**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРАКОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК 004.056.5:510.22(0

43.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Система виявлення та протидії кібератакам на основі стеганографії

|  |  |
| --- | --- |
| **Автор:** | Д.С. Маляренко |
| **Науковий керівник: д**.т.н., професор | С.В.Толюпа |
| **Нормоконтролер:** |  |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_» \_\_\_\_\_\_\_\_\_ 2020 р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Маляренка Дмитра Станіславовича**

1. Тема: Система виявлення та протидії кібератакам на основі стеганографії

затверджена наказом ректора від «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ № \_\_\_\_\_/ст*.*

1. Термін виконання з \_\_.\_\_.20\_\_р. по \_\_.\_\_.20\_\_р*.*
2. Вихідні дані: проаналізувати існуючі системи та методики аналізу виявлення та протидії кібератакам на основі стеганографії, Відомості про атаки на основі методів стеганографії, технології стеганографічного вбудовування SoftTempest таTCP-стеганографії
3. Зміст пояснювальної записки: стеганографія як засіб захисту інформації, методи стеганографії, які використовуються в атаках на системи,розробка засобів виявлення та протидії атакам.

**КАЛЕНДАРНИЙ ПЛАН**

| **№**  **п/п** | **Найменування етапів робіт** | **Термін виконання робіт** | **Примітка** |
| --- | --- | --- | --- |
| 1 | Уточнення виданого завдання |  |  |
| 2 | Аналіз літератури |  |  |
| 3 | Обґрунтування вибору стеганографічних методів |  |  |
| 4 | Нормативно правове забезпечення |  |  |
| 5 | Дослідження відомих прикладів реалізації атак |  |  |
| 6 | Розробка алгоритмів виявлення та протидії атак |  |  |
| 7 | Програмна реалізація методів протидії |  |  |
| 8 | Апробація роботи |  |  |
| 9 | Перевірка на антиплагіат |  |  |
| 10 | Оформлення і друк пояснювальної записки |  |  |
| 11 | Оформлення презентації |  |  |
| 12 | Отримання рецензій від рецензента |  |  |
| 13 | Захист в ЕК |  |  |

Магістрант Д. Маляренко

(підпис, дата)

Науковий керівник С. Толюпа

(підпис, дата)

**РЕФЕРАТ**

Пояснювальна записка до дипломної роботи «Система виявлення та протидії кібератакам на основі стеганографії» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 117 сторінок. Робота містить 29 рисунків, 1 таблицюта 3 додатки. Список використаних джерел включає 60 джерел.

Об’єкт дослідження – процес виявлення та протидії кібератакам на інформаційно-телекомунікаційні системи, в основі яких лежать методи стеганографії.

Мета роботи – розробка алгоритмів й засобів виявлення та протидії атакам, які проводяться із використанням методів стеганографії.

Предмет дослідження – засоби виявлення та протидії кібератакам, основаним на використанні методів стеганографії.

Метод дослідження – аналіз атак із використанням стеганографії, розробка алгоритмів, їх програмне впровадження.

Розробленіпрограмні засоби виявлення та протидії атакам.

Практичне значення роботи полягає у розробціпрограмних засобів виявлення та протидії атакам, заснованим на використанні стеганографії.

Результати здійснених у дипломній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Напрямки подальших досліджень: доопрацювання програмних засобів, створення єдиного програмного комплексу.

Ключові слова: стеганографія, ПЕМВН, TCP/IP, SoftTempest, захист інформації, ключ, зашумлення, поля заголовків.

**ЗМІСТ**

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ……………………………………………...7

ВСТУП……………………………………………………………………………....8

РОЗДІЛ 1. СТЕГАНОГРАФІЯ ЯК ЗАСІБ ЗАХИСТУ ІНФОРМАЦІЇ………...14

1.1 Основні поняття………………………………………………………....14

1.2 Поняття стеганоаналізу………………………………………………....19

1.3 Класифікація методів стеганографії……………………………………24

1.4 Популярні методи стеганографії……………………………………….26

## 1.5 Висновок до розділу ......………...……………………………………....38

РОЗДІЛ 2. МЕТОДИ СТЕГАНОГРАФІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В АТАКАХ НА СИСТЕМИ………………………………………………………….39

2.1 Особливості зорового сприйняття цифрових зображень……………..40

2.2 Особливості обробки цифрових зображень……………………………43

2.3 Побічні електромагнітні випромінювання та наведення (ТЕМПЕСТ)…………………………………………………………………..53

2.4SoftTempest………………………………………………………………..59

2.4 TCP-стеганографія……………………………………………………….71

2.5 Висновок до розділу ..…………………………………….......................76

РОЗДІЛ 3. РОЗРОБКА ЗАСОБІВ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ…..78

3.1 Розробка засобу протидії атаці із використанням Soft Tempest….......78

3.2 Розробка засобу виявлення атаки із використанням TCP-стеганографії…………………………………………………………………86

3.3 Висновок до розділу ..…………………………………………………...92

ВИСНОВКИ………………………………………………………………………...94

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ………………………………………….96

ДОДАТОК А………………………………………………………………………102

ДОДАТОК Б……………………………………………………………………….104

ДОДАТОК В ………………………………………………………………...........108

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ**

|  |  |
| --- | --- |
| АРМ | – автоматизоване робоче місце. |
| АЦП | – аналоговий цифрової перетворювач. |
| ВЧ | – високочастотний шум. |
| ГПВП | – генератор псевдовипадкової перестановки. |
| ГПВФ | – генератор псевдовипадкової функції. |
| ДКП | – дискретне косинусне перетворення. |
| ЕЦП | – електронний цифрової підпис. |
| ЗСЛ | – зорова система людини. |
| ІС та Т | – інформаційні системи та технології. |
| ІВК | – інфраструктура відкритих ключів. |
| КС | – комп’ютерна стеганографія. |
| КП | – матриця косинусного перетворення. |
| НІСТ | – Національний інститут стандартів та технологій CША. |
| НЗБ | – метод заміни найменш значущого біта. |
| НЧ | – низькочастотний (шум). |
| ПВП | – псевдовипадкова послідовність. |
| ПВСШ | – пікове відношення сигнал – шум. |
| СКВ | – середньоквадратичне відхилення. |
| УПФ | – узагальнене перетворення Фур’є. |
| ЦАП | – цифрової аналоговий перетворювач. |
| ЦВДЗ | – цифрові відеозображення. |
| ЦВЗн | – цифрові водяні знаки. |
| ЦОС | – цифрова обробка сигналів. |
| ШСС | – широкосмугові сигнали. |

# **ВСТУП**

Завдяки потужному розвитку обчислювальної техніки велика кількість медіа-інформації постійно завантажується та передається через Інтернет. Різноманітність цих носіїв призводить до труднощів у аналізі нормального та аномального вмісту, а також прогнозування поведінки, що може вимагати значних обчислювальних потужностей та складних алгоритмів.

Таким чином, із розвитком технологій отримання і обробки інформації все більше актуалізуються і проблеми інформаційної безпеки. Людство інтенсивно розвиває засоби як передавання, так і приховування інформації. Найбільш розповсюдженим механізмом захисту є використання криптографічних методів, однак їхнє застосування при транспортуванні носіїв інформації або передаванні в локальних мережах та Інтернет не завжди можливе та/або доцільне. До того ж, такий захист не вирішує проблему приховання повністю, оскільки наявність шифрованого повідомлення привертає увагу, і зловмисник, заволодівши криптографічно захищеним файлом, відразу дізнається про розміщення в ньому секретної інформації й переводить всю сумарну міць своєї комп’ютерної мережі на дешифрування даних. У таких ситуаціях досить актуальними стають стеганографічні методи приховування інформації.

Стеганографія – це наука та мистецтво зберігання й передавання секретних повідомлень прихованими каналами, які створюються всередині відкритих каналів передавання таким чином, що факт передавання секретних даних залишається невідомим для неавторизованого користувача. Методи стеганографії, враховуючи природні неточності пристроїв оцифрування та надлишковість аналогового відео- та аудіосигналу, дозволяють приховати повідомлення в комп’ютерних файлах.

За останні роки комп'ютерна стеганографія остаточно перетворилася з технічного мистецтва у наукову область дослідження і набула статусу самостійної прикладної науки, що вивчає способи і методи приховування секретних повідомлень, а також методи розкриття стеганографічних систем. Стеганографія наразі займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. При цьому обидва способи можуть бути об'єднані та використані для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів). Також дуже перспективним є використання стеганографії у тих країнах, де існують закони, що обмежують застосування криптографії, як ще одного способу обмеження доступу до даних.

У розвиток стеганографії значний внесок зробили в своїх працях такі автори, як В.О. Хорошко, Г.Ф. Конахович, М.Є. Шелест, В.К. Задірака, Н.В. Кошкіна, А.В. Аграновський, В.Г. Грібунін, Бабич І.В., Паламарчук С.А., Паламарчук Н.А., Овсянніков В.В. та інші [1, с. 5]. Питання стеганографічного приховування секретних відомостей, включаючи побудову ефективних алгоритмів приховування, свого часу розглядали в своїх роботах G.J. Simmons, J. Fridrich, R.J. Anderson, W. Bender, N. Morimoto, C. Cachin, I. Pitas та ін. [2, с. 7]. Результати досліджень стеганографічних алгоритмів на стійкість приводять в своїх працях J. Fridrich, R. Popa, N.F. Johnson, S. Voloshynovskiy [2, с. 7]. Також необхідно відзначити праці авторів B. Pfitzmann, B. Schneier і S. Craver з питань узгодження термінології та формування основних стеганографічних протоколів.

Тим не менше, збільшення доступності, складності та популярності прикладних рішень стеганографії також збільшує потенційні можливості для злочинності, серед яких наведемо промислове шпигунство або координацією між злочинними угрупуваннями. Скажімо, зображення, викладене на певному Internet‑ресурсі для загального користування, потенційно може таємно містити важливу для певних кіл інформацію і при цьому не викликати жодних підозр широкого загалу. Публікації деяких світових ЗМІ після вересневих терактів у США навіть вказували на зазначену техніку приховування як можливий засіб зв’язку між членами терористичних організацій, які планували атаки на знак протесту проти впливу Заходу на світовий устрій [2, с. 7].

Додатковим моментом є те, що методи проникнення до мережі наразі широко відомі та розроблені із урахуванням практично усіх принципів захисту систем. Одним із засобів атак є, наприклад, програми-закладки. Найскладнішими етапами за такої крадіжки інформації є встановлення шкідливого ПЗ у системі та передавання розвіданої інформації назовні. Складність зумовлена тим, що на даних етапах розвідувальна діяльність найлегше виявляється законним користувачем. При чому, чим більший обсяг інформації на передачу та розмір шкідливого файлу, тим вища ймовірність того, що нелегальну діяльність буде викрито, а засоби знешкоджено. Якраз через необхідність створення прихованого від користувача каналу витоку інформації в атаках на системи нерідко використовуються методи стеганографії.

Як видно, атаки із використанням методів стеганографії надзвичайно небезпечні, оскільки ефективно приховують як факт проведення самої атаки, так і канал виведення інформації із системи. Таке приховання даних дозволяє успішно пройти сигнатурні системи виявлення вторгнень та деяке антивірусне ПЗ.

Таким чином, усе вищезазначене зумовлює актуальність даної роботи. Результатом невпинного розвитку науки та техніки, у тому числі інформаційних технологій, є постійне ускладнення як засобів атак на інформаційно-телекомунікаційні системи, так і їх захисту, при чому рівень складності зростає із прискоренням. Наразі, одним із найпотужніших та найбільш широко застосовуваних механізмів захисту є криптографія, метою якої є блокування несанкціонованого доступу до інформації шляхом шифрування змісту секретних повідомлень. Тим не менше, криптографічний захист інформації не вирішує проблему приховання повідомлення повною мірою. Механізм, метою застосування якого є приховання власне факту наявності секретного повідомлення, має назву стеганографія. Увага акцентується головним чином на дослідженні алгоритмів вбудовування повідомлень та пошуку нових контейнерів для них. В останні роки було проведено низку досліджень, які продемонстрували, що методи стеганографії можуть використовуватися не тільки для захисту інформації, а й в якості бази для атак на системи. Особлива небезпека таких атак полягає, в першу чергу, у прихованні каналу, яким здійснюється атака. Тим не менше, даному факту увага дослідників майже не приділяється. Не існує ні математичної моделі для стеганографічних алгоритмів в атаках на системи, ні реалізованих засобів із прийнятним рівнем захисту. Практична потреба в механізмах захисту від таких атак полягає в їх специфічному характері, а саме використанні методів стеганографії, які класично розглядаються у якості засобів захисту, а не навпаки. До того ж, не існує запропонованих способів виявлення таких атак.

Таким чином, розробка засобів виявлення та протидії атакам, основаним на методах стеганографії, є актуальним питанням у сфері захисту інформації.

Мета дипломної роботи «Система виявлення та протидії кібератакам на основі стеганографії» полягає у розробці алгоритмів та засобів виявлення та протидії атакам, які проводяться із використанням методів стеганографії.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

* провести аналітичний огляд відомих методів стеганографії, проаналізувати теоретичну базу систем, в яких вони реалізовані;
* аналітично проаналізувати атаку, що базується на використанні технології «SoftTempest» та наявні методи протидії;
* аналітично проаналізувати атаку, в основі якої лежить TCP-стеганографія, а також наявні методи протидії;
* формалізувати вимоги до алгоритмів виявлення вищезазначених атак та засобів протидії ним;
* розробити методи виявлення факту проведення вищезазначених атак на систему;
* обґрунтувати та запропонувати методи захисту систем та інформації у них від вищезазначених атак;
* виконати програмну реалізацію даних методів у формі програмних рішень.

Об’єкт дослідження – процес виявлення та протидії кібератакам на інформаційно-телекомунікаційні системи, в основі яких лежать методи стеганографії.

Предмет дослідження – засоби виявлення та протидії кібератакам, основаним на використанні методів стеганографії.

Практична цінність кваліфікаційної роботи полягає в наступному:

* дослідження характеристик вищезазначених атак з позицій теорії стеганографії, що дозволило навести адекватну модель таких атак та оцінити необхідні параметри;
* розробці алгоритмів виявлення атак, в основі яких лежать технології SoftTempest та TCP-стеганографії;
* розробці методів захисту від вищезазначених атак;
* реалізації даних методів та алгоритмів у вигляді програмних рішень (скриптів для ОС Linuxта програми на мові програмування C);
* розробці програмних засобів для проведення експериментального тестування запропонованих рішень.

Оскільки успіх роботи механізмів безпеки реальної системи багато в чому залежить від індивідуальних особливостей її побудови, а також від умов її експлуатації, жоден із існуючих традиційних методів захисту не можна назвати універсальним.

З точки зору витоку інформації особливу небезпеку становлять побічні електромагнітні випромінювання і наведення (ПЕМВН) засобів обчислювальної техніки (ЗОТ), що беруть участь в процесі передачі, обробки та зберігання конфіденційної інформації. Серед таких ЗОТ можна назвати монітори персональних електронно-обчислювальних машин (ПЕОМ), клавіатури, принтери, провідні лінії зв'язку, фактично будь-які елементи комп’ютерів.

До того ж, постійно зростаючий рівень складності обчислювальної техніки, інформаційних і телекомунікаційних технологій призвів до створення всесвітнього єдиного інформаційного простору, в якому для зберігання, обробки і передавання інформації використовуються ресурси загальнодоступних комп'ютерних мереж, найбільш яскраво представлених глобальною «павутиною» Інтернет. Завдяки мережі Інтернет у всесвітньому інформаційному просторі з'явилася потенційна можливість доступу як до об'єктів обробки і зберігання інформації, так і до процесів її передачі практично з будь-якої точки земної кулі. З одного боку, очевидно, що це велике благо як для людства в цілому, так і для кожного індивідуума окремо. З іншого боку, широкі можливості Інтернету можуть бути також використані для здійснення неправомірної діяльності і кіберзлочинцями, і продавцями наркотиків, і фінансовими аферистами, не кажучи вже про шпигунів та терористів.

Враховуючи сказане, для дослідження було обрано дві технології, які складають методи стеганографії, що використовуються не тільки для захисту інформації, а й для організації кібератак на системи, а саме технологію Soft Tempest та TCP-стеганографію.

У роботі пропонуються рішення, які б забезпечували виявлення та протидію вищезазначеним атакам.

Апробація результатів роботи та публікації.

Anna Romanova, Sergiy Toliupa. Dmitry Malyarenko steganographyas a means of attacking information systems. Матеріали ІІ міжнародної науково-практичної конференції “Проблеми кібербезпеки інформаційно- телекомунікаційних систем” (PCSIТS). – Київ. - 2019. – с. 122-123.

Toliupa S., NakonechnyiV., Romanova A.,Dmitry Malyarenko.Steganographyand cibernetic space. Науково-практична конференція. «Кібербезпекау системі національної безпеки України: проблеми та перспективи розвитку». Маріуполь. 2019. – с. 78-79.

# Толюпа С., Єсипенко О., Маляренко Д. Застосування математичної теорії ігор при побудові систем управління інформаційною безпекою. Матеріали допо-відей. VІ Міжнародна науково-практична конференція «Інформаційні технології та взаємодії» (IT&I 2019). – с. 313-317.

# **РОЗДІЛ 1.** **СТЕГАНОГРАФІЯ ЯК ЗАСІБ ЗАХИСТУ ІНФОРМАЦІЇ**

Як вже було згадано вище, криптографічний захист інформації не вирішує проблему приховання повідомлення повною мірою. Задача приховання навіть факту наявності каналу передавання вирішується методами стеганографії.

Незважаючи на численні відкриті публікації та щорічні конференції, тривалий час стеганографія не мала усталеної термінології [2, с. 7]. З середини 80-х р.р. минулого століття для опису моделі стеганографічної системи використовувалася так звана “проблема ув’язнених”, яку запро­понував у 1983 р. G.J. Simmons. Основні поняття стеганографії були узгоджені у 1996 р. на 1-й Міжнародній конференції з приховування даних – InformationWorkshoponInformationHiding’96 [2, с. 7]. Тим не менш навіть таке першоутворююче поняття як “стеганографія” різними спеціалістами трактується неоднаково. Наприклад, деякі фахівці розуміють під стеганографією лише приховану передачу інформації. Інші ж відносять до неї такі додатки як, наприклад, метеорний радіозв’язок, радіозв’язок із псевдовипадковим перестроюванням частоти, широкосмуговий радіозв’язок.

Перша конференція, присвячена стеганографії, відбулася в липні 2002 р [5, с. 12]. Наразі існує велика кількість прикладів програмної реалізації відомих алгоритмів, проте очевидна недостача саме програм початкового рівня, які б наочно, крок за кроком демонстрували весь процес стеганографічного перетворення, що можна було б використовувати в навчальному процесі при підготовці фахівців у сфері захисту інформації.

## **1.1. Основні поняття**

В одній зі своїх семінарських робіт із систем забезпечення секретності Шеннон заявив, що системи приховування інформації є «насамперед психологічною проблемою» [6, с. 4].

Змоделюємо один із варіантів проблеми двох в’язнів. Аліса і Боб намагаються обмінюватися повідомленнями, які постійно перехоплюються начальником в'язниці Венді. Якщо Венді вважає повідомлення, яким обмінюються Аліса та Боб, підозрілим, вона перерве їхнє спілкування. Наведена вище модель застосовується в реальності, наприклад, в умовах деспотичних режимів або урядових політик, які виключають використання криптографії в межах певної країни. Таким чином, прагнення до конфіденційності між двома сторонами створює потребу у схемах приховування інформації таким чином, що спостерігач не зможе розрізнити секретне повідомлення, передане між сторонами, та звичайне повідомленням (частину їхньої розмови)[6, с. 4]. У цьому і полягає базова проблема класичної стеганографії.

Стеганографія – це наука та мистецтво зберігання й передавання секретних повідомлень прихованими каналами, які створюються всередині відкритих каналів передавання таким чином, що факт передавання секретних даних залишається невідомим для неавторизованого користувача [7, с. 17]. Загальні підходи:

* Повне приховання каналу передавання;
* Ускладнення виявлення, отримання та модифікації повідомлень, прихованих всередині відкритих даних;
* Маскування секретних повідомлень, використовуючи протоколи.

