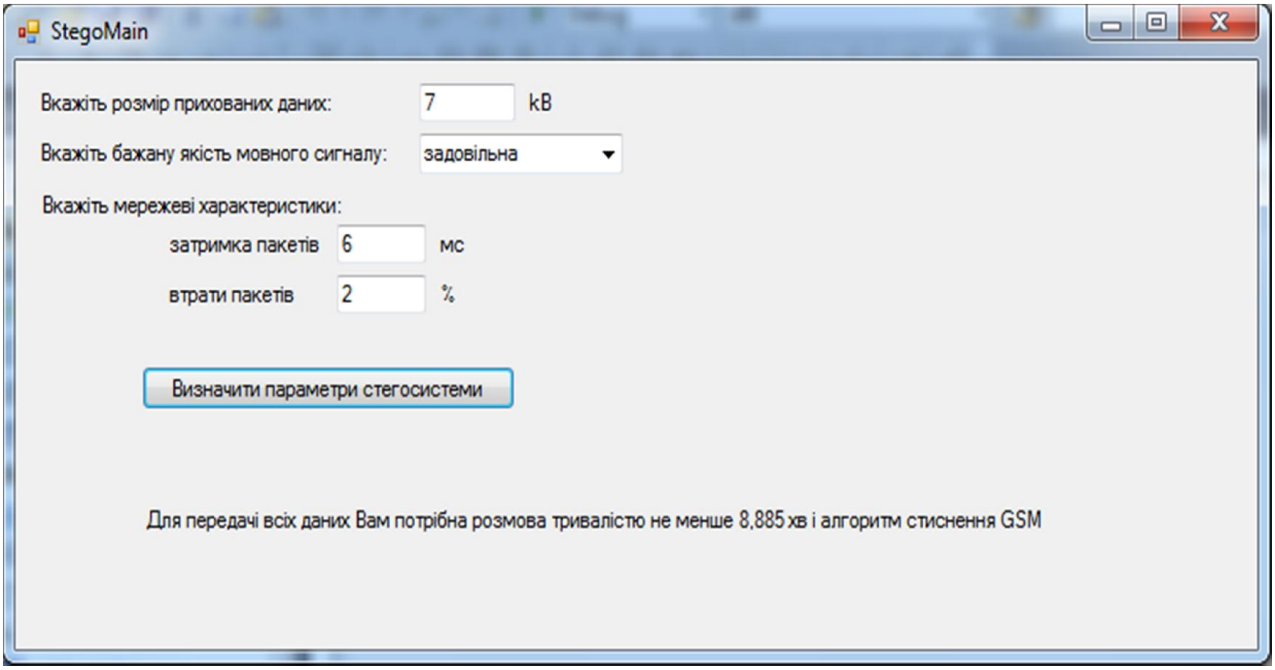

Рисунок 3.5 – Результати роботи програми при задовільній якості мовного сигналу

Приховування даних у звукових аудіо-сигналах є особливо перспективним, оскільки слухова система людини (ССЛ), працює у надширокому динамічному діапазоні. ССЛ сприймає більше ніж мільярд до одного у діапазоні потужності та більше ніж тисяча до одного у частотному діапазоні. Проте, гострою є і чутливість до адитивного флуктуаційного (білого) шуму. Відхилення у звуковому файлі можуть бути виявлені впритул до однієї десятимільйонної (на 70 дБ нижче за рівень зовнішніх шумів).

Не дивлячись на це, існують певні можливості для приховування інформації і в аудіосередовищі. Хоча ССЛ і має широкий динамічний діапазон, вона характеризується досить малим різницевим діапазоном. Як наслідок, гучні звуки сприяють маскуванню тихих звуків. Крім того, ССЛ не спроможна розрізнювати абсолютну фазу, розрізнюючи тільки відносну. Зрештою, існують деякі спотворення, викликані оточуючим середовищем, які є настільки звичайними, що у більшості випадків ігноруються слухачем. Подібні особливості слухового апарату дозволяють вдало використовувати аудіосередовища з метою стеганографічного захисту конфіденційної інформації. Особливий внесок у розвиток аудіостеганографії зробили W. Bender, N. Morimoto та ін.

ВИСНОВКИ

В магістерській роботі розв’язана актуальна науково-технічна підвищення стійкості стеганофонічної системи шляхом моделювання параметрів стегосистем при заданих мережевих характеристиках.