Методи цифрової та комп'ютерної стеганографії стали потужним засобом вирішення задач зі створення різних систем контролю над дотриманням авторських прав на ринку цифрової фото-, аудіо-, відеопродукції та при розповсюдженні програмних продуктів (водяні знаки, підписи, захист від підробки, вставка заголовків в оцифровані аналогові сигнали тощо). Останній факт є серйозним стимулом для фінансування досліджень в цій області з боку великих виробників та некомерційних організацій. Зокрема, WatermarkingWorld [WatermarkingWorld 01] є міжнародною асамблеєю фахівців зі стеганографії, які розробляють системи вбудовування цифрових водяних знаків [8, с. 22]. Використання методів стеганографії особливо доцільно в тих країнах, де заборонено застосовувати криптографічні засоби.

Основними поняттями стеганографії є:

* Контейнер b (container, carrier) – відкриті дані, які використовуються для приховання секретної інформації/в які вбудовується секретне повідомлення;
* Повідомлення m(message, payload) – секретне повідомлення, яке необхідно приховати;
* Ключ k(key) – секретна інформація, що відома тільки авторизованому користувачу та визначає конкретний алгоритм вбудовування;
* Пустий контейнер c (emptycontainer, unmodifiedcontainer) – контейнер, що не містить секретнийх даних; являє собою послідовність елементів довжини lc;
* Модифікований контейнер або стеганограма s (modifiedcontainer, package, steganogram) – контейнер, який містить секретне повідомлення;
* Стеганографічний алгоритм являє собою два перетворення, пряме (EK: Mx С xK → B) та зворотнє (DK: С xK → M) [7, с. 17];
* Стеганографічна система або стеганосистема (steganographicsystem, steganosystem) – сукупність повідомлень, секретних ключів, контейнерів та перетворень, що їх об’єднують: Ψ = (C, M, K, DK, EK), де C є сукупністю усіх контейнерів, M та K – повідомлень та ключів відповідно, так що DK(EK(c, m, k), k) = m[6, с. 4].
* Пакування повідомлення до контейнера відбувається за допомогою стеганокодера;
* Стеганографічний канал – канал передачі контейнера-результату;
* В cтеганодетекторі здійснюється визначення наявності в контейнері (можливо вже зміненому) прихованих даних. Ця зміна може бути обумовлена впливом помилок в каналі зв’язку, операцій обробки сигналу, навмисних атак порушників. В багатьох моделях стеганосистем сигнал-контейнер розглядається як адитивний шум. Тоді задача виявлення і виділення стеганоповідомлення є класичною для теорії зв’язку. Але такий підхід не враховує двох факторів: невипадкового характеру контейнера і вимог по збереженню його якості.

На рис.1.1 представлено блок-схему, яка представляє основні компоненти стеганосистеми та їх взаємодію. Варто зауважити, що дана блок-схема бере до уваги тільки сценарій із пасивним порушником (Венді не може модифікувати повідомлення, тільки дозволити чи заборонити його передавання; порушник, який вносить зміни у канал, контейнер чи повідомлення, називається активним). У більшості випадків, необхідним вважається одночасне виконання умов приховування даних при пасивній та активній протидії [9, с. 3].

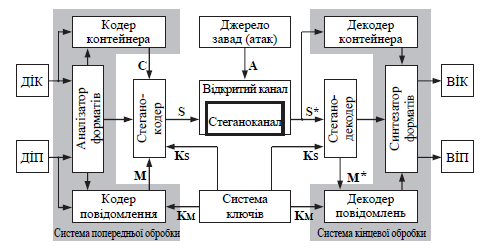


Рис.1.1. Компоненти типової стеганосистеми та їх взаємодія [6, с. 4]

На рис. 1.1 сигнал з виходу джерела інформації-контейнера (ДİК),який повинен бути відкритим чином переданий системою зв’язку іпопередньо може мати певний формат, надходить на входи аналізатораформатів (АФ) і кодера контейнера у системі попередньої обробки(СПО). Крім цього на входи АФ і кодера повідомлення СПО подаєтьсясигнал з виходу джерела інформації-повідомлення (ДİП), який такожможе мати довільний формат. Встановивши структуру інформації насвоїх входах, АФ видає керувальні сигнали на входи відповіднихджерелам кодерів стосовно наявності або відсутності потреби узастосуванні операцій додаткового кодування (перекодування). Прицьому до задач кодерів контейнера і повідомлення входить забезпечення сумісності форматів даних ДİК та ДİП із засобами подальшоїцифрової обробки у стеганокодері, за допомогою якого здійснюєтьсявбудовування повідомлення **M** до контейнера **C**.

Стеганогрфія використовує контейнери різної природи; вибір залежить від конкретного завдання. Можна вирізнити поняття комп’ютерної стеганографії – розділу стеганографії, який займається питаннями реалізації стеганосистем із використанням комп’ютерної техніки [10, с. 11]. Оскільки цифрова інформація передається у вигляді файлів, то елементами стеганосистеми будуть, відповідно, файл-контейнер та файл-повідомлення. При цьому, за загальним принципом файл-контейнер не повинен викликати підозри, а додавання секретної інформації не повинно змінювати його основні властивості [10, с. 11].

Якщо у якості контейнера використовуюється аудіо-файл, то довжина елементів визначатиметься кількістю відрахунків за одиницю часу. Якщо ж контейнером виступає, наприклад, цифрове зображення, тоді послідовність елементів можна отримати за допомогою векторизації зображення (перетворення масиву пікселів на вектор).

Більшість методів стеганографії основані на двох ключових принципах:

* Людські органи чуттів не можуть рорізнити незначні зміни при сприйнятті кольору, форми та звуку;
* Як наслідок, існують файли, для яких абсолюна точність не обов’язкова, тобто, їх можна модифікувати без втрати їх функціонального значення.

Таким чином, зазначені методи передбачають виявлення незначущих фрагментів контейнера та заміщення інформації всередині них інформацією, яку необхідно приховати.

Стеганографічні системи можуть бути ключовими та безключовими. У даному питанні полягає найбільша прогалина у теорії стеганографії. Якщо мова йде про ключові системи, то за аналогією із криптографією існують стеганографія із відкритим та закритим ключем (secretkeysteganography, publickeysteganography), при чому у першому випадку модель не розглядає, яким чином відбувається обмін секретним ключем (найчастіше використовуються ті самі підходи, що і в криптографії). Проте, як було зазначено, існують безключові системи (так звані системи чистої стеганографії) [6, с. 4]. Повторимо, що базовою проблемою класичної стеганографії є передавання повідомлення так, що у третьої сторони навіть не виникне підозри щодо наявності прихованого каналу передавання. Таким чином, питання ключа (секретного чи відкритого) тут і не стоїть. Отже, безключові системи більшою мірою відповідають теоретичній основі. Проте, фактично, ефективність «чистої» стеганосистеми залежить тільки від секретності двох функцій (вбудовування та виділення стеганограми, описані вище як алгоритми), що суперечить принципу Кірхгоффса – безпека системи повинна залежати тільки від секретності ключа, а не алгоритма.

В жодній розглянутій роботі не запропоновано єдиного теоретичного підґрунтя, яке б визначило базовий принцип для секретності стеганографічних систем (місце принципу Кірхгоффса у стеганографії або його аналог, що повною мірою забзпечує теоретичний апарат). З цього витікає, що розрахунок рівня секретності (та ефективності) стеганографічних алгоритмів та систем залишається відкритим питанням, оскільки усі існуючі метрики не враховують повний спектр проблем, що з ним пов’язані.

Якщо розглядати ключові стеганосистеми, то математичний апарат значною мірою подібний до теорії криптографічних систем.

## **Поняття стеганоаналізу**

Процес виявлення та вилучення вбудованої стеганограми носить назву стеганоаналізу. Він існує у двох видах – статичному та динамічному [11, с. 2]. Метою статичного стеганоаналізу є визначення існування/неіснування прихованого повідомлення та розпізнавання алгоритму вбудовування, динамічного – прийняття гіпотези по параметр(и) алгоритму вбдовування або секретного повідомлення (здогадка про довжину, позиції вбудованого повідомлення, ключ тощо).



Рис. 1.2. Взаємозв’язок між стійкістю стегано­системи та об’ємом приховуваного повідомлення при незмінному розмірі файлу – контейнера [2, с. 7]

Щодо загальної стійкості стеганографічних систем, можна вирізнити такі типи [2, с. 7]:

* Теоретично стійка (абсолютно надійна) cтеганосистема здійснює приховування ін­формації лише в тих фрагментах контейнера, значення елементів яких не перевищують рівень шумів або помилок квантування, і при цьому теоретично доведено, що неможливо створити стеганоаналітичний метод виявлення прихованої інформації;
* Практично стійка cтеганосистема передбачає таку модифікацію фрагментів контей­нера, зміни яких можуть бути виявлені, але відомо, що на даний момент необхідні стегано­аналітичні методи в порушника відсутні або поки що не розроблені;
* Нестійка cтеганосистема приховує інформацію таким чином, що існуючі стегано­аналітичні засоби дозво­ляють її виявити.

Також, враховуючи можливі атаки (компресія із втратою даних, атака на руйнування повідомлення, атака на основі відомого чи обраного контейнера (оригіналу чи результату), на основі відомого вбудованого повідомлення тощо), можна виділити стеганографічні системи, стійкі до пасивних та активних атак. Щодо пасивних атак, означимо поняття абсолютно стійкої стеганосистеми [6, с. 4]:

Нехай PC – ймовірність розподілу контейнерів, а PS – імовірність формування стеганограми E(c, m, k) на множині S всіх можливих стеганограм, отриманих за допомогою стеганосистеми. Зауважимо, що неавторизована особа не повинна мати доступ до набору контейнерів, що використовуються для секретного зв’язку. Тоді відносна ентропія на множині Q може бути визначена наступним чином:

, (1.1)

де P0 та P1 – ймовірності прийняття вірної та хибної гіпотези про розподіл відповідно. Відносна ентропія між двома розподілами завжди є невід’ємною і дорівнює 0 лише у випадку тотожності даних розподілів.

Означення. Нехай Σ – стеганографічна система; PS – розподіл імовірностей пере­дачі каналом зв’язку стеганограм; PC – розподіл імовірностей передачі каналом зв’язку пустих контейнерів. Система Σ називається ρ-надійною до пасивних атак, якщо ≤ ρ, і є абсолютно надійною, якщо ρ = 0. Як вже зазначалося, співвідношення дорівнює нулеві тільки у тому випадку, коли обидва розподіли імовірностей є рівними один одному. Отже, cтеганосистема Σ є тео­ретично абсолютно надійною, якщо процес вбудовування секретного повідомлення до контей­неру не змінює розподіл PC[6, с. 4].

Абсолютно безпечна система може бути створена, наприклад, на основі одноразової гамми [2, с. 7].

Вище було визначено P0 та P1, які відповідають гіпотезам:

* Н0 – повідомлення не містить секретних даних;
* Н1 – у повідомленні приховано секретні дані.

З точки зору можливих дій Венді, хибним позитивним є рішення Венді заблокувати передавання звичайного повідомлення. Хибним негативним, відповідно, є рішення дозволити передавання прихованого повідомлення.

Основною метрикою для оцінки якості стеганосистеми є ефективність вбудовування: чим вона вища, тим більше одиниць інформації можна вбудувати у контейнер, не викликаючи значних спотворень початкової послідовності, що, у свою чергу, знижує ймовірність виявлення каналу передавання атакуючою стороною.

Пропускна здатність стеганоканалу є ще однією з найважливіших метрик; під нею розуміють відношення розміру контейнера до розміру повідомлення, для систем прихованої передачі даних повинна бути суттєво вищою, ніж для інших видів систем.

Ще одним важливим показником останнім часом стала вважатися робастність (Robustness) – міра можливості при використанні алгоритма зберегти вбудовані дані навіть після того, як контейнер було піддано компресії та декомпресії із втратами або іншим змінам, як-от перетворенню на аналоговий сигнал та назад у цифровий [8, с. 22].

Найбільшим недоліком відомих показників спотворення як для графічних, так і для аудіо- та відео-контейнерів, є відсутність відповдності органам чуття людини. Розробка нових методів, а також встановлення кореляції реальних показників із теоретичними, все ще залишаються важливими напрямками подальшого розвитку стеганографії. Наразі, одним із запропонованих рішень є показник спотворення J.E. Farrell та C.J. van den Branden Lambrecht[2, с. 7].

Ступінь сприйманої людиною якості оперує чутливістю до контрасту та явищем маскування системою візуалізації людини і базується на багато­канальній моделі людського просторового зору. Обчислення даного показника полягає в: проведенні великокрокової сег­ментації зображення; розкладанні помилки кодування і первинного зображення на перцепційні (такі що відносяться до сприйняття органами відчуттів) компоненти, використовуючи гребін­часті фільтри; обчисленні порогу виявлення для кожного пікселя, використовуючи первинне зображення як маску; розподіленні фільтрованої помилки за допомогою порогу прийняття рішення, об’єднанні по всім колірним каналам. Одиниця вимірювання показника визначається як одиниця перевищення порогу, що розуміє під собою тільки значиму (помітну) відмінність (JustNoticeableDifference – JND). Загальний показник, приховане максимальне відно­шення сигнал/шум (MaskedPeakSignaltoNoiseRatio – MPSNR):

                          (1.2)

де ε – обчислене спотворення. Оскільки даний показник якості не відповідає смислу, який закладено у поняття децибел, його називають візуальним або зоровим децибелом (ВдБ).

У випадку протидії активним атакам, існує два підходи до створення стійких стеганосистем [2, с. 7]:

1) передбачаючи можливі атаки на стеганограми з боку порушників, cтегано­графічне перетворення відразу проектується стійким до знищення прихованих даних певним класом модифікацій;

2) реалізуються перетворення, які мають властивість оберненості до можливих моди­фікацій з метою відновлення початкового вигляду стеганограми. При цьому передбачається оцінка параметрів перетворень, вимірювання змін форми, розмірів і напрямків деяких кодованих образів.

Небезпечною та специфічною для даного виду стеганосистем є атака змовою (коаліцією): декілька користувачів, кожен з яких отримав свій екземпляр контейнера з вкрапленим у нього унікальним ідентифікаційним номером, стають порушниками та, погоджено діючи, намагаються побудувати досить близьку до оригіналу оцінку пустого контейнера, що зберігає його функціональність, але не містить ідентифікаційної інформації. На практиці це актуально, наприклад, для задач захисту авторських прав та прав власності на CD/DVDдиски з музикою чи фільмами і т.п.

На рис. 1.3 [8, с. 22] наведено схему конфлікту між характеристиками стеганографічної системи.

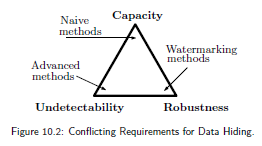


Рис. 1.3. Конфлікт між значеннями характеристики

стеганографічних систем

У [12, с. 6] запропоновано варіант реалізації програмного комплексу на мові C#, який дозволяє проводити аналіз відомих методів вбудовування у цифрові зображення із різними параметрами, при чому зображення стають об’єктом різноманітних атак з варіативними ступенями спотворення. Таким чином, стає можливою практична оцінка стійкості стеганографічних систем.

Беззаперечно, стеганографічні рішення викликають практичний інтерес. Вони можуть використовуватися в якості альтернативи криптографічним засобам приховування інформації, у деяких випадках більш ефективно. Крім того, вони служать потужною базою для створення цифрових і нецифрових водяних знаків, а також для контролю автентичності. Нарешті, в той час як використання криптосистем юридично регулюється та певною мірою обмежується, у жодній країні подібних обмежень щодо проектування та розповсюдження стеганосистем не існує [7, с. 17].

## **1.3.Класифікація методів стеганографії**

За способом вибору контейнера можна виділити безальтернативні, селективні та конструктивні стеганографічні методи [2, с. 7].

Безальтренативні методи передбачають вибір першого можливого контейнера, щоб приховати повідомлення. Селективні методи передбачають, що приховане повідомлення повинно відтворювати певні статистичні характеристики шуму контейнера. У конструктивних методах контейнер генерується власне стеганосистемою.

За типом доступу до секретних даних існують методи для потокових і фіксованих контейнерів.

Потокові контейнери – це послідовність бітів, яка постійно змінюється. Повідомлення вбудовується у нього в реальному режимі часу, тому заздалегідь невідомо, чи вистачить розміру даного контейнера для передачі повідомлення повністю. Фіксовані ж контейнери мають фіксований розмір, тому є можливість обрати оптимальний контейнер для передачі повідомлення [13, с. 8].

За типом організації існують методи систематичних і несистематичних контейнерів. У перших можна виділити біти шуму та самого контейнера. Для других така операція неможлива.

За принципом приховування існують два основні класи: методи прямого заміщення та спектральні методи. Перші використовують надмірність контейнерів і замінюють незначимі ділянки контейнера бітами секретного повідомлення, тоді як другі приховують дані, використовуючи спектральне представлення елементів у середовищі, в якому вбудовано приховані дані (наприклад, коефіцієнти масивів перетворень Фур'є).

За призначенням можна розрізняти методи прихованої передачі або зберігання даних і способи приховування даних у цифрових об'єктах у сфері захисту авторського права.

За ще однією класифікацією стеганографію можна поділити на нестійку (fragile; при зміні контейнера вбудовану інформацію буде знищено) та стійку/робастну (robust; захищеність від знищення через модифікацї) [14, с. 3].

Специфічну групу складають методи, які використовують властивості форматів файлів:

* Зарезервовані поля, що зазвичай заповнені нулями та не беруться до уваги програмою
* Спеціальне форматування даних (зміщення слів, речень, параграфів, або вибір конкретних позицій для символів);
* Видалення заголовків ідентифікаторів тощо [2, с. 7].

## **1.4.Популярні методи стеганографії**

Далі наведені найбільш широко використовувані підходи до реалізації стеганографічних алгоритмів.

В основному, стеганографія використовує приховування даних у цифрових зображеннях та аудіофайлах, меншою мірою – у відеофайлах та тексті, хоча відомі випадки використання і нецифрових контейнерів. Електронні системи зв’язку можуть також включати в себе приховування даних на транспортному рівні (всередині програми або протоколу). Такий канал значно спрощує передавання даних, оскільки його параметри та структура залишаються незмінними після вбудовування секретного повідомлення. Цифрові мультимедійні файли надзвичайно придатні для виконання задач стеганографії, в першу чергу завдяки їх великим розмірам. Незначні зміни в їхній структурі навряд чи будуть помічені неінформованим стороннім користувачем.

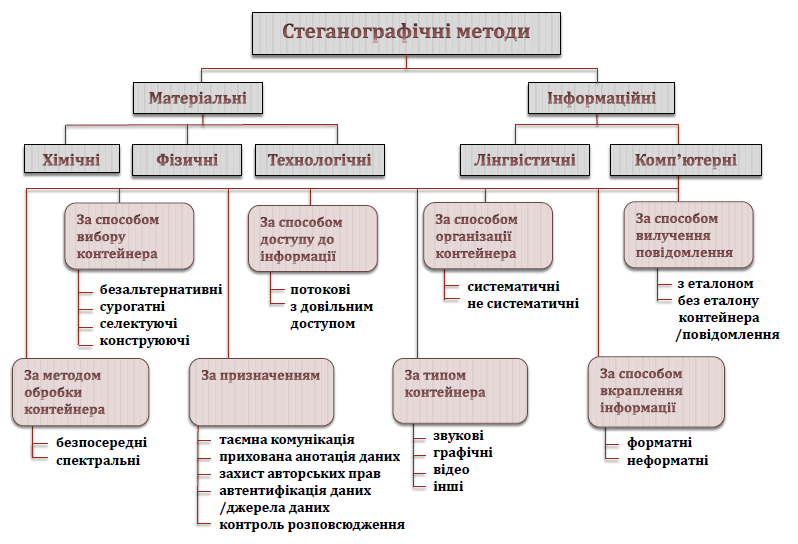


Рис. 1.4 – Класифікація методів стеганографії [13, с. 8]

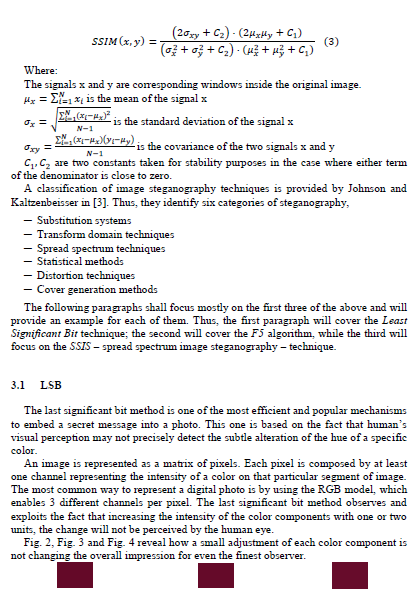
Однак, розпочиналося використання стеганограм, очевидно, не з цифрових контейнерів, тож не варто забувати про техніку фізичної стеганографії. Вона існує вже століття і включає найрізноманітніші прийоми, як-от відомий випадок, коли військовополонені під час відеозвернення кліпали очима азбукою Морзе, таким чином передаючи таємне послання своїм [7, с. 17].

Іншим прикладом є додавання крихітних жовтих точок на кожну сторінку друкованого документа. Їх не розрізнити незброєним оком, а всередині таких точок міститься інформації про модель, серійний номер та мітки часу друкуючого пристрою. Ця інформація не може бути отримана з цифрового файлу та вбудовується до роздрукованого матеріалу із використанням матричного коду. Таку технологію використовують чимало виробників кольорових лазерних принтерів, такі як Xerox і Hewlett-Packard, задля забезпечення відстежуваності продукції [7, с. 17].

У [14, с. 3] наведена таблиця порівняння груп стеганографіних методів за основними параметрами.

Методи вбудовування даних у зображення в якості контейнера [2, 15]:

* Метод найменш значимого біта (LSB) (послідовне вбудовування) є найбільш популярним стеганографічним методом. Найменш значущий біт кожного пікселя є фактично шумом. Якщо його змінити, людське око не розрізниь зміну. Таким чином, ці біти можуть бути замінені бітами секретного повідомлення. На Рис. 1.5 [6, с. 4] представлено, як незначні зміни, внесені до компонент кольорів, недостатні для зміни сприйняття зображення спостерігачем.



а)б)в)

Рис. 1.5 – Застосування методу найменш значимого біта: а) R = 100, G = 10, B = 40; б) R = 101, G = 11, B = 41; в) R = 103, G = 13, B = 43

Інший приклад, наведений у [6, с. 4] – QR-код, вбудований у зображення (Рис. 1.6)

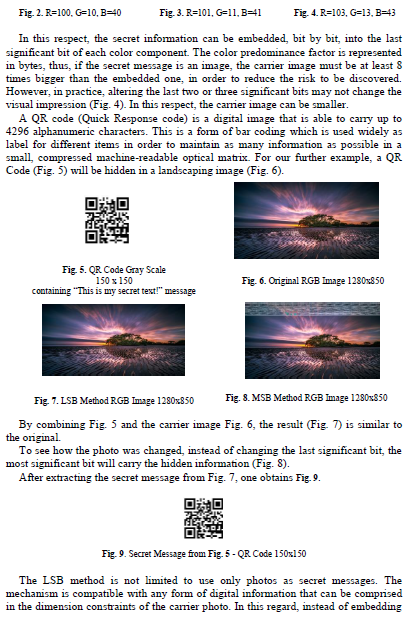


Рис. 1.6.Метод LSB у зображенні

Проблема методу LSB яскраво виражена при розгляді Лаплас-фільтрованого зображення. Розподіл: . Функція розподілу пустого контейнера швидко зростає та спадає навколо 0. На Рис. 1.7 [6, с. 4] помітно, як графіки розподілу заповнених контейнерів маю нижчий максимум функції та повільніші зростання та спадання на фронтах.

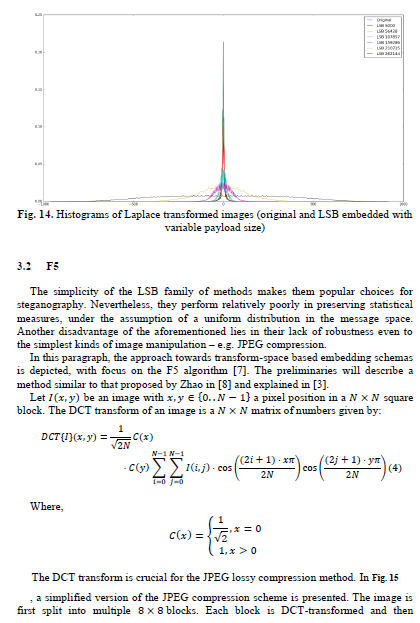


Рис. 1.7. Гістограма Лаплас-фільтрованого зображення

* Псеводвипадкове вбудовування LSB. На відміну від попереднього способу, в якому кожен змінений біт даних йде за попереднім, цей метод використовує псевдо випадковий розподіл бітів секретного повідомлення контейнером. Таким чином, інтервал між двома бітами визначається псевдовипадково, що ускладнює як візуальні, так і статистичні атаки, а також вилучення всіх прихованих бітів.
* Псеводвипадкова перестановка LSB. Не тільки найменш значущі біти вибираються псевдовипадковим чином, але і біти секретного повідомлення рівномірно розподіляються по контейнеру згідно з псевдовипадковою послідовностю.
* Метод блокового вбудовування. Контейнер розбивається на непересічні блоки; для кожного з них обчислюється біт парності. Один секретний біт прихований в одному блоці. Якщо біт парності не дорівнює відповідному секретному біту, то один з LSB в блоці інвертується, так що парність і секретні біти є однаковими.
* Перестановка палітри. Будь-яка палітра складається з пар індексів. Кожен піксель зображення відповідає певному індексу в таблиці. Послідовність кольорів у палітрі не важлива, тому можна приховати повідомлення, змінюючи цю послідовність.
* Квантування зображень. Міжпіксельна кореляція може бути визначена функцією Θ. Можна розрахувати різницю εI між сусідніми пікселями ci та ci + 1 (або ci-1 та ci) і встановити її як параметр функції: Δi = Θ(сi – сi+1), де ΔI є дискретним наближенням різниці сигналів ci - ci + 1. Оскільки ΔI є цілим числом, а різниця ci - ci + 1 – дійсним, то виникають помилки квантування δi = Δi – εi. Приховування інформаії здійснюється шляхом корекції сигнала різниці Δi.
* Метод Куттера-Джордана-Боссена. Людське око найменш чутливе до синього кольору. Метод оснований на вбудованні секретного повідомлення в синій канал.
* Метод Коха-Джао (відносний DCT (дискретне косинусне перетворення)). Початкове зображення розбивається на блоки розміром 8x8 пікселів. В результаті застосування DCT до кожного блоку формується таблиця DCT коефіцієнтів. Використовуються три пари коефіцієнтів для блоку, перетвореного за допомогою ДКП:

якщо

та , кодує 1

якщо

та , кодує 0,  
де – коефіцієнти квантування. Тобто, Аліса повинна змінити значення відповідних коефіцієнтів. При цьому зміни, які вимагає блок, не повинні перевищувати певного порогу, аби Венді не змогла помітити спотворення, спричинені алгоритмом. Кожен секретний біт прихований в окремому блоці. Частота квантування дещо спотворює зображення, але ці зміни все ще не розрізнити людським оком.

* F5 – метод, який враховує недоліки LSB [1, 6] (низька стійкість до атак, основаних на проведенні статистичних досліджень контейнера). Подібний до методу Коха-Джао, проте значно модернізований з метою підвищення стійкості до атак на основі статистичних вимірювань, в тому числі χ2-атак. Зображення спершу розбивається на блоки 8х8. Кожен блок підлягає дискретному косинусному перетворенню (ДКП), після чого він квантується за допомогою деякої таблиці квантування. Останнім кроком є стиснення без втрат (відомі методи – RunLengthEncoding, EntropyEncoding тощо [6, с. 4]).
* Метод Бенгама-Мемона-Ео-Юнг (Benham-Memon-Yeo-Yeung). Оптимізована версія попереднього методу. По-перше, використовуються лише найбільш пристосовані до цього блоки. По-друге, замість двох обираються три коефіцієнта DCT, що дозволяє знизити спотворення в контейнері.
* Метод Хсу-Ву (Hsu-Wu) – алгоритм вбудовування двійкових цифрових водяних знаків. Пікселі можуть приймати значення тільки "0" або "1", тому безпосереднє спостереження такого зображення неможливе, оскільки інтенсивності "0" і "1" відповідають чорному кольору. Водяний знак може бути створений чорно-білим, а потім весь масив можна розділити на 255, щоб замінити інтенсивність білих пікселів на «1».
* Метод Фрідріх (Fridrich) передбачає каскадне вбудовування в низько- і високочастотні DCT коефіцієнти.
* метод Дармстедтера-Делейгла-Квісквотера-Макка (V. Darmstaedter, J.-F. Delaigle, J.J. Quisquater та B. Macq) – блоковий метод вбудовування у просторову область контейнера, який базується на елементарному пер­цептуальному (відчуттєвому) сприйнятті і дозволяє пристосовувати вбудовування відносно поточного вмісту блоків; виділяються зони з приблизно однорідними значеннями яскравості, після чого вони ділять на категорії у відповідності до індивідуальної (псевдовипадкової) маски; вбудовування біту відбувається в залежності від співвідношення між середніми значеннями кате­горій кожної зони шляхом модифікації значень яскравості кожної категорії в кожній зоні [2, с. 7];
* метод шаблонного вбудовування даних на основі матричного представлення кодів Хеммінга та метод, в основі якого лежить вейвлет-перетворення [1, с. 5];
* Широковмуговий метод (spread-spectrum) передбачає три варіанти:
  + Реальна ширина смуга набагато більша, ніж це необхідно. Відношення сигнал/шум (SNR) достатньо низьке, через що виявлення сигналу малоймовірне;
  + Спектр розширюється із використанням спеціального незалежного (кодового) сигналу. Енергія сигналу рівномірно роподілється по всій полосі частот, що дозволяє зробити сигнал стійким до шуму;
  + Відновлення початкової інформації відбувається шляхом порівняння отриманого сигналу та синхронізованої копії кодового сигналу.

Відновлення початкової інформації (тобто “звуження спектру”) здійснюється шля­хом співставлення одержаного сигналу та синхронізо­ваної копії кодового сигналу.

* Вбудовування зображень у відео-файли [13, 15] (використовується найрідше, оскільки оскільки даний файл складається з динамічних зображень (фреймів) та звукової доріжки; для цих цілей найчастіше використовуються контейнери у форматах MPEG – 2, MPEG– 4 та AVI. Варто такожзазначити, що досі не використовуються як контейнери одночасно аудіодоріжки тафрейми):
  + метод вбудовування на рівні коефіцієнтів;
  + метод вбудовування на рівні бітової площини;
  + метод вбудовування за рахунок енергетичної різниці між коефіцієнтами.

Аудіо-стеганографія:

* Метод LSB для аудіофайлів ідентичний LSB для зображень, але працює з форматом аудіо-файлу. Він спричиняє значні спотворення в контейнері.
* Метод фазового кодування передбачає заміщення початкової фази звукового сегмента еталонною фазою, що і становить приховані даними. Сусідні сегменти узгоджуються з метою зберегти різницю фаз між ними.
* Використання ехо-сигналу. Дані вбудовуються в контейнер шляхом додавання до нього ехо-сигналу. Змінюються три параметри ехо-сигналу: початкова амплітуда, затухання і швидкість зсуву. Він сприймається вухом лише як додатковий резонанс.

Текстова стеганографія, яку можна розділити на форматну та лінгвістичну:

* Методи випадкового інтервалу[2, с. 7]. Зміна кількості пробілів в кінці текстового рядка не викликає значних змін у значенні речення. Більш того, середньостатистичний читач навряд чи зможе виявити незначні просторові зміни:
  + Зміна інтервалу між реченнями. Після речення додаються один або два додаткові пробіли. Цей метод вимагає використання файла значного розміру для вбудовування невеликого числа секретних бітів. Крім того, більшість текстових редакторів автоматично змінюють надлишкові знаки пунктуації та пробіли, що може знищити приховані дані;
  + Зміна кількості пробілів в кінці рядків тексту. Пробіли додаються відповідно до біта, який необхідно приховати. Два пробіли кодують один біт рядка, чотири пробіли - два біти і т.д. У порівнянні з попереднім методом, цей метод дозволяє вбудувати більшу кількість інформації;
  + Зміна кількості пробілів між словами в тексті із вирівнюванням по ширині сторінки. Коли текст вирівнюється по ширині, пробіли між словами не мають однакової довжини, і деякі з них можна використовувати для приховування даних.
* Задання для тексту того ж кольору, що й фон;
* Використання символів Unicode та ASCII, що мають візуальну схожість;
* Використання недрукованих символів Unicode;
* Створення послідовності навмисних помилок та/або відмічених виправлень [7, с. 17].

Форматна стеганографія:

* BMP:
  + Дописування даних у кінець файлу передбачає штучне розширення крайнього сектору зображення;
  + Перестановка палітри.
* JPEG:
  + Дописування даних до кінця файлу. Використання стандартної системи маркерів для дописування за ними інформації, що призведе до ігнорування програмою секретного повідомлення;
  + Використання супутніх даних. Дані попередньо маскуються як допоміжна інформація (індекс сканування, індекс назви тощо), яка найчастіше ігноруються програмами, а потім вбудовуються після певних ідентифікаторів;
  + Використання маркерів коментарів подібно до попереднього методу, але застосовується використання полів коментарів.

Деякі інші методи:

* Конвертування файлу таким чином, що він набуває статистичних характеристик іншого файлу;
* Вбудовування затримок до пакетів, що надсилаються мережею з клавіатури;
* Блог-стеганографія – секретні дані додаються у вигляді коментарів чи дошок об’яв у соціальних мережах;
* Стеганофонія – вбудовування даних у розмовах за протоколом Voice-over-IP, наприклад, використання затриманих або пошкоджених пакетів, які, як правило, ігноруються приймачем (цей метод називається LACK – стеганографія втрачених аудіопакетів,LostAudioPacketsSteganography);
* WLAN стеганографія – передавання стеганограм засобами WirelessLocalAreaNetworks (прикладом реалізації є HICCUPS системи – HiddenCommunicationSystemforCorruptedNetworks).

Нарешті, існує чимало розроблених прогамних продуктів, які реалізують стеганографічне приховування даних за методами, наведеними вище [17, с. 9]:

* Використання методу LSB: OutGuess, JSTEG, JPHS, Hide-and-Seek, Steganos, Steghide, DC-Stegano;
* Використання перестановки палітри: Gifshuffle;
* Формат JPEG: OutGuess, JSTEG, JPHS;
* Формат GIF: Gifshuffle, Hide-and-Seek;
* Формат BMP: Steganos, Steghide;
* Формат PCX: DC-Stegano;
* Використання методу LSB в аудіо-файлах: Invisiblesecrets, Hide4PGP, Steghide, StegoWav, Steghan, S-Tools;
* Використання парності квантування частотних коефіцієнтів: MP3Stego;
* Використання некоректних фреймів у стиснутому потоці: UnderMP3Cover.

Перспективні напрямки розвитку стеганографії наведені у Додатку В.

Наразі, існує чимало наукових робіт, присвячених окремим стеганографічним та стеганоаналітичним рішенням.

Зокрема, роботу [11, с. 2] присвячено стеганографічному аналізу із використанням спеціальних методик видобутку даних (datamining). Операція, яка виводить ряд нових нетривіальних моделей, включених до величезних записів або бази даних називається Data Mining (видобуток даних, інтелектуальний аналіз даних). Він включає використання комплексного аналізу даних, ідентифікацію раніше невідомих структури та асоціаціативних зв’зків в безлічі розрізнених наборів даних. Таким чином, Data Mining передбачає аналіз, прогнозувння, збір та організацію даних. Метою його є реалізація прихованих моделей, непередбачених тенденцій, використовуючи поєднання різноманітних методів, від машинного навчання до біо-модельованої мета-евристики [11, с. 2].

Основною проблемою даного дослідження була велика кількість розрізнених потенційних контейнерів. Метою було представлення підвищеної ефективності використання datamining в стеганоаналізі порівняно зі методами, основаними на моделях систем. До розгляду запропоновані такі методи, як: Дерево рішень (DecisionTree, DT), Векторні машини (SupportVectorMachines, SVM), Naive Bayes (NB), K-наближений сусід (K-nearestneighbour, KNN), нейронна мережа (NeuralNetwork, NN), а також методи кластеризації, агломерації та випадкові алгоритми. У якості доменів прийнято такі типи даних: Зображення, Аудіо, Текст, Відео та Протокол, при цьому кожен з них ділиться на піддомени методів datamining. За результатми дослідження, SVM отримав найкращі результати в порівнянні з іншими методами класифікації. Запропоновані напрямки подальшого вивчення питання.

У [6, с. 4] наведено приклад програмної реалізації стеганосистеми із широкосмуговим вбудовуванням в зображення (SSIS), а також алгоритм взламу F5-стеганографічних систем. Додатково, метод F5 детально описаний в [18, с. 21].

Роботу [19, с. 18] присвячено методу стеганографії, який значною мірою враховує особливості зорової системи людини (ЗСД). Запропонований коефіцієнт масштабування , який залежить безпосередньо від кількості бітів зображення-контейнера. Він виступає фактором вирівнювання для енергії в кожній підматриці, а також дозволяє нормалізувати контраст та яскравість зміненого зображення, що знижує можливість виявлення прихованого каналу.

У роботі [20, с. 3] запропоновано адаптивну пакетну стеганографію на основі правил (Rule-basedAdaptiveBatchSteganography, RABS), яка є покращеною версією статичної пакетної стеганографії. За статичної пакетної стеганографії, секретне повідомлення розбивається на рівні елементи та вбудовується у рівній пропорції в декілька контейнерів (це спричинено обмеженою можливістю вбудовування стеганографічних контейнерів різної природи). Авторами визначено дві основні проблеми такого підходу:

* неефективне використання можливості вбудовування, якщо повідомлення значно менше за стеганографічну потужність контейнера;
* відсутність зваженої оцінки контейнерів при їх виборі для вбудовування секретного повідомлення.

Запропонований метод полягає в нерівномірному поділі повідомлення на елементи на основі сигнатур (набір нечітких правил if-then, що представляє подібність між зображеннями) пустих контейнерів. Такий підхід має знизити час на оцінку потужності вбудовування та підвищити показники стійкості контейнерів до атак незалежно від розмірів початкового секретного повідомлення.

Роботу [21, с. 9] присвячено демаскуючим ознакам стеганографічних систем, в тому числі розроблену математичну модель їх виявлення та оцінки.

У роботі [22, с. 10] наведено оцінку стійкості стеганосистем, основаних на використанні методу модифікації гістограм зображень. Гістограма зображення – це тип гістограми, що виступає графічним представленням тонального розподілу в цифровому зображенні. Зображення-контейнери, створені з використанням такого методу приховування даних, за воєю природою є стійкими до геометричних атак, а експерименти, проведені над тестовими зображеннями, показали високу стійкість до статистичних атак. Крім цього, у [23, с. 12] також запропоновано використання методу гістрограм, проте вже на стороні стеганоаналітика. Атака спрямована на системи, які використовуються LSB, і суть її полягає в тому, що гістограма такого зобаження прийме формму сходинок (по два сусідні значення яскравості, оскільки метод вбудовування вирівнює кількість пікселей у парах).

У [24, с. 8] запропоновано програмну реалізацію (C++) алгоритм вбудовування в аудіо-файл, який не спотворює просторову область та зберігає статистичні показники пустого контейнера.

Особливо цікавий та недостатньо вивчений розділ стеганографії розглянуто у [25, с. 19] – стеганографія без втрат у мовних каналах на прикладі телефонії. Запропонована методика використовує характеристику складеного двійкового коду, що використовується в деяких кодеках, зокрема G.711 та DVI-ADPCM.

Роботу [23, с. 12] присвячено файловій системі StegFS для ОС Linux, яка дозволяє стеганографічно приховувати файли та папки у користуваькому проторі. Система виключає секретні об’єкти з центральної директорії файлової системи, замість цього прописуючи метадані у заголовках самих об’єктів.