У результаті роботи проведений аналіз методів побудови стеганофонічних систем та вимог, які на сьогоднішній день до них висуваються, виявлені недоліки цих методів за розглянуті можливі алгоритми усунення цих недоліків.Для досягнення поставленої задачі виконано такі дії:

1. Проведено аналіз атак на стегосистеми. Зокрема, досліджено основні етапи здійснення атаки та послідовність дій, яку виконує зловмисник. Протидія статистичному стегоаналізу повинна полягати в побудові математичних моделей сигналів-контейнерів, пошуку на їх основі «дозволених» для модифікації областей і вбудові в них таємної інформації, статистика якої не буде відрізнятися від статистики контейнера.

2. Встановлено, що для побудови абсолютно стійкої в рамках моделі пасивного противника стеганофонічної системи приховане повідомлення не повинно змінювати статистику контейнера.

3. Проведено аналіз критеріїв, за якими здійснюється оцінка стійкості стеганофонічної системи.

4. Представлено модель стеганофонічної системи та проаналізовані параметри, які впливають на якість роботи стеганофонічної системи. На основі цих даних шляхом експериментального дослідження встановлено, які з алгоритмів стиснення є оптимальними при певних параметрах мережі та вхідних даних стеганофонічної системи.

5. Розроблено та протестовано програмне забезпечення, яке дозволяє виконувати пошук оптимальних параметрів стегосистеми при заданих критеріях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hiding data in VoIP / Mazurczyk W., Lubacz J., Szczypiorski K.– December, 2008.
2. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М.: СОЛОН-Пресс, 2002. – 261 с.
3. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.
4. К оценке эффективности защиты акустической (речевой) информации / Хорев А.А., Макаров Ю.К. –Специальная техника, 2000.– 46–56 с.
5. Введение в компьютерную стеганографию / Хорошко В.А., Шелест М.Е. – К., 2002. – 140 с.
6. Defining Security in Steganographic Systems / Katzenbeisser S., Petitcolas F. – 2002.
7. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации / Барсуков В.С. – Специальная техника, 1999 – №6. – 51 с.
8. Исследования критерия стойкости при пассивнных атаках/Никитенко Л.Л. – Компьютерная математика, 2009 – №1 – 21 с.
9. Теория вероятностей и математическая статистика / Гихман И.И., Скороход А.В., Ядренко М.И. – Киев: Вища шк., 1979. – 408 с.
10. Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой святи / Алиев А.Т. – Ростов-на-Дону: ЦВВР, 2008.
11. Алгоритм сжатия JPEG с позиции компьютерной стеганографии / Быков С. Ф. – Защита информации. Конфидент: СПб., 2000 – № 3 – 4 с.
12. Компьютерная стеганография. Теория и практика / Конахович Г. Ф.,

Пузыренко А. Ю. – К.: МК-Пресс, 2006. – 288 с.

13. Цифровая стеганография / Грибунин В. Г., Оков И. Н., Туринцев И. В. – М.: Солон-Пресс, 2002. – 272 с

14. Keyprivacy in public-key encryption / Bellare M., Boldyreva A., Desai A., Pointcheval D. – ASIACRYPT, 2001. LCNS 2248. – 566–582p.

15. Towards foundatioms of cryptography: investigation of perfect secrecy /Jurgensen H., Robbins L. – J. of universal computer science, 1996. – 2, N 5. –347–379 p.

16. О совместной стойкости защиты информации и ключа в секретных системах /Штарьков Ю.М., Юхансон Т., Смитс Б.Д.М. – Пробл. передачи информации, 1998. – 34, вып. 2. – 117–127 с.

17. Non-malleable cryptography /Dolev D., Dwork C., Naor M. – Proc. of twenty-third annual ACM symposium on theory of computing. – New Orleans, Lousiana, 1991. –542–552 p.

18. Lecture Notes on Cryptography / Goldwasser S., Bellare M. – Cambridge, Massachusetts, 2001. – 283 p.

19. Reconciling two views of cryptography (The computational soundness of formal encryption) /Abadi M., Rogaway P. – J. of Cryptology, 2002. – 15, N 2. – 103– 127 p.

20. Analysis and design of stream ciphers. With a foreword by James L. Massey. Communications and Control Engineering Series / Rueppe R., Rainer A. – Berlin: Springer-Verlag, 1986. – 244 p.