Окремим алгоритмам лінгвістичної стеганографії присвячені числені роботи, як-от:

* техніка безневинного тексту (InnocuousText), яка полягає у компонуванні секретного повідомлення тільки з «дозволених» слів, що робить систему стійкою до атак за словником [8, с. 22];
* мімічні функції (MimicFunctions) – використання так званої контекстно-незалежної граматики для генерування штучного тексту, який «мімікрує» під реальний текст (має ідентичні середні значення статистичних показників) [8, с. 22];
* алгоритм, заснований на використанні алгоритму компресії Шеннона-Фано, статистичного аналізатора Стенфорда та методу синтаксичного банку (для автентифікації додатково застосовується SHA 512) [26, с. 15];
* Поєднання лексичної та синтаксичної стеганографії – власне алгоритм працює на рівні речення, тоді як ЦВЗ вбудовується на рівні слова; використовується аналізатор XTAG, дерево залежностей та виділення лінгвістичних ознак задля генерування «природної» мови [16, с. 21];
* GoogleN-gramMethod – автоматична перевірка граматичної корректності та природності парафраз у контексті із використанням Googlen-gramcorpus[27, с. 8].

## **Висновок до розділу**

Таким чином в даному розділі було представлено поняття стеганографії, основні визначення, параметри, об’єкти та суб’єкти стеганографічних систем. Було виконано огляд існуючих популярних методів стеганографії, а також перспективних напрямків її розвитку.

# **РОЗДІЛ 2.** **МЕТОДИ СТЕГАНОГРАФІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В АТАКАХ НА СИСТЕМИ**

Безперечно, пошук інформації у системі є важливим кроком атаки. Більш цікаве питання полягає в тому, як вивести викрадені дані із системи, не викликаючи підозри авторизованого користувача. Інтернет є надзвичайно зручним каналом передавання розвіданої інформації, проте не завжди є можливість його використати. Наприклад, важко передати отримані дані у випадку, коли у мережі коректно налаштовані міжмережеві екрани та запроваджене жорстке адміністрування передавання інформації. Тим більше, що для цього не потрібно продивлятися кожен файл, шукаючи нелегітимні вкладення. Як правило, аналізуються вхідні та вихідні адреси, яких цілком достатньо для виявлення підозрілого трафіку.

Під час роботи кожен електронний пристрій (включаючи ті, що знаходяться в комп'ютері) спричиняє паразитні випромінювання – електромагнітні хвилі, які можна демодулювати і відповідно обробити, аби незаконно отримати з них критичну інформацію.

Об'єктом атак можуть бути системи, заражені шкідливим програмним забезпеченням, яке здійснює пошук необхідної інформації (ключові дані, паролі, конкретні файли тощо) та індукує витік через паразитні випромінювання. Наприклад, якщо приймається сигнал від монітора, то інформація, скажімо, піддається амплітудній модуляції та передається у вигляді візуального зображення на монітор. Очевидним недоліком є ​​те, що подібна діяльність ніяк не може бути пропущена оператором та викличе очевидну підозру, що, зі свого боку, призведе до пошуку та нейтралізації шкідливого ПЗ.

Можливе рішення було запропоноване М. Куном і Р. Андерсоном, які провели серію експериментів щодо програмного управління побічними випромінюваннями. Для кращого розуміння даної технології представимо необхідну теоретичну базу.

## **2.1.Особливості зорового сприйняття цифрових зображень**

Незалежно від алгоритму обробки та задіяного апаратного чи програмного забезпечення, цифрові зображення у будь-якому разі сприймаються зоровою системою людини як і будь-який інший елемент навколишнього середовища. На кінцевому етапі обробки вони виводяться на периферійні пристрої, як-от монітори, дисплеї смартфонів, планшетів тощо.

Стеганографічні системи працюють за принципом введення в оману систем сприйняття, у тому числі зір, тож для розуміння подальшого матеріалу та запропонованого методу необхідно розглянути зорову систему людини.

Зорове сприйняття забезпечується органами зору (очі) та зоровим аналізатором. Зоровими функціями при цьому виступають світловідчуття, кольорове відчуття, центральний, периферичний зір та стереоскопія [9, с. 3].

Світловідчуття – це здатність сприймати світло як специфічний подразник в діапазоні сонячного випромінювання і пристосовуватися до сприйняття навколишнього середовища при різних рівнях освітленості. Світловідчуття людини має такі кількісні характеристики:

* Межа подразнення. Визначається мінімальною кількістю світлової енергії, яка викликає відчуття світла;
* Світлочутливість – величина, зворотна межі подразнення;
* Межа розрізнення. Визначається мінімальною помітною для ока різницею освітленості;
* Швидкість світлової адаптації;
* Швидкість темнової адаптації.

Пристосованість до змінних умов освітленості називається адаптацією. Пристосованість до більш яскравого світла називається світловою, а до менш інтенсивної освітленості – темновою адаптацією.

Кольорове відчуття – здатність сприймати хвильову природу світла, тобто диференціювати його за довжиною хвилі. Кожен колір має три характеристики – тон, насиченість і яскравість. Кольоровий тон визначається довжиною хвилі чистого спектрального кольору, насиченість забезпечується вмістом у ньому чистого тону, а яскравість залежить від домішок білого. Все різноманіття кольорових відтінків виникає в результаті змішування семи чистих тонів спектра, які в свою чергу по закону оптичного змішування кольорів утворюються із трьох основних – червоного, зеленого та синього.

Центральний або предметний зір – здатність розрізняти форму і величину предмета, тобто центральний або предметний зір.Кожен предмет у просторі обмежується площинами, межею яких є лінії, що складаються із точок. Тому в основі центрального зору лежить здатність роздільного сприйняття точок.

Периферичний зір – функція, що забезпечує просторове орієнтування.

Стереоскопія – здатність сприймати об’єм та відстань між об’єктами, а також між спостерігачем та об’єктом у спокої та у русі [9, с. 3].

Людське око сприймає колірну інформацію в діапазоні хвиль приблизно від 380 нм (синій колір) до 770 нм (червоний колір), причому найкращу чутливість має в діапазоні 510 – 530 нм (зелений колір). При цьому, згідно із законом тривимірності сприйняття кольору, око реагує саме на ці три складові – червону, зелену та синю.

Для практичного застосування стеганографії важливими параметрами є пороги кольоророзрізнення, тобто мінімальна змінакольоровості, яку здатне помітити людське око. Кольоророзрізнення має нелінійний характер.

На основі кількісних характеристик, які використовуються для математичного опису зорової системи, виділяють її властивості, спершу об’єднані у дві групи – низькорівневі (фізіологічні) та високорівневі (психофізіологічні) [9, с. 3]. Різниця між ними полягає у тому, що високорівневі властивості проявляються не одразу зі сприйняттям хвиль видимого спектру, а вже після обробки інформації мозком та видачі ним команд на «підлаштування» зору. До низькорівневих властивостей належать (основні, які впливають на розрізнення спотворення у зображенні):

* Чутливість до зміни яскравості – виявлення зміни яскравості при подоланні порогу адаптації; наразі межа нерозрізненості оцінюється у 0,01-0,03 від середніх значень яскравості;
* Частотна чутливість – через нерівномірну амплітудно-частотну характеристику зорової системи, людина є більш сприйнятливою до низькочастотного, ніж до високочастотного шуму;
* Ефект маскування – збудження одних і тих самих підканалів зорової системи компонентами, що мають подібні характеристики, призводить до підвищення порогу виявлення сигналу в присутності іншого сигналу із аналогічними характеристиками; так, наприклад, аддитивний шум менш помітний на високочастотних ділянках зображення.

До високорівневих властивостей відносять [9, с. 3]:

* Чутливість до контраста – висококонтрасні ділянки зображення, перепади яскравості звертають насебе увагу;
* Чутливість до розміру деталей – великі ділянки зображення «помітніші», ніж менші за розміром; при цьому існує межа насичення, коли подальше збільшення розміру не суттєве;
* Чутливість до форми – довгі і тонкі об’єкти викликають більше уваги, ніж круглі однорідні;
* Чутливість до кольору – деякі кольори (наприклад, червоний)помітніші за інші. Цей ефектпідсилюється, якщо фон відрізняється від кольору об’єктів на ньому;
* Чутливість до місця розташування – людина схильна упершучергу розглядати центр зображення та передній план, людей, обличчя, очі, руки;
* Чутливість до зовнішніх подразників – рух очей спостерігача залежить від конкретної обстановки, отриманих інструкції, додаткової інформації.

Усі перераховані властивості враховуються під час обробки цифрових зображень та є ключовими для побудови стеганографічних систем із контейнерами, розробленими для візуального сприйняття.

## **2.2.Особливості обробки цифрових зображень**

Сучасні методи обробки цифрових зображень надзвичайно розвинені та різноманітні. Для розуміння подальшого матеріалу сконцентруємося на основних технологіях, що становлять практичний інтерес для даного дослідження.

Першим механізмом обробки розглянемо квантування.

Воно є цікавим питанням в області комп'ютерної графіки як з теоретичної, так і з практичної точки зору. Метою квантування є зменшення кількості кольорів без будь-яких значно помітних для людського ока ефектів. Квантування є необхідним для обробки зображень, оскільки усі апаратні засоби мають обмеження кількості кольорів зображення. Алгоритми квантування можуть бути статичними або адаптивними. Статичний алгоритм приймає заданий набір кольорів для квантованого зображення, не враховуючи ніяких даних про зображення, яке необхідно квантувати. Адаптивний алгоритм складніший. Він передбачає створення таблиці кольорів на основі параметрів вихідного зображення [28, с. 11].

У квантованому зображенні можуть з'являтися видимі помилки. Процес мінімізації таких помилок називається цифровим напівтонуванням або просторовим дізерингом (зміщенням або дрижжанням). Ідея полягає в тому, щоб змінити квантовані кольори деяких пікселів, аби помилки були менш помітними. Це можливо тому, що людське око інтегрує колір пікселів, що сприймаються. Вхідним є поділ значень червоного, зеленого і синього компонентів оцифрованого зображення (RGB). У типовому форматі кожен з цих трьох колірних компонентів представлений 8 бітами, що дає більше 16-ти мільйонів різних кольорів.

Результатом квантування є таблиця, яка містить кольори, що є певною мірою типовими для початкового зображення. Зберігається лише одне значення з восьми біт у таблиці кольорів, що використовуються для кожного пікселя в кінцевому зображенні [28, с. 11].

У математичному представленні, нехай набір А містить усі різні значення кольорів с у початковому зображенні. При цьому є 24-бітним RGB значенням у множині кольорів. є розміром масиву А. Варто зауважити різницю між кольором та пікселем: являють собою просторові координати пікселя , тоді як є значенням кольору [28, с. 11].

Множина В містить значення, обрані засобом квантування. Із В для кожного пікселя зображення обирається значення представника кольору [28, с. 11].

Ще одним важливим поняттям, необхідним до розгляду, є компресія зображень.

З практичної точки зору компресія інформації взагалі і зображень зокрема – це або зменшення об’ємів пам’яті, що необхідна для зберігання даних, або збільшення об’ємів даних, які передаються за одиницю часу.

Сутність методів компактного подання цифрових зображень полягає у тому, що елементам початкового масиву, які зустрічаються частіше, привласнюється коротший код ніж тим, що зустрічаються рідше. Взаємозв’язок між різноманіттям кодів та ймовірностями їх появи вперше описано в кінці 40-х років ХХ століття Клодом Шенноном у його роботі «Математична теорія зв’язку». Теорема стверджує, що в каналі зв’язку без завад можна так перетворити послідовність символів джерела в послідовність символів коду, що середня довжина символів коду може бути наскільки завгодно близькою до ентропії джерела повідомлень Н(S), що дорівнює

біт/символ, (2.1)

де – ймовірність появи визначеного повідомлення із множини N символів алфавіту джерела [9, с. 3].

Ентропія джерела при цьому максимальна, коли апріорна та апостеріорна ймовірності видачі повідомлення рівні одне одному:

біт/символ (2.2)

Надмірність джерела інформації (необхідний для стеганографічної системи параметр) визначається співвідношенням ентропії даного джерела до максимальної ентропії джерел, що належать до одного (даного) типу. У процесі цифрової обробки максимальна ентропія дорівнює, фактично, кількості розрядів, що використовуються для кодування повідомлення. Коефіцієнт надмірності дає її числове значення [9, с. 3]

(2.3)

та дозволяє кількісно оцінити можливості контейнера у стеганосистемі.

Надмірність може бути зменшена за рахунок використання програмних або апаратних засобів компресії даних, що реалізовують той або інший метод компактного подання даних. Під методом компресії даних розуміється сукупність дій, що дозволяє однозначно зіставити початковий набір даних з набором стиснутих даних. Причому об’єм отриманих в результаті компресії даних менший об’єму початкових даних. Ступінь стиснення (коефіцієнт компресії) визначається як відношення об’єму початкових даних до об’єму їх стиснутого подання

де – об’єм початкових даних (найчастіше – у двійкових одиницях), – об’єм стиснутих даних. Максимально можливий ступінь стиснення без втрат при цьому зворотний коефіцієнту надмірності і становить

(2.4)

де – значення ентропії зображення [9, с. 3].

Наступним показником наведемо співвідношення сигнал/шум у відновлених даних. Шумом тут виступають спотворення, що виникають у результаті виконання компрсії та декомпресії. Співвідношення розраховується як (дБ)

(2.5)

«Майже без втрат» відбувається стиснення зображень у межах 1-2 рівня квантування, а співвідношення сигнал/шум становить більше 50-55 дБ [9, с. 3]. Такі спотворення непомітні для людини через недосконалість зорової системи (див. Особливості зорового сприйняття цифрових зображень).

Останніми наведемо такі об’єктивні параметри, як кореляційні показники спотворення зображень.

Нормована взаємна кореляція становить[9, с. 3]

Якість кореляції при цьому [9, с. 3]

Розглянуті показники належать до об’єктивних. На противагу до них, суб`єктивні показники визначаються за допомогою системи людського зору та не дозволяють однозначно кількісно оцінити якість відновленого зображення.

Поєднання об’єктивних та суб’єктивних показників у повній мірі не вирішена через значну складність кореляції та обчислень. Відносним успіхом у даній сфері можна назвати показник Фаррелла та Ван де Брандена, який знаходиться у такій послідовності:

* зображення ділиться на сегменти
* зображення та помилки кодування розкладаються на компоненти, що враховують особливості органів сприйняття людини (використовуються гребінчасті фільтри)
* знаходиться поріг виявлення для кожного пікселя на основі початкового зображення-маски
* фільтрована помилка розподіляється за допомогою порогу прийняття рішення
* помилки об’єднуються за усіма колірними компонентами [9, с. 3].

У загальному вигляді, комплексний показник вираховується за формулою (ВдБ)

де – обчислене спотворення, ВдБ – так званий «візуальний децибел» [9, с. 3].

Як основний показник, що визначає область застосування того або іншого методу, можна виділити наявність втрат інформації при компресії. Методи компресії з втратами, незважаючи на високі коефіцієнти стиснення, не є ефективними у застосуванні щодо інформації у вигляді тексту або цифрових послідовностей. Не можуть застосовуватися вони також для даних, на основі яких ухвалюються важливі управлінські рішення. Отже, методи компресії з втратами можуть знайти лише обмежене застосування в системах зв’язку універсального призначення.

Нарешті, при роботі із зображеннями у комп’ютерних системах важливим поняттям є так званий дізеринг (image dithering).

Аналоговий сигнал може бути представлений як безперервна функція, залежна від часу, наприклад, напруги на виході аналогової схеми. Безперервність тут розуміється в тому ж сенсі, що і безперервність в математичному аналізі: якщо наявні будь-які два різні моменти часу, то завжди можна вирізнити якийсь момент часу між ними, і так до нескінченності. У цифровій електроніці від аналогового сигналу беруть його значення тільки в певні моменти часу (з частотою наприклад 44,1 кГц або 96 кГц) та округлюють їх до певних значень (найчастіше 16/20/24 двійкових цифр).

Дізеринг, дітеринг (англ. – дрижжати) – при обробці цифрових сигналів являє собою підмішування до початкового сигналу псевдовипадкового шуму зі спеціально підібраним спектром. Застосовується при обробці цифрового звуку, відео та графічної інформації для зменшення негативного ефекту від квантування [29, с. 12].

Багато різних видів апаратних засобів відображення, включаючи ранні комп'ютерні відеоадаптери, а також багато сучасних LCD-дисплеїв, що використовуються в мобільних телефонах і недорогих цифрових камерах, відображають набагато менший колірний діапазон, ніж дисплеї вищого рівня. Як приклад, дізеринг може бути використано для того, аби зображення, що містить мільйони кольорів, відобразити на засобах візуалізації, здатних виробляти лише 256 кольорів одночасно. 256 доступних кольорів будуть використовуватися для генерації розмитої апроксимації почтакового зображення. Без дізерингу, кольори у вихідному зображенні будуть «округлені» до найближчого доступного кольору, в результаті чого нове зображення лише приблизно відповідатиме оригіналу. Дізеринг використовує властивість людського ока змішуватидва колльори в безпосередній близькості один від одного.

Таким чином, у комп'ютерній графіці дізеринг використовується для створення ілюзії глибини кольору для зображень з відносно невеликою кількістю кольорів у палітрі. Відсутні кольори складаються з наявних шляхом їх «перемішування». Наприклад, якщо необхідно отримати відсутній у палітрі фіолетовий колір, його можна отримати, розмістивши червоні та сині пікселі в шаховому порядку (Рис. 2.1); помаранчевий колір може бути складений із червоних і жовтих точок тощо.

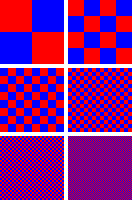
[](https://commons.wikimedia.org/wiki/File:Dithering_example_red_blue.png?uselang=ru)

Рис. 2.1.Приклад отримання фіолетового кольору шляхом розташування червоних та синіх пікселів у шаховому порядку [29, с. 12]

Наведемо такий приклад на реальному зображенні [30, с. 6]:

Поєднуючи чорні та білі пікселі за складним алгоритмом, програми графічної обробки, як-от Adobe Photoshop, можуть створювати ілюзію сірих тонів:



Рис. 2.2.Дізеринг до двох кольорів

Аналогічно, для кольорових зображень можна добитися «згладжування» ефекту від зменшення кількості кольорів:

Рис. 2.3.Оригінальне зображення Рис. 2.4.Зображення з 256-ти кольорів із застосуванням дізерингу

Деякі LCD-дисплеї можуть використовувати часовий дізеринг для досягнення подібного ефекту. Швидко змінюючи значення кольору кожного пікселя між двома приблизними кольорами в колірному просторі (також відомому як контроль частоти кадрів – Frame Rate Control), панель дисплея, яка початково підтримує лише 18-бітний колір (6 біт на канал), може представляти 24-бітне зображення (8 біт на канал).

Але навіть якщо загальна кількість доступних кольорів на дисплеї є достатньо високою для належного відображення повнокольорових цифрових фотографій (наприклад, таких, що використовують 15- і 16-бітові кольорові режими RGB Hicolor 32,768/65,536), об’єднання все одно може бути помітним, особливо у великих областях плавних переходів відтінків. Навіть з оптимізованими палітрами в зображенні будуть присутні значні області суцільного кольору. Дізеринг 32 або 64 RGB-рівнів дасть у результаті прийнятне наближення кольору зображення, яке не виглядатиме «зернистим» для людського ока. Крім того, зображення, що відображаються на 24-бітному апаратному забезпеченні (8 біт на компонент), можуть піддаватися дізерингу з метою імітувати дещо більшу глибину біта та/або мінімізувати втрату відтінків після гамма-корекції (нелінійна операція, що полягає у предспотворенні яскравості компонент зображення для підлаштування його до сприйняття зоровою системою людини) [29, с. 12].

Насправді, дізеринг використовується в багатьох різних областях, де присутні цифрові обробка та аналіз. До таких застосувань належать системи, що використовують цифрову обробку сигналів, як-от цифрове аудіо, цифрове відео, цифрову фотографію, сейсмологію, радіолокаційні комплекси та системи прогнозування погоди. Квантування за своєю природою дає помилку. Якщо ця помилка корелюється із сигналом, результат стає потенційно циклічним та/або передбачуваним. У деяких застосуваннях циклічні помилки дають небажані результати. У таких випадках введення дізерингу перетворює помилку на випадковий шум. Обробка аудіо є яскравим прикладом подібної ситуації. Людське вухо працює подібно до перетворення Фур'є, тобто чує окремі частоти. Отже, слухова система дуже чутлива до спотворень або до додаткового частотного вмісту, проте набагато менш чутлива до додаткових випадкових шумів на всіх частотах, таких як у сигналі після застосування дізерингу [29, с. 12]. Таким чином, в обробці звуку дізеринг полягає в додаванні до сигналу невеликої кількості шуму (псевдовипадкового цифрового сигналу) різного спектру (білий, рожевий тощо). При цьому помітно послаблюється кореляція помилок квантування із корисним сигналом («розсіюються» помилки округлення) і, незважаючи на деяке збільшення шуму, суб'єктивна якість звучання помітно підвищується. Рівень додаткового шуму обирається залежно від ситуації та коливається від половини молодшого розряду відліку до декількох розрядів.

Отже, наразі створено певну кількість алгоритмів дізерингу, які у загальному випадку допомагають зменшити видимі помилки кванутвання та створюють ілюзію більшої кількості кольорів, ніж їх є насправді. Найпростішим способом є додавання білого шуму до зображення. Білий шум рівномірно розподілений по всьому спектру потужності. Ефект цієї простої ідеї не дуже прийнятний для користувача, оскільки шум викликає спотворення. За своєю природою, дізеринг вводить закономірності до зображення – теоретично вважається, що зображення буде розглядатися з такої відстані, що ніякий паттерн не буде помітним для людського ока. На жаль, на практиці це не завжди працює, особливо із зображеннями в Інтернеті. Ulichney провів дослідження, результатом яких став той факт, що шум повинен розміщуватися на високих частотах спектру потужності. Він представив модель, що називається блакитним шумом, що виступає найменш помітним при сприйнятті зображення. Іншим методом є розподілення помилки (псевдозміщення, стохастичне вирівнювання) квантування по сусідніх пікселях. У цьому підході, як локальні, так і глобальні значення інтенсивності залишаються на почтаковому рівні. Флойд і Штейнберг розробили алгоритм розподілення помилок такого роду [28, с. 11]. Тим не менше, інші методи, такі як впорядкований дізеринг, також можуть використовувати синій шум без виродження в колірних областях [29, с. 12].

У загальному випадку, можна навести такі популярні методи дізерингу:

* Використання порогового значення (усереднений дізринг): кожне значення пікселя порівнюється із фіксованим порогом. Найпростіший алгоритм згладжування, який призводить до втрати деталей і контурів;
* Випадковий дізеринг. Кожне значення пікселя порівнюється із випадковим порогом, що призводить до зображення із візуальним шумом. Метод не створює закономірностей, проте «змазує» деталі зображення. Подібний до мезотонування;
* Дізеринг із фіксованим паттерном. Для кожного із вхідних значень застосовується шаблон так, що результат стає значенням результуючого зображення;
* Впорядкований дізеринг (використовує дізер-матрицю). Для кожного пікселя зображення значення шаблону у відповідному місці використовується у якості порогу. Сусідні пікселі не впливають один на одного, роблячи даний алгоритм придатним для використання в анімації. Різні шаблони можуть генерувати абсолютно різні ефекти змішування. Важко провести модифікації для роботи з довільними палітрами. Він зазвичай використовується програмами, які повинні забезпечувати безперервне зображення «вищих» кольорів із меншою глибиною кольору. Наприклад, Microsoft Windows використовує його в 16-кольорових графічних режимах. Легко виявити за помітним «перехрещуванням» на зображенні:
  + Матриця напівтонового дізерингу створює вигляд, схожий на напівтони у газетах. Форма кластерного дізерингу. Основним використанням цього методу є офсетний друк і лазерні принтери;
  + Матриця Байєра створює дуже характерний хрестоподібний малюнок;
  + Матриця, налаштована на блакитний шум; генерація методом «void-and-cluster» призводить до наближення до методу розподілення помилок;

[https://upload.wikimedia.org/wikipedia/commons/e/e5/Ordered_4x4_Bayer_matrix_dithering.png](https://en.wikipedia.org/wiki/File:Ordered_4x4_Bayer_matrix_dithering.png)

Рис. 2.5 – Характерні 17 візерунків матриці 4 × 4 для впорядкованого дізерингу [29, с. 12]

* Розподілення помилок – це процес зворотного зв'язку, який розподіляє помилку квантування на сусідні пікселі:
  + Дизеринг Флойда-Штейнберга (FS) поширює помилку лише на сусідні пікселі;
  + Дізеринг із мінімізованою усередненою помилкою, розроблений Джарвісом, Джудісом і Нінке, розсіює помилку на кожні два сусідні пікселі;
  + Алгоритм Стакі, алгоритм Беркса, алгоритм Сьєрра та його дворядний варіант – модифікації вищезазначеного алгоритму;
  + FilterLite – пришвидшений алгоритм Флойда-Штейнберга;
  + Дізеринг Аткінсона подібний до алгоритмів Джарвіса та Сьєрра. Відмінність полягає в тому, що розсіюється не вся помилка квантування, а лише її три чверті. Як результат, темні та світлі ділянки сильно вирізняються на фоні інших;
  + Нещодавно розроблене градієнтне розподілення помилок використовує модульовану рандомізацію та градієнтну модуляцію для роботи зі структурним компонентом зображення [29, с. 12].

У роботі [28, с. 11] запропоновано новий алгоритм дізерингу – так званий n-bestalgorithm, який полягає у додаванні шуму, пропорційного помилкам квантування. «Сильною стороною» даного алгоритму є те, що він не створює закономірностей у зображенні.

## **2.3.Побічні електромагнітні випромінювання та наведення (ТЕМПЕСТ).**

У процесі функціонування будь-який електронний пристрій, у тому числі елементи комп’ютерів, випромінюють електромагнітні коливання, за допомогою яких після демодуляції та спеціальної обробки можна отримати інформацію, яка власне обробляється на пристрої, а також про процеси, які у ньому відбуваються. Загальна назва для таких коливань в українській нормативній документації – побічні електромагнітні випромінювання та наводки (ПЕМВН), а в зарубіжній – TEMPEST (TelecommunicationsElectronicsMaterialProtectedFromEmanatingSpuriousTransmissions), за першим американським стандартом, присвяченим цьому питанню, або “compromisingemanations” [32, с. 15].

Умови виникнення ПЕМВН:

* великі значення паразитних індуктивностей і ємностей пристроїв;
* наявність шлейфів, що з'єднують елементи всередині пристроїв, по яких течуть електричні струми інформативних сигналів;
* великі довжини спільного пробігу з'єднувальних ліній технічних засобів передачі інформації і сторонніх провідників;
* неекрановані (або слабо екрановані) дроти;
* елементна база з високим рівнем випромінювання сигналів[33, с. 17].

Наприклад, сполучні кабелі утворюють резонансні ланцюги, що складаються з індуктивності кабелю і ємності між пристроєм і землею; ці ланцюги збуджуються високочастотними компонентами сигналу даних, і результуючі ВЧ-коливання спричиняють електромагнітні хвилі.

Найбільш небезпечні сигнали (потенційно інформативними ПЕМВ) створють елементи ПК (особливо у пластикових неметалізованим корпусах), наведені у таблиці [34, с. 20].

Таблиця 2.1

Виявлення полів від різних пристроїв

|  |  |  |
| --- | --- | --- |
| ПЕМВН | Дальність виявлення полів, м  електромагнітного    електричного | |
| Системний  блок | 2 – 40 | 1 - 30 |
| Дисплей | 25 – 120 | 10 - 55 |
| Клавіатура | 15 – 50 | 15 - 30 |
| Друкуючий пристрій | 5 – 35 | 10 -80 |

У більшості країн світу прийняті стандарти, які вимагають обмеження рівня побічних випромінювань. Тим не менше, якщо вказані обмеження і дозволяють знизити рівень так, що вони не шкодять людині та не впливають на роботу інших пристроїв, їх все ще можна перехопити ззовні, особливо зважаючи на не менш стрімкий розвиток пристроїв технічної розвідки.

Сучасні досягнення в області технології виробництва радіоприймальних пристроїв дозволили створювати дуже мініатюрні чутливі приймачі. Успішно впроваджується багатоканальний прийом сигналів (як з різних напрямків, так і на різних частотах), з подальшою їх кореляційної обробкою. Це дозволило значно збільшити дальність перехоплення інформації. Найбільшою загрозою є той факт, що із використанням ПЕМВН інформацію можна отримати, не залишивши жодних слідів у системі.

Якщо розвиток питання про ПЕМВН розпочинався із суто військового застосування (у тому числі спецслужбами), то наразі і конкуруючі комерційні організації, і кримінальні структури проводять такі атаки задля отримання необхідної інформації. Крім того, застосування при передачі інформації стійких алгоритмів шифрування на даному етапі розвитку криптографії часто не залишає шансів дешифрувати перехоплене повідомлення. У цих умовах TEMPEST-атака може бути єдиним способом отримання хоча б частини інформації до того, як вона буде зашифрована, оскільки випромінювання модулюються інформативним сигналом ще до початку шифрування та випромінюються у простір. Ще одним широким простором для використання ПЕМВН є шахрайство із кредитними картками, під час якого застосування спеціальних технологій дозволяє отримати дані власників, не торкаючись картки чи банкомата [35, с. 14]. Припускають, що зловмисник, озброївшись досить простим радіоустаткуванням і вставши біля банкомату, може реєструвати як сигнали від магнітної смужки, так і PIN-дані користувачів, оскільки зчитувач карти та клавіатура, як правило, з'єднуються з ЦПУ за послідовними лініями.

Розроблено чимало способів та засобів захисту від подібних атак, організаційних (головним чином, контроль доступу), а також технічних – фільтрація із більшим затуханням у широкій полосі частот, інженерне та технічне екранування, зонування, зашумлення тощо. Розглянемо детальніше деякі з них.

Екранування дозволяє знизити рівень побічних електромагінтних випромінювань на межі контрольованої зони до величин, які забезпечують неможливість виділення інформативного сигналу на фоні шумів. Воно здійснюється шляхом проведення інженерних заходів та/або налаштуванням технічних засобів, які відбивають випромінювання всередину пристрою. Недоліком є складність забезпечення екранування в широкому діапазоні частот, а також незручність в ергономічному плані. У роботах Меллера, Бернштайна і Кольберга обговорюються різні методи екранування. Тим не менше, Смулдерсом показано, що часто можна перехоплювати навіть сигнали від екранованих кабелів, наприклад, RS-232 [36, с. 18].

Зашумлення застосовується для захисту інформації шляхом внесення додаткового електромагнітного шуму у визначеному діапазоні частот. При цьому ускладнюється знімання інформації за допомогою закладних підслуховуючих пристроїв малої потужності. До недоліків можна віднести нерівномірність зашумлення у просторі, яка робить необхідним проведення складних вимірювань та обстежень приміщення. До того ж, наявність додаткового джерела випромінювань може впливати на здоров’я людини та вносити завади для роботи легітимних пристроїв [33, с. 17].

Фільтрація забезпечує захист від паразитних наводок шляхом відсікання певних частин випромінення. Вузька направленість даного метода не дозволяє використовувати його комплексно для захисту інформації в системі.

Довгий час вважалося, що сучасні LCD та LED монітори не піддаються ефективній TEMPEST-атаці, так як неодноразово демонструвалося на CRT-дисплеях. Значну роль тут грала властивість CRT-дисплеїв працювати на високих частотах. Випромінювали компоненти відеоадаптера (широкополосне випромінювання відеопідсилювача та вузькополосне – підсистеми синхронізації), а також кабелі з’єднання, при чому такі дефекти як контакт, що окислився, чи погана пропайка у кабелях чи роз’ємах могли підсилювати рівень на кілька порядків. LCD не були вразливими до такого типу атак, не тільки тому, що їхні пікселі реагують набагато повільніше, ніж люмінесцентні фосфори CRT, але й тому, що за нової технології всі пікселі ряду оновлюються одночасно [37, с. 5].

Тим не менше, у роботах [38, с. 19] та [37, с. 5] продемонстровано, що начебто більша захищеність LCD-дисплеїв порівняно із CRT є міфом. Випромінювання у деяких випадках дійсно нижче за рівнем, особливо для портативних комп’ютерів, проте те пов’язано не із типом дисплея, а із меншою довжиною шлейфу, що поєднує екран із відео-чіпом.

Частоти пікселів і смуги пропускання для сигналів візуального відображення збільшилися на порядок, оскільки аналогова передача сигналу замінилася цифровими відеоінтерфейсами Гбіт/с. Різноманітні технології плоских дисплеїв (Flat-PanelDisplay – FPD) прийшли на зміну моніторам із електронно-променевою трубкою (CRT).

Таким чином, фактично, два факти сприяли припущенню, що нові монітори не були вразливими до Темпест-атак. По-перше, FPD не мають котушок відхилення, що робить їх (в порівнянні з CRT) пристроями з низьким рівнем випромінення на частотах нижче 400 кГц, де напруженість поля обмежена Шведським ергономічним стандартом [37, с. 5]. По-друге, LCD-дисплеї працюють із низькою напругою і, на відміну від CRT, не посилюють відеосигнал з метою контролю сітки управління, що модулює електронний промінь.

Проведені експерименти демонструють, що деякі типи плоских дисплеїв створюють реальний ризик витоку через канали ПЕМВН. Зокрема, за використання деяких сучасних відеоінтерфейсів, досить легко налаштувати відображення тексту так, що стійкість сигналу (витоку) буде максимізовано.

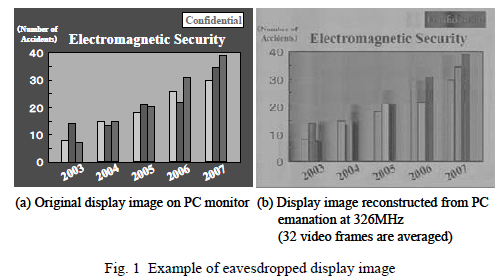
У роботі [37, с. 5] проаналізовано компрометуючі радіовипромінювання спочатку на LCD -моніторі ноутбука, а потім на LCD -дисплеї, підключеному до відеокарти із цифровим інтерфейсом (DVI). В обох випадках відеокабель, який використовується для підключення дисплейної панелі до графічного контролера, виявився основним джерелом сигналу, що створює канал витоку інформації.

Оскільки плоскі дисплеї повинні зберігати відеолінії у цифровій пам'яті, вони потребують відеоінформації не тільки у вигляді бінарного коду, що відповідає відтінкам кольорів, але і як послідовність дискретних значень пікселів. Тому всі нові стандарти цифрового інтерфейсу включають в себе лінію так званого pixelclock (частоти слідування пікселів), уникаючи реконструкції піксельного синхронізуючого сигналу, який повинен виконуватися в FPD із входом VGA [37, с. 5].

Сучасні FPD поміщують у буфер в цифровому вигляді лише декілька рядків пікселів. Все зображення все ще зберігається тільки в буфері кадрів відеоконтролера. Таким чином, сучасні відеоінтерфейси FPD все ще повинні постійно оновлювати весь вміст зображення від 60 до 85 разів на секунду, як і з CRT. Таке безперервне оновлення забезпечує періодичність сигналів на відеоінтерфейсі, принаймні на час змін відображуваної інформації. Періодичний сигнал має частотний спектр, який складається з вузьких ліній на відстані частоти повторення між ними. Приймач може послабити весь інший спектральний вміст шляхом періодичного усереднення з ідентичною частотою повторення [37, с. 5].

Ще одним яскравим практичним прикладом можуть бути пристрої із «повільними» послідовними портами (104–105 біт/с), такі як деякі модеми із LED індикацією для представлення логічного рівня рядів даних. Практично будь-який електронний пристрій має світлодіодні індикатори режимів роботи. Світлодіоди мають малу інерційність та дозволяють модулювати світловий потік сигналами з частотою до сотень мегагерц. Наведення від всіх елементів блоку, в якому встановлений світлодіод, призводять до того, що світловий потік постійно включеного світлодіода модулюється високочастотними коливаннями, непомітними для ока, але які можуть бути виявлені за допомогою спеціальної апаратури [35, с. 14]. Якщо сигнал не спотворюється, наприклад, за допомогою моностабільної мультивібраційної схеми, що забезпечує мінімальний період щонайменше рівня байта, на приймачі можна реконструювати передані дані шляхом моніторингу світимості LED на відстані [38, с. 19].

У роботі [39, с. 23] наочно продемонстровано реконструкцію сигналу з монітора, прийнятого від пристрою через побічні випромінювання. В експерименті використовувалась логоперіодична антена UHALP9107 (Schwarzbeck) та аналізатор спектра FSET (Rohde&Schwarz) у якості приймача. На 3х метрах від ПК на частоті 326 МГц було прийнято та реконструйовано сигнал із великою часткою шуму, якого можна позбутися, провівши усереднення відеокадрів. Результати представлено на Рис. 2.6[39, с. 23]:



а) б)

Рис. 2.6.Перехоплене зображення із дисплея ПК: а) оригінальне зображення на моніторі; б) реконструйоване з випромінювань на 326 МГц

## **2.4.SoftTempest**

Отже, як було вказано у вступі до даного розділу, сильною стороною використання SoftTempest є експлуатація каналу витоку ПЕМВН із отриманням інформації, яка представляє безпосередній інтерес. До того ж, використовується найпотужніше джерело випромінювання (монітор), тим самим спрощуючи приймання корисного сигналу. Розглянемо дану технологію детальніше.

Технологію SoftTempest (іноді перекладають як «м’який ПЕМВН», проте це не є коректним; мається на увазі «програмний ПЕМВН») було запропоновано вченими Маркусом Куном та Россом Андерсом у відповідній роботі [36, с. 18]. Власне кажучи, під технологією Софт Темпест можна розуміти кілька варіацій застосувань. Найпростіше програмне управління побічними випромінюваннями можна уявити як роботу програмної закладки, що для передачі «1» буде використовувати збільшення сигналу, для передачі «0» - зниження рівня випромінювань. Ускладнити цей алгоритм можна, змінюючи яскравість у деяких точках монітора та передаючи інформацію на заздалегідь відомих частотах [40, с. 29]. Ще одним відносно простим варіантом застосування є використання амплітудної модуляції зображення на екрані та звичайний АМ-приймач. Недоліком такого підходу є те, що на екрані з’являється характерне зображення, зумовлене частотою амплітудної модуляції [10, с. 11]:

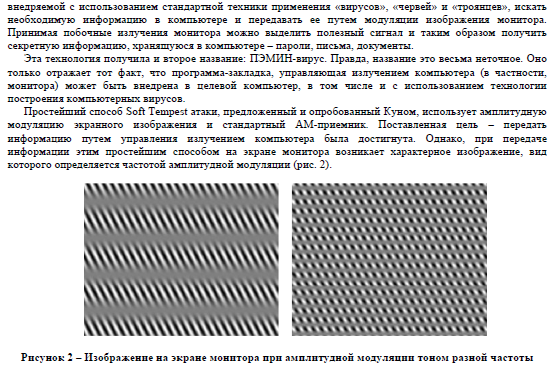


Рис. 2.7. Зображення на моніторі при використанні амплітудної модуляції тоном різної частоти

Подібне спотворення інформації, що відображається на екрані, важко не помітити, що робить прихованість атаки неможливою (принаймні, під час безпосередньої роботи оператора). Таким чином, усе зводиться до необхідності рішення задачі стеганографії у класичному її формулюванні («проблема в’язнів). А саме, необхідно вбудувати секретну інформацію у випромінювання таким чином, що законний користувач не виявить канал передавання.

Темпест-приймач головним чином висвічує високочастотну частину відеосигналу. Найсильніші корисні спектральні компоненти знаходяться на частотах, близьких до частоти пікселів і її гармонікам.

Як було зазначено у попередніх розділах, людське око більш чутливе до низькочастотних, ніж до високочастотних коливань, тоді як TEMPEST-приймачі працюють навпаки. Власне, на цьому принципі працює дізеринг (див. розділ «Особливості обробки цифрових зображень»). При цьому, «шаховий» паттерн, який створює дізеринг, породжує максимально можливий за силою сигнал, тоді як постійний однотонний колір дає в результаті найслабший сигнал [32, с. 15]. Більш того, будь-які пристрої в першу чергу лінійно сприймають світність, а люди більш чутливі до темних кольорів. Така різниця сприйняття та спектральної чутливості може бути використана для вбудовування повідомлення у випромінювання так, що воно не викличе підозри користувача, оскільки дві сторони «бачитимуть» різні картинки.