21. Криптографические методы защиты информации. Совершенные шифры: Учеб. пос. / Зубов А.Ю. – М.: Гелиос АРВ, 2005. – 192 с.

22. Theory and application of trapdoor functions /Yao A.C. – Annual symposium on foundations of computer science. – Chicago, 1982. –80–91 p.

23. Колмогоровская сложность / Успенский В., Верещагин Н., Шень А.. – М., 2004. – 326 с.

24. Об одном классе криптографических преобразований для модели источников информации Колмогорова / Кудин А.М. – Пр. міжнар. симп.

“Питання оптимізації обчислень ПОО–XXXV”. – К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2009. – Том 1. –394–399 с.

25. Спектральні алгоритми комп’ютерної стеганографії /Задірака В.К., Мельнікова С.С., Бородавка Н.В. –Искусственный интеллект, 2002. –532 – 541с.

26. О качестве алгоритмов решения задач конструирующей стеганографии / Бородавка Н.В. – Компьютерная математика, 2003.– 109-119 с.

27. Стеганоалгоритмы на базе теоремы о свертке /Бородавка Н. В., Задирака В. К. – Кибернетика и системный аналіз, 2004. 139-144 с.

28. Аналіз стійкості стеганографічних систем в моделі пасивного противника / Задірака В. К., Кошкіна Н. В., Олексюк О. С. – Искусственный интеллект, 2004.– 801–805 с.

29. Ефективні алгоритми побудови стегоконтейнерів з використанням швидкого перетворення Фур’є / Задірака В.К., Кошкіна Н.В., Мельникова С.С. – Праці міжнар. конф. “Питання оптимізації обчислень-XXXII”. – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України, 2005. –76-78 с.

30. Применение преобразования высокой корреляции для решения задач компьютерной стеганографии / Кошкина Н. В., Шевчук Е.С. – Компьютерная математика, 2005. – 87-94 с.

31. Методичні рекомендації до виконання та захисту дипломної роботи на здобуття освітньо-кваліфікаційного рівня магістр за спеціальностями: 8.05010301 “Програмне забезпечення систем” та 8.05010302 “Інженерія програмного забезпечення” / Дивак М. П., Шпінталь М.Я., Шевчук Р.П., Козак О.Л., Пукас А.В., Спільчук В.М., Гончар Л.І. – Тернопіль : Економічна думка, 2011. – 31 с.

32. Методичні вказівки щодо проходження переддипломної практики студентами ОКР «Магістр» / Л.О. Дубчак, І.Р. Паздрій, Г.М.Мельник – Тернопіль: ТНЕУ, 2016. - 16 с.

33. Основи інформаційної безпеки в ОВС / Аполлонскій А. В., Домбровська Л. А., Прімакін А. І., Смирнова О. Г.– Підручник для вузів– СПб : Університет МВС РФ, 2010 – 10 с.

34. Основи інформаційної безпеки / Бєлов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. – Підручник для вузів – М .: Вид-во Гаряча лінія - Телеком, 2011. – 78 с.

35. Теорія захисту інформації / Малюк А. А. – М .: Вид-во Гаряча лінія - Телеком, 2012. – 49 с.

36. Основи класичної криптології. Секрети шифрів і кодів / Адаменко М. – ДМК Пресс, 2012. – 22 с.

37. Інформаційна безпека та захист інформації / Мельников В. П., Клейменов С. А., Петраков А. М. – М .: Академія, 2011. – 51 с.

38. Розслідування злочинів у сфері комп'ютерної інформації / Андрєєв Б. В., Пак П. Н., Хорст В. П. – М .: Юрлітінформ, 2001. – 66 с.

39. Захист комп'ютерної інформації / Анін Б. Ю. – СПб., 2000. – 177 с.

40. Історія криптографії. Ч.1. / Бабаш А. В., Шанкін Г. П.– М .: Геліос АРВ, 2002. – 11 с.

41. Сучасні алгоритми блокового шифрування і методи їх аналізу: навч. посібник для студентів вузів, що навчаються за спеціальністю 090103 «Організація і технологія захисту інформації» / БабенкоЛ. К., ІщуковаЕ. А. – М .: Геліос АРВ, 2006. – 90-101 с.

42. Основи технології PKI / В. С. Горбатов, О. Ю. Полянська. – М .: Гаряча лінія-Телеком, 2004. – 32-33 с.