Суть запропонованого методу полягає у контролі та модифікації моделей дізерингу на моніторі [36, с. 18]. Тобто, з одного боку, пікселі двох кольорів, розміщені у шаховому порядку, сприймаються як єдиний колір; з іншого боку, вони створюють високочастотний сигнал, а до таких сигналів TEMPEST-обладнання найбільш чутливе. Єдиним етапом обробки, що залишається після модифікації паттернів дізерингу, що перетворюють монітор на стеганосистему, є гамма-корекція.

Текст, який бачить перехоплювач, - це гамма-скоригована амплітудна модуляція паттерна фону, а власне повідомлення для користувача – просто низькочастотний сигнал.

У кожному конкретному випадку параметри дізерингу повинні вручну калібруватися під конкретний монітор. Зміни налаштувань залежать не тільки від типу монітора, але і від яскравості, контрастності та інших параметрів, які користувач може змінювати. З точки зору стеганографії, оптимальним рішенням буде приховати секретний текст не в рівномірно забарвлених областях, а в структурно-багатому екранному вмісті, як-от фонові фотографії або анімація скрин-сейверів [36, с. 18].

Складніший варіант алгоритму атаки полягає в оптимізації частини зображення для цілей вбудовування інформації. У разі професійної атаки для подолання глушіння сигналу можна використовувати техніку «розсіяного спектра». Програма-закладка за допомогою дізерингу розкладатиме один або кілька кольорів в декількох рядках екранної картинки, використовуючи псевдовипадкову бітову послідовність (ПВБП). Наприклад, може вбудувати «тремтіння» в рядок меню вікна. Крос-коррелятор у приймачі отримує один вхід з антени та шукає на інших своїх входах ідентичну послідовність псевдовипадкових біт, що видається з передбачуваною частотою піксель монітора. Крос-коррелятор генерує вихідний пік, що дає різницю фаз між приймачем і комп’ютером-мішенню. Потім цикл із замкненою фазою може керувати осциллятором приймача таким чином, усереднення екранного вмісту було стабільним та якомога більш довготривалим. Інформацію можна транслювати інвертуванням ПВБП, в залежності від того, чи повинен передаватися біт зі значенням «0» або «1».

Якщо ж ПВБП, що кодується рядом чорних і білих пікселів, занадто відрізняється від зазвичай сірої (або іншого кольору, від цього залежатиме і паттерн дізерингу) інструментальної лінійки меню, звичної користувачеві, то замість цього можна використовувати фазову модуляцію. Амплітуду паттерна дізерингу можна змінювати поступово для декількох пікселів поблизу фазових стрибків, аби уникнути видимих змін яскравості на лінійці меню [36, с. 18].

Змінювати параметри, необхідні для такої атаки, можна у файлах конфігурації, залежно від ОС, типу монітора, яскравості, освітленості, контрастності тощо. Наприклад, для більшості Linux-систем можна модифікувати файл /usr/lib/X11/XF86Config.

Загалом, комп'ютер-мішень програмується таким чином, що він діє у якості радіопередавача та випромінює складений паразитний сигнал: авторизований користувач бачить одне зображення, а зловмисник отримує інше – вбудоване – виведеним на монітор свого TEMPEST-приймача. Якщо у якості зображення, що виконує роль стеганографічного контейнера, використати фон робочого стола, то подібна атака не викличе підозри у користувача, не дивлячись на те, що саме у цей час до ефір випромінюватиметься секретна інформація [10, с. 11].

Запропонована вченими Кембриджу технологія Soft Tempest за своєю суттю є різновидом комп'ютерної стеганографії, тобто методу прихованої передачі корисного повідомлення у відео, аудіо, графічних і текстових файлах, що не викликають підозри.

Особливістю технології Soft Tempest є використання для передачі даних каналу ПЕМВН, що значно ускладнює виявлення самого факту несанкціонованої передачі в порівнянні з традиційною комп'ютерною стеганографією. Дійсно, якщо для запобігання несанкціонованій передачі даних локальною мережею або мережею Інтернет існують апаратні та програмні засоби (FireWall, Proxy, VPN тощо), то інструментів для виявлення прихованої передачі даних по ПЕМВН немає, а виявити таке випромінювання в загальному широкополосном спектрі (більше 1000 МГц) паразитних випромінювань без знання параметрів корисного сигналу вельми проблематично [35, с. 14].

Основна небезпека технології Soft Tempest полягає у прихованості роботи програми-вірусу. Така програма, на відміну від більшості вірусів, не псує дані, не порушує роботу ПК, не створює несанкціоновану розсилку мережею, а отже, довгий час залишається непомітною для користувача та адміністратора мережі. Тому, якщо віруси, що використовують Інтернет для передачі даних, проявляють себе практично миттєво, що дозволяє на них швидко зреагувати, то програмні засоби, що використовують ПЕМВН для передачі даних, можуть працювати роками, не виявляючи себе.

Оригінальний експеримент Куна та Андерсона було проведено у комп’ютерній лабораторії університету Кембридж. Для Темпест-моніторингу вони використовували приймач ESL model 400 фірми DataSafe Ltd. (Челтнем, Англія). По суті своїй, це звичайний чорно-білий телевізор із деякими модифікаціями, найбільш важлива з яких полягає у тому, що схеми відновлення сигналу синхронізації замінені двома осцилляторами, що налаштовуються вручну. Частота горизонтального відхилення або частота рядків може обиратися в межах 10 - 20 КГц з майже міллігерцовою роздільною здатністю, а частота вертикального відхилення або частота кадрів – в межах 40.0 - 99.9 Гц із роздільною здатністю 0.1 Гц. Таким чином, даний пристрій можна було налаштувати на 4 смуги в діапазоні 20 - 860 МГц зі змінною чутливістю (60 µV та 5 µV відповідно) [36, с. 18]. Також для експерименту використовувалась 4-метрова дипольна та логарифмічно-спіральна конічна антени, що дали різні за якістю результати. Монітор – 43-см Super-VGA ПК-монітор зі смугою відеосигналу 160 МГц.

Далі наведені отримані вченими результати [36, с. 18]:

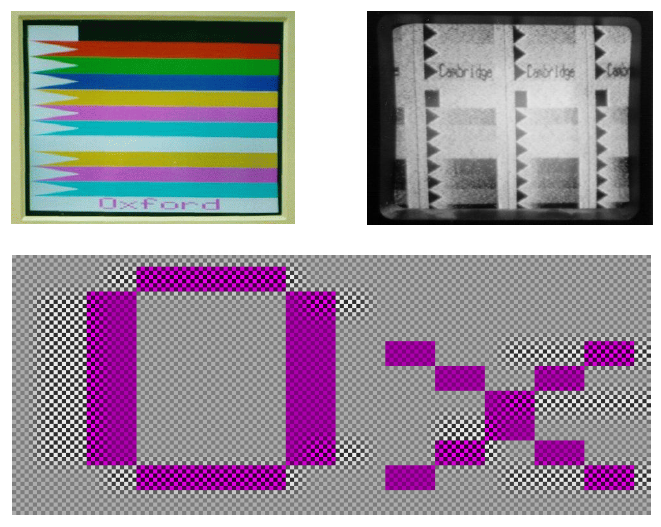


Рис. 2.8. Зліва: зображення на моніторі; справа: перехоплений сигнал на моніторі приймача (три копії через те, що частота вертикального відхилення нижча, а саме 16,1 кГц замість 64 кГц, а четверту копію втрачено у процесі відкату променя CRT)

Тестова картинка складається з:

* ліва частина – один прямокутний і кілька трикутних маркерів, намальованих патерном дізерингу із вертикальних чорних і білих ліній. Ці маркери допомагають простежити властивості картинки, і навіть із простою дипольною антеною їх чітко видно на моніторі приймача, навіть з інших приміщень на відстані понад 20 метрів;
* праворуч від кожного маркера – кольорова смуга, що здається рівномірною на моніторі комп'ютера. Ці смуги, слідом за сімома трикутниками, були намальовані рівномірними кольорами (темно-червоний, темно-зелений, темно-синій, жовтий, рожевий, блакитний та сірий) з лівого краю і поступово відтінялися дізерингом праворуч (червоний/чорний, зелений/чорний , синій/чорний, жовтий/чорний, рожевий/чорний, блакитний/чорний, білий/чорний);
* три смуги нижче – знову жовта, рожева та блакитна з лівого краю, але на цей раз дізеринг дає фазовий зсув між початковими кольорами так, що цей патерн до правого краю стає червоно/зеленим, червоно/синім і синьо/зеленим. Між лівим і правим краями смуг амплітуда паттерна лінійно наростає. Подябна тестова картинка дозволяє виявити поріг, з якого починається ефективне прийняття сигналу [36, с. 18].

Наочною є демонстрація чутливості перехоплювача до амплітуд «тремтіння» в кольоровий смузі праворуч від одинадцятого трикутника. У той час як комп'ютерний монітор явно висвічує великими літерами слово «Оксфорд», натомість на екрані приймача видно слово «Кембридж»:

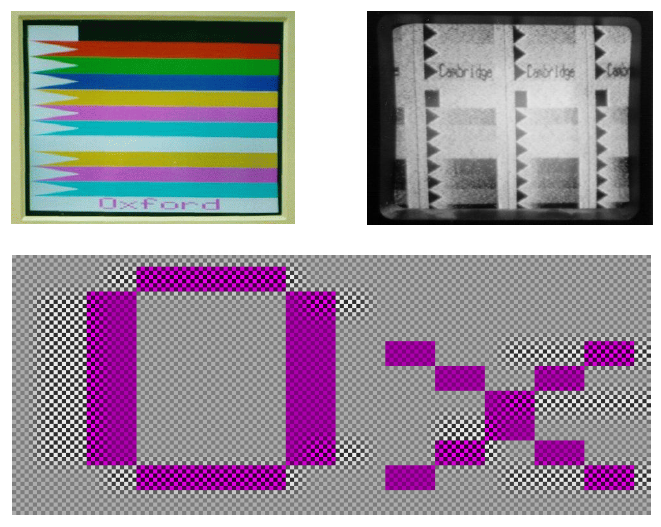


Рис. 2.9.«Oxford» намальовано рожевим замість сірого шляхом виключення зеленої компоненти, а «Cambridge» вбудовано нарощуванням амплітуди тремтіння [36, с. 18]

Як показано на рис. 2.10, текст та зображення можна взаємозамінно вбудовувати одну в одне:

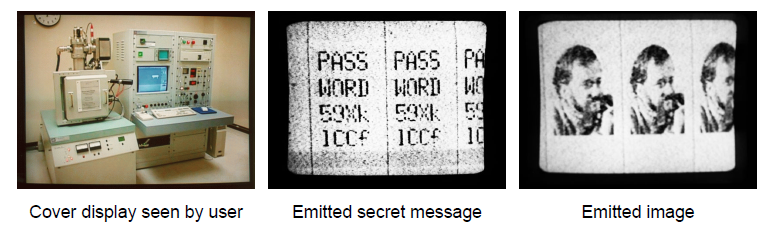


Рис. 2.10.Зображення на моніторах Темпест-приймача (ліворуч) та комп’ютера користувача (праворуч) [36, с. 18]

Окрім оригінального експерименту Куна та Андерса, вченими з різних країн світу було проведено низку досліджень, присвячених технології Soft Tempest, проте більшість з них було присвячено покращенню вбудовування інформації, а не засобам захисту від подібних атак.

Так, на виставці «Безпека 2012» у Києві представники компанії ЕПОС продемонстрували можливість програмної передачі інформації шляхом її виведення на незадіяний послідовний порт (інтерфейс розробленого програмного продукту зображено на рис. 2.11) [35, с. 14]:

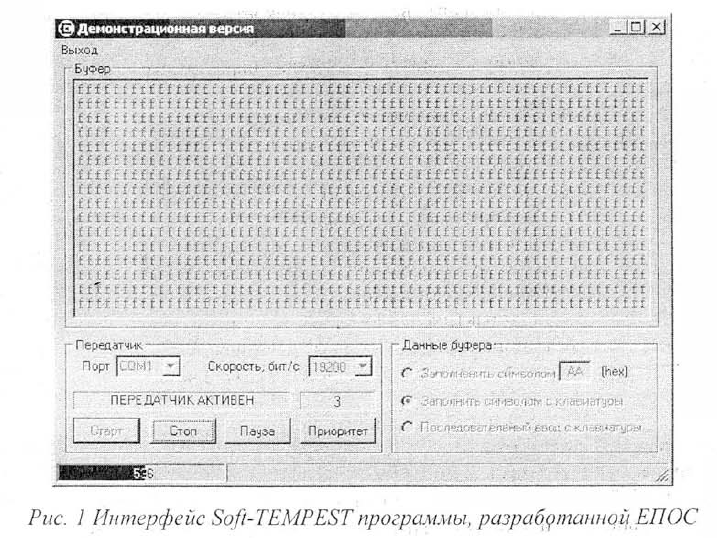


Рис. 2.11.Інтерфейс програми, розробленої ЕПОС (у якості приймача використовувався AR3000A

Ще одним вітчизняним дослідженням було запропоноване виведення та подальше зняття інформації із SATA-інтерфейсу [10, с. 11].

Для демонстрації рівнів випромінювань було використано настільний ПК із жорстким диском Seagate Desktop SSHD, підключений через SATA інтерфейс. Для перехоплення використовується спектроаналізатор Agilent NS30A, повністю синтезований аналізатор спектру з діапазоном частот від 1 кГц до 3 ГГц, фільтри смуг пропускання від 10 Гц до 3 МГц, діапазон вхідних рівнів -110 ... 30 дБм Вт, режим приймача сигналів із ЧМ і АМ демодуляторами, а також антена АІ5-0 розміщена на висоті 1 м і відстані 1 м від системного блоку досліджуваного комп'ютера. У якості ПЗ для формування тест-сигналів використовується ПЗ Sigurd-test, яке генерує меандри на тестований канал, у даному випадку SATA-інтерфейс.

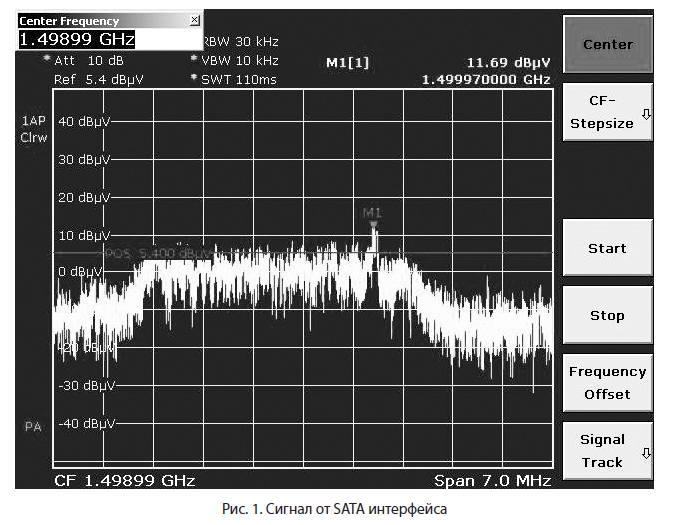


Рис. 2.12. Сигнал, прийнятий від SATA-інтерфейсу [10, с. 11]

У роботі [39, с. 23] та [40, с. 29] представлено дослідження окремих питань, що стосуються SoftTempest, у Японії та Росії, відповідно. У роботі [19, с. 18] запропоновано адаптивну модель для стиснення зображень із використанням квантування хвильових коефіцієнтів, основану на спостереженнях, що чутливість людського ока до шуму у конформних до зображення текстурних компонентах знижується у напрямку до країв.

Нарешті, у роботах [37, с. 5] та [41, с. 7] яскраво продемонстровано, що сучасні дисплеї є не менш, а навіть більш вразливими до застосування SoftTempest:

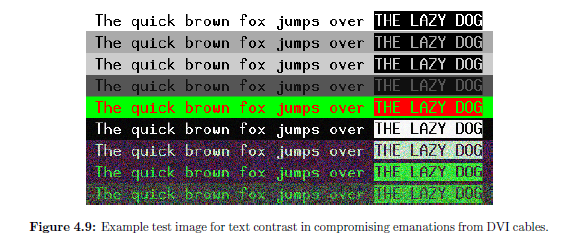


Рис. 2.13. Тестове зображення для контрасту тексту у побічних випромінюваннях від DVI-кабелю

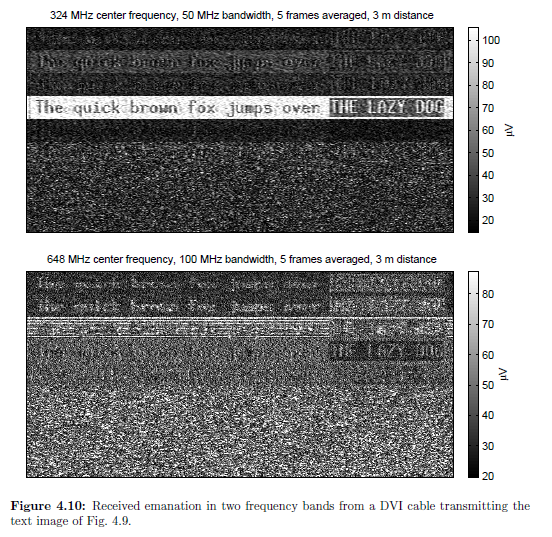


Рис. 2.14. Відповідні зображення на приймачі, отримані від DVI-кабелю

Єдиний запропонований метод протидії, який є достатньо специфічним для цього типу атак, теж базується на використанні різниці в чутливості сприйняття людей і пристроїв.

Пристрій перехоплення, як і зазначалося раніше, приймає із достатньою ефективністю лише високочастотні компоненти сигналу. На рис. Х зображено зонне зображення, яке дозволяє визначити, яка власне частина спектра породжує Tempest-сигнал [36, с. 18]. Вона генерується на основі функції cos(x2+y2), за якої початок системи координат розташований у центрі екрана. У кожній точці цього тестового сигналу локальний спектр має єдиний пік по горизонтальній та вертикальної частоті, пропорційний горизонтальній та вертикальній координатами цієї точки. Даний частотний пік досягає частоти Найквіста для точок на кордоні «зонного» зображення [36, с. 18].

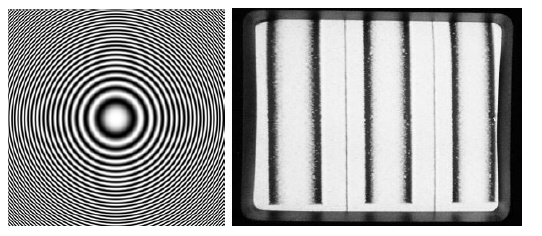


Рис. 2.15. Прийняття випромінювань від тестового «зонного» зображення

Як видно із рис. 2.15, тільки зовнішні 30% «зонного» зображення виглядаються темними на екрані приймача. Тобто, ефективно приймається інформація, представлена у спектрі Фур’є приблизно частотами

(2.6)

У TEMPEST-шрифтах видаляються верхні 30% перетворення Фур'є сигналу (використовується НЧ-фільтр ), що скоріш за все не буде помічено людським оком, зате унеможливлює отримання побічного сигналу, достатньо сильного для ефективної демодуляції.