43. Найпростіші методи шифрування тексту / Златопольский Д. М. – М .: Чисті ставки, 2007. – 11-12 с.

44. Комп'ютерна злочинність. Основи захисту комп'ютерної інформації: навчально-практичний посібник / ГерасимовВ. А., ІвановаН. В. – Міністерство внутрішніх справ Російської Федерації, Нижегородська акад. – Іжевськ, 2008. – 25 с.

45. Інформатизація та інформаційна безпека правоохоронців: XVI міжнародна наукової конференції, 22-23 травня 2007 р .: збірник праць / ред. Кірєєв В. І., Лигин Е. А. та ін. – М .: Акад. управління МВС Росії, 2007. – 15-16 с.

46. Введення в захист інформації в автоматизованих системах / Малюк А. А., Пазізін С. В., Погожину Н. С. – М .: Гаряча лінія Телеком, 2001. – 18 с.

47. Методика розслідування комп'ютерних злочинів: навчальний посібник / Махтаев М. Ш. – Російський новий університет. – М.: РосНОУ, 2007. – 21 с.

48. Інформаційна безпека та захист інформації: Навчальний посібник / МельниковВ. П., КлейменовС. А., ПетраковА. М.: під ред. КлейменоваС. А. – М .: Академія, 2007. – 36 с.

49. Злочини у сфері комп'ютерної інформації: Основи теорії і практики розслідування / Мещеряков В. А.– Воронеж, 2002. – 115 с.

50. Введення в асиметричні алгоритми шифрування: проблематика криптографії / Молдовян Н. А. – СПб .: БХВ, 2005. – 44-46 с.

51. Комп'ютерні злочини: кваліфікація, розслідування, експертиза / Нехорошев А. Б. – Саратов: Саратовський юридичний інститут МВС Росії, 2003. – 90 с.

52. Основи інформаційної безпеки: навчальний посібник для студентів вищих навчальних закладів, що навчаються за спеціальністю 351400 «Прикладна інформатика» / ГалатенкоВ. А. – Москва: Інтернет-Університет інформаційних технологій, 2008. – 11-15 с.

53. Правове забезпечення інформаційної безпеки: Учеб. посібник / Казанцев С.Я., Згадзай О. Е., Оболенський Р. М. та ін.; Під ред. С. Я. Казанцева. – М .: Академія, 2009. – 21 с.

54. Захист конфіденційної інформації / Іщейнов В. Я., Мецатунян М. В. – М .: Форум, 2009. – 78 с.

55. Правове забезпечення інформаційної безпеки: Навчальний посібник для студентів вищих навчальних закладів / КазанцевС. Я., ЗгадзайО. Е., ОболенськийР. М. та ін.; Під ред. КазанцеваС. Я.. М .: Академія, 2005. – 5-10 с.

56. Основи інформаційної безпеки: Навчальний посібник для студентів вищих навчальних закладів / Расторгуєв С. П. – М .: Академія, 2007. – 37 с.

57. Основи правового забезпечення захисту інформації: Навчальний посібник / С. Н.Сьомкін – М .: Гаряча лінія, Телеком, 2007. – 21 с.

58. Захист інформації в розподілених корпоративних мережах і системах / А. В. Соколов, В. Ф. Шаньгина. – М .: ДМК, 2002. – 54 с.

59. Захист від комп'ютерного тероризму: Справ. посібник / А. Соколов, О. Степанюк. – СПб. : БХВ-Петербург: Арліт, 2002. – 101 с.

60. Методи і засоби забезпечення безпеки інформації / Степанов П. В. – М .: Московський державний інститут електроніки і математики, 2005. – 97-98 с.

61. Тайнопис: посібник з ручного шифрування / Е. А. Лигин. – Саратов: Техно-Декор, 2007. – 3-6 с.

62. Інформаційне суспільство і комп'ютерна злочинність в Росії / С. Н. Ткаченко, Н. А. Борчева, Н. К. Кудріна. – М .: Тіссен, 2003. – 36 с.

63. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації за кордоном: Лекція / Д. А. Ястребов; під заг. ред. Л. А. Каламкарян. – М .: Прима-Прес, 2004. – 12 с.

64. Худьо В.Д. Моделювання стійкоїстеганофонічної системи із заданими характеристиками мережі / В.Д.Худьо – Сучасні комп'ютерні інформаційні технології, 2016. – 177 с.