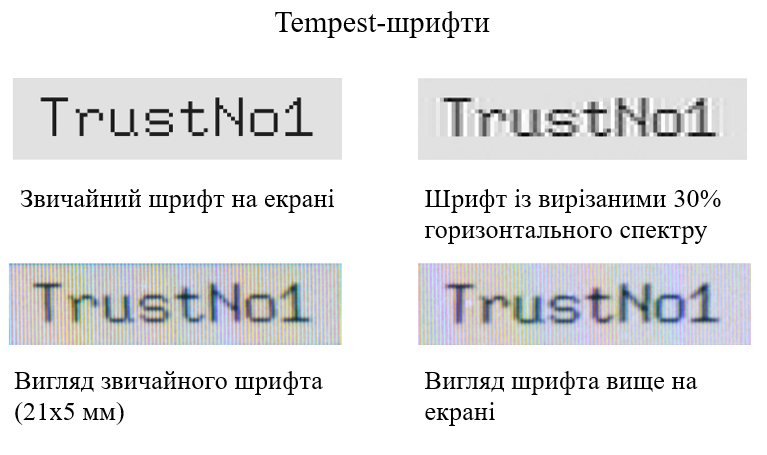


Рис. 2.16. Збільшене зображення звичайних та відфільтрованих Темпест-шрифтів

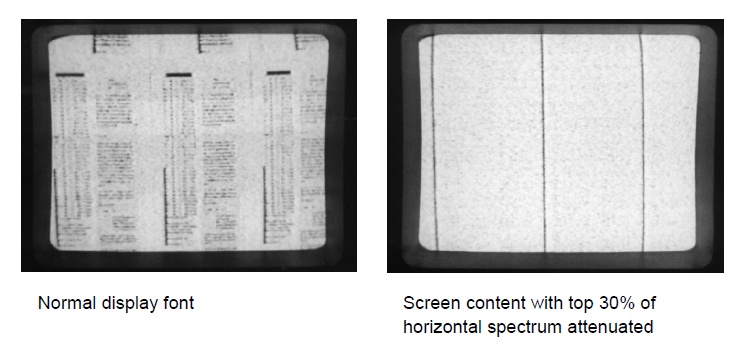


Рис. 2.17. Демонстрація прийняття тексту, створеного Темпест-шрифтом, від CRT-дисплея

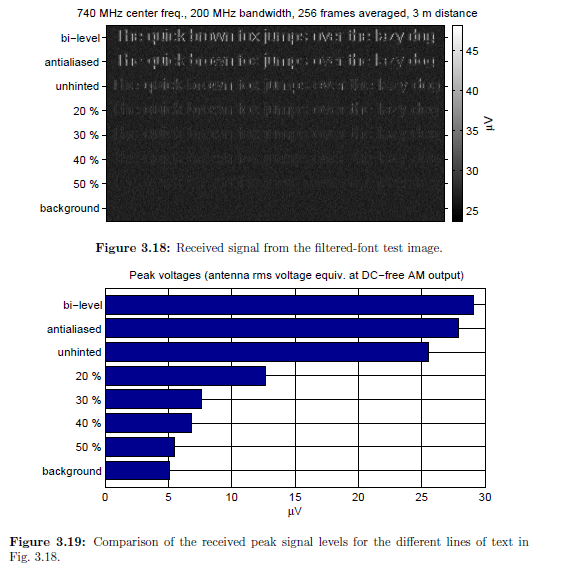


Рис. 2.18. Демонстрація прийняття тексту, написаного Темпест-шрифтом, від DVI-кабелю

Окрім використання Темпест-шрифтів, наразі пропонуються і більш «класичні» рішення, як-от допрацювання засобів обчислювальної техніки, екранування (приміщень та ПК), активне радіотехнічне маскування (енергетичне та неенергетичне) тощо [34, с. 20].

Наявні навіть реальні практичні застосування таких засобів захисту. Наприклад, PGP останніх версій мають опцію SecureViewer, що передбачає використання шрифтів та фону, захищених від Tempest-атак. Іншим продуктом є STEGANOSII, який використовує Темпест-шрифти. Тим не менше, цілком можливо розробити спеціальне обладнання із необхідними параметрами (наприклад, підвищена чутливість до низькочастотних випромінювань), що зробить використання таких шрифтів неефективним [32, с. 15].

Таким чином, огляд стану питання щодо SoftTempest атак демонструє, що наразі не існує засобів протидії із адекватним рівнем захисту, не кажучи про механізми виявлення, яким увагу не приділено взагалі. Тому, одним із завдань даної роботи є розробка програмного засобу із можливостями виявлення та протидії вищезазначеним атакам.

## **2.4.TCP-стеганографія**

На сьогоднішній день, до мережі Інтернет підключено практично кожен комп'ютер у світі, і одним з основних протоколів передачі даних в мережі є TCP. Цілком природно, що використовувати таку величезну мережу можна і для прихованої передачі даних. TCP-стеганографія входить до складу методів під загальною назвою «мережева стеганографія». Мережева стеганографія – вид стеганографії, де в якості контейнерів використовуються мережеві протоколи еталонної моделі OSI. Основними параметрами мережевої стеганографії є пропускна здатність прихованого каналу, ймовірність виявлення та стеганографічна вартість [42, с. 8]. WLAN-стеганографія – частковий випадок мережевої стеганографії; передача стеганограм в бездротових локальних мережах. Прикладом її практичної реалізації є система HICCUPS (Hidden Communication System for Corrupted Networks) [43, с. 10].

У загальному випадку, існують кілька способів прихованої передачі інформації за допомогою протоколу TCP:

* використання особливості повторної відправки пакетів TCP-протоколу;
* зміна властивостей з'єднання;
* використання допоміжних протоколів стека TCP/IP, модифікація пакетів, що відправляються.

Найкраще описати TCP-стеганографічну систему можна за допомогою такого варіанту моделі «проблеми в’язнів» [44, с. 19]. Аліса може вносити довільні модифікації до мережевих пакетів у системі Венді. Вона хоче надіслати повідомлення Бобу, який може лише відслідковувати пакети на виході з мережі, при чому повідомлення повинно бути приховане від Венді. Для прикладу візьмемо сценарій із пасивною атакою (Венді може лише виявляти повідомлення, не маючи змоги їх змінити). Пояснимо це тим, що у більшості випадків застосування активної атаки не видається можливим – фільтрація, необхідна для знищення вбудованої інформації, значною мірою збільшить затримку у мережі, а фільтруючий роутер повинен буде зберігати велику кількість даних конфігурації. До того ж, у такому випадку важко буде приховати відповідні засоби захисту від атакуючої сторони, що може призвести до кращої підготовки до атаки чи пошуку ефективних «обхідних шляхів».

Таким чином, прихований канал, оснований на використанні TCP-стеганографії повинен забезпечувати [44, с. 19]:

* нерозрізнюваність звичайних пакетів та пакетів-контейнерів;
* надійність, тобто Аліса хоче отримувати підтвердження про отримання Бобом повідомлення, аби за необхідності надіслати його повторно.

Формат заголовків пакетів протоколів TCP та IP наведено на Рис. 2.27 [44, с. 19].

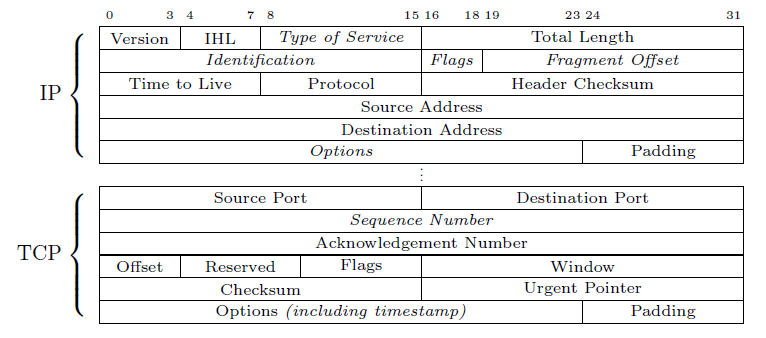


Рис. 2.19. Базова структура заголовків пакетів IP та TCP

Сам по собі протокол IP власне не гарантує надійності передавання, а дозволяє клієнтським протоколам на хості передавати датаграми (блоки даних) від джерела до отримувача. Важливою для стеганографії є можливість фрагментації та об’єднання на приймаючій стороні занадто довгих датаграм, що створює необхідність у додаткових полях заголовка.

TCP забезпечує надійний канал передавання даних. Даний протокол має потоко-орієнтований інтерфейс та не втрачає властивості надійного передавання навіть у мережах із втратою пакетів, зміною порядку передавання та дуплікацією.

TCP та IP заголовки можуть використовуватись для побудови стеганографічної системи лише у тому випадку, коли поля можуть приймати значення, що виглядають легітимними для атакуючої сторони (пакети, згенеровані звичайним для мережі чином, не можна відрізнити від пакетів, створених стеганосистемою). Показники ентропії для значень кожного поля заголовків відрізняються та можуть бути використані для виявлення факту застосування стеганографії [44, с. 19].

Особливістю протоколу TCP є ретрансміссія пакетів у разі їх втрати, що можна використовувати в якості прихованого каналу передачі. Якщо пакет із якихось причин не доходить до одержувача, або доходить, але не в первісному вигляді, протокол відправляє копію цього пакета, яку можна використовувати у якості контейнера для секретних даних. Кількість TCP-з'єднань навіть у середньостатистичного провайдера величезна, а отже, виявити подібні пакети – вкрай непросте завдання. Втім варто зауважити, що ретрансміссія відбувається лише як наслідок втрати пакету, кількість таких випадків незрівнянно менша за кількість звичайних TCP-запитів, що робить ідентифікацію відправленого пакета посильною задачею. Зменшити ймовірність виявлення подібного каналу можливо за рахунок зменшення його пропускної спроможності до одного біта в секунду, що зменшить кількість виконуваних ретрансміссій; це дозволить приховати секретний канал під більш високошвидкісними каналами [42, с. 8].

Зміна властивостей TCP-з'єднань також складає один із можливих методів прихованої передачі інформації. Використання таких методів як:

* зміна затримки між переданими пакетами;
* зміна порядку проходження переданих пакетів;
* навмисне скидання деяких пакетів

дозволяє передавати секретні дані, використовуючи стандартні засоби мережі та TCP-протоколу.

Модифікація полів заголовків пакету можлива за рахунок надмірності в даних полях, яка дозволяє визначити, що в інформація даного поля не використовується при передачі пакета, отже, її можна використовувати в якості стеганографічного контейнера. Наприклад, значення поля «Ідентифікатор пакету» генерується під час пересилання і містить в собі випадковий номер. Поле використовується лише за проведення фрагментації пакета, отже для побудови каналу необхідно знати MTU в мережі, аби пакет не був фрагментований під час передачі. За відсутності фрагментації надмірність виникає в полі «Прапори», а саме у другому біті, де можливо виставити значення DF, «Don’t Fragment». Передача подібним методом забезпечує збереження інформації, хоч і значно зменшує кількість переданої інформації [45, с. 17].

Використання ICMP для передачі інформації також працює за подібним принципом. ICMP – мережевий протокол, що входить до складу стека TCP/IP і використовується для передачі повідомлень про помилки або виняткові ситуації при передачі даних. Саме на ньому працюють ping та traceroute. Структура пакета ICMP\_ECHO\_REPLY утиліти ping, тобто пакета «відповіді», містить зарезервовані поля, які зазвичай заповнюються нулями і не впливають на процес передачі пакета. Такі поля, як приклад, можуть використовуватись у якості контейнера у мережевій стеганографічній системі [46, с. 21].

Наразі продовжуються оптимізація існуючих та пошуки нових алгоритмів стеганографічного вбудовування даних на рівні протоколів стеку TCP/IP. Тим не менше, стеганографічний аналіз також не стоїть на місці, триває пошук «слабких місць» вищевказаних алгоритмів та способів їх використання.

У роботі [44, с. 19] наведено теоретичне обґрунтування незахищеності вбудованої у заголовки пакетів інформації. Це пояснюється тим, що залежно від операційної системи, заголовки пакетів містять все ж доволі передбачувані показники полів, для яких розраховано значення ентропії. Фактично, для вбудовування підходять усі рівні стеку протоколів, і для кожного розроблено низку відповідних алгоритмів, що і наведено у численних роботах.

Практичну реалізацію алгоритму, що використовує вбудовування на фізичному рівні, представлено у [43, с. 10]. Такий підхід вимагає контролю над апаратним забезпеченням на низькому рівні. До того ж, на вищих рівнях мережі не складе проблеми виявити та зупинити повідомлення про отримання.

Роботу [47, с. 17] присвячено використанню особливостей IPv6 для побудови мережевих стеганографічних систем. Наведено «слабкі місця» запропонованого підходу, а також пропозиції щодо подальших досліджень.

Як було сказано вище, допоки розглядалися системи із пасивним порушником. У роботах [48, с. 3] та [49, с. 2] наведено модель із активною атакуючою стороною, виконано розрахунок ймовірнісних параметрів атаки. У результаті наведено алгоритм, який дозволяє знищити більшість вбудованої інформації, а іноді і повністю відновити початковий стан контейнера, без ушкодження пакету та його заголовку. При цьому питання низькорівневої мережевої стеганографії вирішується стандартною маршрутизацією.

У роботі [50, с. 12] детально розглянуто можливості використання прапорів DF та MFIP-пакетів. Тим не менше, варто зауважити, що нормальний стан DF легко передбачити з контексту пакету, що може бути застосовано для виявлення факту застосування стеганографії. У тій самій роботі відмічено можливість зміни порядку пакетів за використання мережі IPSec (володіє властивістю відновлювати коректний порядок переданих пакетів). Проте, знову-таки, виявити таку атаку не стане значною проблемою, оскільки порядок пакетів у трафіку у більшості випадків залишається стабільним або змінюється незначною мірою. Таким чином, перестановка пакетів за стеганографічним алгоритмом буде помітною для стороннього спостерігача, якщо він має підозри щодо застосування стеганографії у мережі.

TCP-стеганографія є, безперечно, потужним засобом забезпечення секретності інформації. Втім, за аналогією із технологією SoftTempest, дані методи можуть застосовуватися в кібератаках на інформаційно-телекомунікаційні системи.

З точки зору моделі «проблеми в’язнів», Аліса та Боб тут виступають одним суб’єктом – ініціатором атаки. Дана сторона у розрізі атаки отримує короткочасний доступ до системи, вхідний та вихідний трафік якої жорстко контролюється. Із використанням будь-якої відомої технології (наприклад, keylogger) відбувається пошук та отримання цінної інформації, найчастіше паролів, ключових даних тощо. Далі необхідним кроком є виведення інформації із системи так, що власник системи не помітить злочинної активності, навіть за наявності засобів моніторингу у мережі. На цьому етапі і застосовується стеганографічне вбудовування даних на рівні TCP/IP.

Головним чином, придатність даних методів для атаки визначається використанням мережевого з’єднання, наявного у більшості систем, та можливістю виведення інформації із системи так, що навіть аналізатор трафіку не зможе виявити канал передавання. Це зумовлено тим, що фактично, не відбувається передавання додаткових даних-контейнерів, а використовуються вже наявні пакети, що циркулюють мережею і так чи інакше виходять з неї.

## **Висновок до розділу**

Технології SoftTempest присвячено перший модуль програми. Оскільки основа атаки носить програмний характер (навіть назва може трактуватися як «програмний ПЕМВН»), то і «слабкі місця» варто розглядати такі, які притаманні більшості програмних реалізацій атак на системи. Для проведення атаки необхідним є модифікація певних файлів конфігурації за певними значеннями, як було зазначено раніше. Таким чином, у якості засобу виявлення пропонується алгоритм пошуку ПЗ, у коді якого міститься звертання до переліку файлів із подальшою зміною відповідного переліку параметрів у заданих діапазонах, а також перевірка вищезазначених файлів вже на наявність таких змін. Щодо протидії, розповсюдженим методом протидії витоку через ПЕМВН є зашумлення. За аналогією для «програмного» ПЕМВН пропонується програмне зашумлення. При факті виявлення атаки, запускається модуль, який модифікує параметри дізерингу тим самим шляхом, що і проводиться атака, але змінює параметри так, що окремі знаки стають нерозрізнюваними та непридатними для приймання.

У якості засобу виявлення атак, які використовують TCP-стеганографію, пропонується окремий модуль програмного продукту, отриманого у результаті даної роботи.

Кожна операційна система має цілком специфічні характеристики згенерованих полів TCP/IP. Вони можуть бути використані для виявлення будь-яких аномалій, що слугують показником потенційного використання стеганографії. Другий модуль програми містить тести, які можуть бути застосовані до мережевих дампів для порівняння на співпадіння із характерними для ОС показниками. У першу чергу, ці тести сконцентровані на властивостях таких параметрів, як IPID, TCP прапори та часові мітки TCP.

**РОЗДІЛ 3.** **РОЗРОБКА ЗАСОБІВ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ**

**3.1.Розробка засобу протидії атаці із використанням Soft Tempest**

У даному розділі пропонується алгоритм обробки зображення на моніторі таким чином, що прийом інформації за допомогою атаки із використанням Soft Tempest стане неможливим з причин, описаних далі. Алгоритм імплементовано у вигляді програмного модуля на мові програмування C. Даний модуль може бути використаний у комплексному засобі захисту від вищезазначеної атаки, що також буде описано у розділі.

У загальному вигляді, пропонується створити програмний засіб, який дозволяв би як виявлення, так і протидію атаці, що розглядається. У даній роботі наведено розроблений алгоритм для протидії, а також загальні принципи та рекомендації щодо алгоритму виявлення, що є питанням подальшої роботи.

Варто ще раз зазначити, звідки можна отримати високочастотний сигнал, що містить зображення з монітора для сучасних технологій екранів.

У якості прикладу можна навести той факт, що у сучасних моніторів кабелями, візьмемо VGA як найчастіший випадок, передається як відеовивід, так і безліч службових пакетів. Найчастіше, управління службовими параметрами монітора реалізовано через шину I2C, сигнал від неї знаходиться на рівні 100 кГц. Іншим варіантом є майже будь-який послідовний порт, який, навіть коли до нього нічого не підключено, випромінює в ефір, і змінюючи швидкість передавання даних на порт, можна отримати на окремих частотах значне перевищення рівня випромінювання порту над рівнем випромінювання інших елементів комп’ютера. Якщо ж до порту підключено який-небудь пристрій, то сполучний кабель відіграє роль антени. У такому разі рівень випромінювання достатній навіть для прийняття апаратурою із дуже слабкими характеристиками.

Отже, розпочнемо із алгоритму протидії. Загальна ідея пропонованого підходу, природньо, витікає з принципів самої атаки. Як було зазначено у попередніх розділах, технологія SoftTempest полягає у стеганографічному вбудовуванні секретної інформації у зображення на екрані шляхом модифікації паттернів дізерингу таким чином, що для оператора зображення не зміниться, а чутливості середньостатистичного приймача та іншої відповідної апаратури вистачить для отримання та відповідної обробки зовсім іншого сигналу, що випромінюється в ефір. Можливість виведення різних зображень існує через різницю чутливості сприйняття у людей та приймачів випромінювання: люди нечутливі у високочастотній смузі, та навпаки, як експериментально доведено у [36, с. 18], достатній для сприйняття немодифікованим приймачем сигнал отримується лише з верхніх 30% спектру (Фур’є-сигналу).

З цього випливає два висновки, необхідні для атакуючої сторони:

* для людського ока не дуже важливо, чи буде масив пікселів виставлений однотонним кольором певного значення у доступній палітрі, чи чергуванням двох кольорів відповідних характеристик, що дадуть ідентичний колір у сумі;
* чим більший контраст кольорів, що чергуються, тим краще сприймається сигнал приймачем.

Істинність другого твердження доведено експериментально в [36, с. 18], при чому, наприклад, чергування чорного та червоного, чорного та синього й чорного та зеленого давали близькі за відтінками «темні» значення на приймачі, а чергування жовтого та зеленого – значно світліші (менш придатні для сприймання).

Аби пояснити цей феномен, необхідно звернути увагу на кілька понять з теорії обробки кольору та їх математичне представлення [9, 51]:

1. Колірний простір – модель представлення кольору, заснована на використанні колірних координат.
2. Колірна модель – абстрактна модель опису представлення кольорів у вигляді кортежів (наборів) чисел, зазвичай з трьох або чотирьох значень, званих колірними компонентами або колірними координатами, множина кольорів колірної моделі та метод інтерпретації цих даних визначають колірний простір.
3. Тон (Hue) – чисельно визначається довжиною хвилі домінуючого чистого спектрального кольору (монохромного випромінювання, що у змішуванні з білим дає колір); якщо на круговій діаграмі розташувати чистий червоний на 0°, зелений на 120°, а синій на 240°, то тон окремої точки всередині діаграми становитиме .
4. Насиченість (Saturation) – властивість кольору, що виражає ступінь його відмінності від ахроматичного (сірого) кольору тієї ж яскравості, забезпечується вмістом чистого тону, чисельно обумовлена відношенням яскравості домінуючого спектрального кольору до повної яскравості суміші (мінімальна для білого кольору); становить 0, якщо R = G = B, якщо світність L< 128, то 255 \* (M - m) / (M + m), в інших випадках 255 \* (M - m) / (511 - (M + m)).
5. Яскравість (Luminance) – світлова характеристика тіл-джерел світла, що визначається силою світла на одиницю площі для потоку в даному напрямі; фактично, описує кількість світла, що проходить, випромінюється чи відбивається від конкретної поверхні, та попадає у площу проекції сили світла в площині, перпендикулярній напряму спостереження; визначається як , де – світловий потік, – елемент площі поверхні, – елемент кута, – кут між напрямком до спостерігача та нормаллю до поверхні.
6. Світність (Luminosity) – характеризується інтенсивністю світлового потоку, що випромінюється одиницею площі джерела (випромінює, відбиває або пропускає світловий потік) в усіх напрямках; , де – світловий потік, що випромінюється з площі .
7. Хроматичність (тональність, колірність) (Chromaticity) – об’єктивна характеристика чистоти кольору незалежно від його світності (часто використовується як синонім насиченості, проте насправді є поєднанням насиченості та тону); нейтральною точкою відліку вважається так звана «біла точка» діаграм колірних моделей, усі інші значення розраховуються відносно полярних координат точок та враховуючи особливості моделей; фактично, тон є кутовим компонентом, а чистота тону – радіальним компонентом, нормалізованим максимальним радіусом для даного тону.
8. Відносна спектральна світлова ефективність (Relativeluminosity) – фотометрична світність, нормалізована значеннями у діапазоні від 0 до 100 (іноді від 1 до 100); наприклад, у колірних моделях XYZ, xyZ тощоY власне і позначає «відносну світність». Для колірних просторівRGB (у першу чергу, sRGB як найбільш широковживаного) стандарт [51, с. 7] визначає необхідність конвертувати гамма-корректовані значення до лінійних значень, а тоді

(3.1)

для інших моделей відмінний розрахунок хроматичності вимагає відмінних коефіцієнтів.

Перелічені поняття розглядатимуться надалі у розрізі використання колірної моделі sRGB та колірного простору CIE 1931, оскільки саме дані системи є наразі найбільш широковживаними у сфері цифрової обробки кольору.

sRGB (англ. standartRedGreenBlue) — стандарт подання колірного спектру з використанням моделі RGB, створений спільно компаніями HP та Microsoft у 1996 році для уніфікації використання моделі RGB в моніторах, принтерах та на інтернет-сайтах [51, с. 7]. Варто зазначити, що гамма тут не може бути виражена одним числовим значенням, оскільки функція коррекції складається з лінійної частини ближче до чорного (гамма становить 1) та нелінійної до значення 2,4 включно.

CIE 1931 є стандартом, що поєднує розподіл довжин хвиль у видимому спектрі електромагнітних випромінювань та кольорами, які фізіологічно здатна сприймати зорова система людини. Гамма для CIERGB наведена на рис. 3.1.

Пояснюючи простішими словами, кожна з колірних компонент (червона, зелена та синя) кодується, як відомо, 8-ма бітами, і отримані значення можна привести у відповідність із тоном, насиченістю та світністю (яскравістю), а саме:

* насиченість визначається значенням від 0 до 255 для кожної з колірних компонент;
* тон визначається пропорційним відношенням значень компонент одна до одної;
* світність вираховується за формулою (3.1).

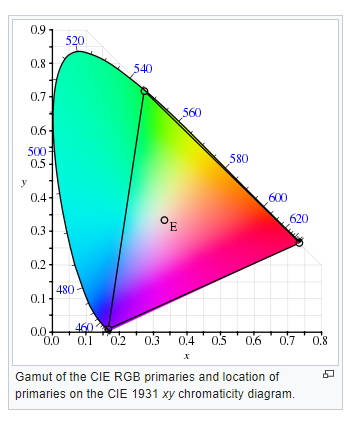


Рис. 3.1. Діаграма хроматичності та гамма CIERGB[45, с. 17]

Такі три параметри можна вирахувати для кожного пікселя, проте нам необхідно перейти до базису ПЕМВН. Людина сприймає кольорове зображення, а приймач ПЕМВН – у градієнтній шкалі від чорного до білого, при чому більший контраст між кольорами дає темніший відтінок сірого (фактично, дві палітри, що формуються за різними параметрами). Тобто, система зору людини за допомогою рецепторів дозволяє сприймати як яскравість тонів, так і відношення між ними, а приймальна техніка – тільки загальну яскравість без значень пропорцій компонент, якими вона була складена. Тому, надалі оперуватимемо лише двома поняттями – хроматичністю та світністю. При чому, мова йтиме як для параметрів окремих пікселів, так і для комплексних значень для їх комбінацій.

Фактично, сутність атаки полягає лишень у таких моментах:

* необхідно вбудувати зображення в інше зображення, маніпулюючи дізерингом;
* для кожного окремо взятого блоку зображення необхідно зберегти загальні значення хроматичності та світності;
* поки попереднє виконується, зовсім не важливо, у якій саме пропорції (за умови точних математичних розрахунків) кілька різних значень пікселів формують загальні значення блоку;
* світності окремих пікселів повинні мати якомога більшу різницю, себто давати найбільший контраст.

З вищезазначеного зроблено наступні висновки, що лежать в основі запропонованого підходу протидії:

* для того, аби користувач не помітив втручання програми та міг продовжувати роботу, початкові значення хроматичності та світності для блоку повинні залишитися незмінними;
* пропорції окремих пікселів все ще не маються значення для законного користувача, якщо виконується попередня умова;
* контраст між світностями пікселів необхідно звести до мінімуму, що дасть найгірший для приймача сигнал при збереженні зображення на екрані.

У даній роботі ми розглядатимемо найпростіший алгоритм дізерингу зображення – чергування двох кольорів у шаховому порядку без розподілу помилки кодування на сусідні пікселі.

Для подальшої роботи введемо позначення параметрів. Деякі значення отримуються із зображення та можуть незалежно змінюватись, в той час як інші від них залежать або мають постійні величини:

* параметри, що стосуються людського ока, позначатимемо з індексом A;
* параметри, що стосуються приймача, позначатимемо з індексомB;
* p1та p2 – пікселі, що формують шаховий паттерн;
* та – значення колірних компонент пікселів p1та p2 відповідно;
* ch1та ch2 – хроматичність для p1та p2 відповідно;
* l1та l2 – світність для p1та p2 відповідно;
* C – значення контрасту між p1та p2; formula Michelson definition (l normalized, so we are looking for 0,7 and less)
* та - значення колірних компонент після, які є метою модифікації, тобто такі, які необхідно отримати.

Для простішого досягнення наочності, оперуватимемо за припущення, що атакуючою стороною зображення розбивається на блоки 2х2 пікселі та маніпулюється відповідно. Алгоритм, необхідний для розрахунку та модифікації зображення монітору, що пропонується у даній дипломній роботі, наступний:

1. Отримати зображення, виведене у певний момент часу на екран.
2. Отримати значення колірних компонент, для чого:
   1. розбити зображення на блоки 2х2 пікселі;
   2. оскільки вважаємо, що застосовано найпростіший шаховий паттерн дізерингу, вирізнити перший та другий пікселі першого рядка;
   3. отримати значення та .
3. Вирахувати l1, та l2, нормовані в діапазоні 0…100:
4. Вирахувати загальну хроматичність, яку дає змішування кольорів :
5. Вирахувати загальну світність, що отримується lA=lB:
6. За даних значень пунктів 4 та 5, знайти таку комбінацію та , що значення відповідних колірних компонент попарно дають найменший контраст:
   1. – цілі значення?
   2. якщо так, то та приймають значення ;
   3. якщо ні, то , .
7. Контраст становить 0 у разі виконання умови 6ab() та у разі виконання умови 6c.

Звичайно, досягнення нульового контрасту не є абсолютно необхідною умовою, достатнім є перехід порогового значення. У [36, с. 18] експериментально визначено, що безпечними є 0,7 спектру сигналу, і можна було б розрахувати поріг контрасту та знижувати і підвищувати світність пікселів зі збереженням пропорцій, аж допоки не буде отримано необхідне значення. Тим не менше, існує ряд моментів, які роблять такий підхід неприйнятним. По-перше, це не є ефективним з точки зору обчислень (запропонований вище алгоритм вимагає значно менше математичних операцій). По-друге, сучасніше та просто потужніше обладнання може дозволити отримати сигнал і поза заданими межами. Запропонований же алгоритм дозволяє не зважати на можливості приймача, оскільки контраст світностей результуючих пікселів дорівнює нулю або прямує до нього.

У Додатку А міститься модуль коду на мові програмування С, що імплементує вищезазначений алгоритм.

Звичайно, оскільки атакуючий працює із якнайвищими контрастами пікселів, що чергуються, значно найпростішим рішенням проблеми витоку було б не опрацьовувати кожен піксель зображення, а усереднити їх до розрахованих значень, що гарантовано знизять контраст. Тобто, йдеться мова про такий алгоритм:

* розбити спектр світностей навпіл – (-L;0), (0;L);
* за допомогою одного знімку зображення на моніторі можна визначити, яку послідовність вбудовування використовує атакуючий – темний/світлий чи світлий/темний пікселі (навряд чи буде змінюватись, оскільки ускладнить автоматизацію процесу для атакуючого);
* для темних пікселів обирається величина –L/2, для світлих – L/2.

Просто виконати примусову «заливку» екрана одним кольором не буде ефективним рішенням через те, що атакуючий все одно зможе подолати бар’єр контрасту, принаймні із деякими кольорами.

Тим не менше, такий підхід хоч і максимально усереднить усі можливі значення світностей, його результатом буде повне спотворення зображення на екрані комп’ютера. Завданням же даної роботи було розробити такий алгоритм, що залишиться у рамках класичної постановки задачі стеганографії та дозволить законному користувачу продовжувати роботу, навіть одночасно із роботою модуля «зашумлення».

Отже, запропонований підхід дозволяє, не припиняючи роботу оператора, гнучко провести «зашумлення» сигналу витоку та унеможливити отримання секретної інформації.

**3.2. Розробка засобу виявлення атаки із використанням TCP-стеганографії**

У даному розділі міститься опис роботи щодо розробки програмного засобу виявлення каналу передавання, основаного на методах TCP-стеганографії.

Сутність алгоритму виявлення полягає у тому, що не дивлячись на відому стеганоспільноті надмірність, поля пакетів у протоколах TCP та IP генеруються певним цілком визначеним чином для кожної операційної системи, а точніше сімейств їх версій. Порушення деяких характеристик може і не призвести до втрати пакета чи взагалі припинення передавання, проте яскраво сигналізує про втручання у початкові установки генерації трафіку. Таким чином, аналіз трафіку на наявність подібних неспівпадінь довзолить з певною мірою ймовірності визначити факт проведення TCP-стеганографічної атаки.

Параметрами до розгляду було прийнято поля TCP та IP пакетів, які мають найкращі показники у прихованому передаванні даних (згідно із розглянутими науковими працями, присвяченими цьому питанню) та, як результат, найчастіше використовуються для створення стеганографічного каналу, а саме:

* IP ID;
* IP Flags;
* TCP URG;
* IP ToS;
* TCP RST;
* TCP Timestamp.

Відповідно для них визначено такі принципи стеганографічного вбудовування даних:

* IPID: ASCII-коди літер прихованого тексту множаться на 256 та виставляються у полі (проведення фрагментації ніяк не вплинена передавання, оскільки залежить від кінцевого розміру пакета, а не окремого значення IPID);
* IPFlags: стосується прапорів Fragmentation – у нефрагментованій датаграмі MoreFragment (MF), DoNotFragment (DF) та FragmentOffset встановлені у 0; використання DF (010 для “1” та 000 для “0”) та FragmentOffset дозволяє передавати 17 біт на пакет при генерації пакетів, менших за MTU (8 старших біт за замовчуванням вважається найбільш прийнятною практикою);
* TCPURG: прапор URG у TCPFlags встановлюється у 0, а дані записуються до UrgentPointer (не розглядається при відсутності встановленого прапора);
* IPTypeofService: використання деяких із доступних значень за розсудом атакуючого (наразі навіть просто встановлення цього значення є рідкісним та суто спеціалізованим явищем);
* TCPTimestamp: модифікація міток часу у пакеті;
* TCPRST: встановлення прапора в 1 та вбудовування даних до поля Payload – пакет ігноруватиметься, втім, його можна простежити та отримати вбудовані дані.

Системою для проведення експерименту біло обрано ManjaroLinux на ядрі Linux 4.14.66-1.

Задля демонстрації тестового трафіку без наявних вбудованих даних, було застосовано команди утиліт ОС Linuxsendip та tcpdump (паралельне виконання, обмежене замкненим циклом localloop задля безпеки проведення експерименту):

* sendip -p ipv4 -is 192.68.102.1 127.0.0.1
* sudo tcpdump -i lo -vv -c 10 >> trafficDump.txt

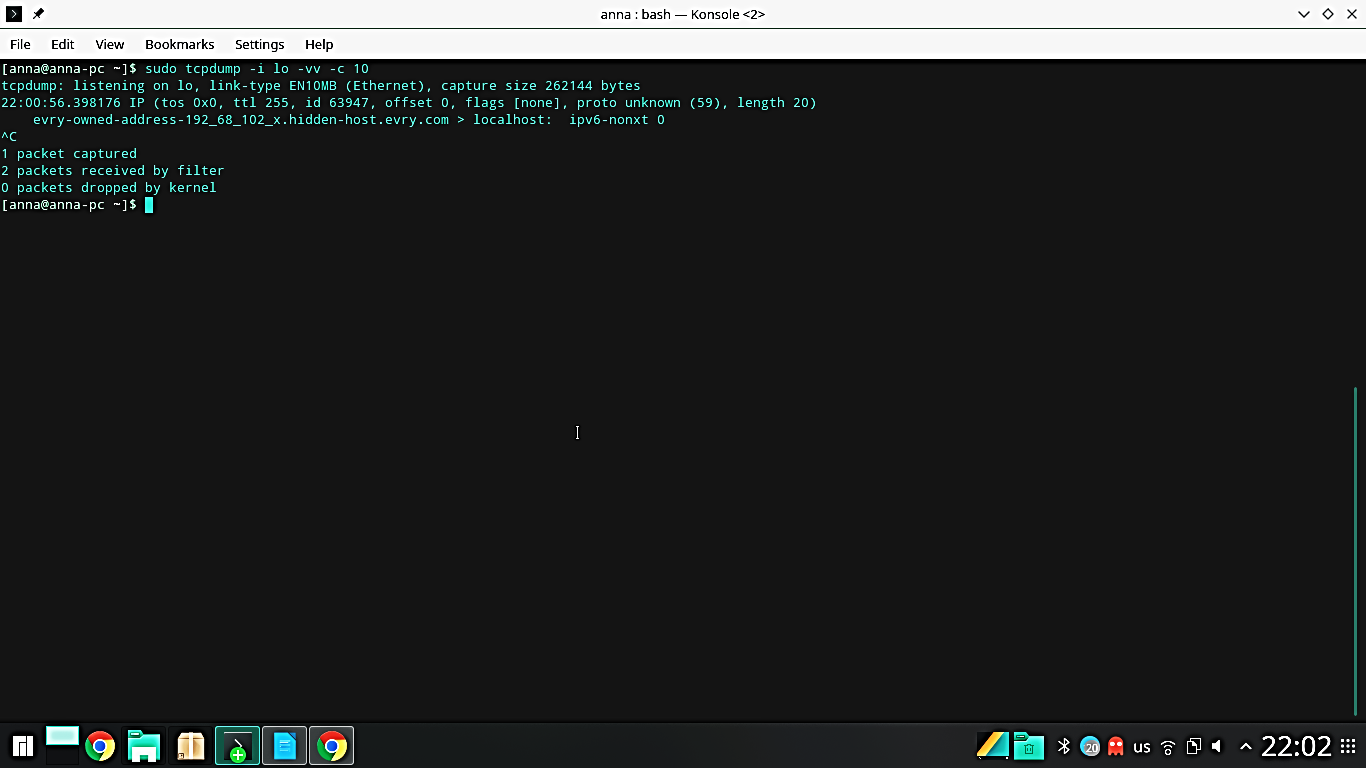


Рис. 3.2.Приклад тестового “чистого” трафіку із обмеженням по кількості пакетів до 5-ти з sendip

Наразі існують готові програмні рішення, які реалізують стеганографічне TCP-вбудовування, наприклад,covert-tcp[44, с. 19]. Ти не менше, заради безпеки проведення тест, було вирішено згенерувати необхідний трафік самостійно із застосуванням утиліти ОС Linuxsendip.

Отримано такий трафік:

22:03:26.368240 IP (tos 0xc0, ttl 64, id 7320, offset 0, flags [none], protoICMP (1), length 88)

anna-pc.local>anna-pc.local: ICMPhostapollo.archlinux.orgunreachable, length 68

IP (tos 0x0, ttl 64, id 28797, offset 0, flags [DF], proto TCP (6), length 60)

anna-pc.local.56236> apollo.archlinux.org.http: Flags [S], cksum 0x9ed0 (incorrect -> 0x21fd), seq 1435672098, win 29200, options [mss 1460,sackOK,TS val 4170272013 ecr 0,nop,wscale 7], length 0

22:03:30.421652 IP (tos 0xc0, ttl 64, id 7708, offset 0, flags [none], proto ICMP (1), length 88)

anna-pc.local> anna-pc.local: ICMP host apollo.archlinux.org unreachable, length 68

IP (tos 0x0, ttl 64, id 28798, offset 0, flags [DF], proto TCP (6), length 60)

anna-pc.local.56236> apollo.archlinux.org.http: Flags [S], cksum 0x9ed0 (incorrect -> 0x1228), seq 1435672098, win 29200, options [mss 1460,sackOK,TS val 4170276066 ecr 0,nop,wscale 7], length 0

22:03:31.647418 IP (tos 0x0, ttl 255, id 10332, offset 0, flags [none], proto unknown (59), length 20)

evry-owned-address-192\_68\_102\_x.hidden-host.evry.com > localhost: ipv6-nonxt 0

22:03:38.528511 IP (tos 0xc0, ttl 64, id 9957, offset 0, flags [none], proto ICMP (1), length 88)

anna-pc.local> anna-pc.local: ICMP host apollo.archlinux.org unreachable, length 68

IP (tos 0x0, ttl 64, id 28799, offset 0, flags [DF], proto TCP (6), length 60)

anna-pc.local.56236> apollo.archlinux.org.http: Flags [S], cksum 0x9ed0 (incorrect -> 0xf27c), seq 1435672098, win 29200, options [mss 1460,sackOK,TS val 4170284173 ecr 0,nop,wscale 7], length 0

22:03:52.851107 IP (tos 0x0, ttl 255, id 38730, offset 0, flags [none], proto unknown (59), length 20)

evry-owned-address-192\_68\_102\_x.hidden-host.evry.com > localhost: ipv6-nonxt 0

Базуючись на стеганографічних алгоритмах, зазначених вище, можна виділити закономірності, порушення яких сигналізуватимуть про факт використання прихованого каналу. Наведені далі “сценарії” послугували основою для тестів, спрямованих на виявлення застосування стеганографії:

* IPID: ділення на 256 дає послідовні значення, що лежать в діапазоні ASCII-кодів (переведення видасть літерне значення);
* IPFlags (Fragmentation): DF встановлено в 1, тоді як MF та Offset ні, а поле Fragmentoffset заповнене не нульовими значеннями;
* TCPURGPointer: прапор URG встановлено у 0, а поле Urgentpointer містить ненульове значення;
* IPTypeofService: ненульове значення або заповнене все поле;
* TCPTimestamp: відношення різних значень міток часу до різниці між значеннями початкової та кінцевої міток становить близько 0,75 (без вбудовування близько 1) [44, с. 19];
* TCPRST: прапор RST встановлено в 1, а дані пакету становлять ненульові значення.

Тестовий трафік задано за допомогою команд sendip -p ipv4 -ii 19200 127.0.0.1, sendip -p ipv4 -ii 16896 127.0.0.1, sendip -p ipv4 -ii 23040 127.0.0.1, sendip -p ipv4 -ii 18688 127.0.0.1. Як видно з команди, задля тестування було впроваджено алгоритми із вбудовуванням за допомогою IP ID. Тестові пакети із застосуванням стеганографії дають такий вигляд трафіку:

10:15:10.952580 IP (tos 0x0, ttl 255, id 19200, offset 0, flags [none], proto unknown (59), length 20)

localhost > localhost: ipv6-nonxt 0

10:15:10.952606 IP (tos 0xc0, ttl 64, id 55287, offset 0, flags [none], proto ICMP (1), length 48)

localhost > localhost: ICMP localhost protocol 59 unreachable, length 28

10:15:33.811880 IP (tos 0x0, ttl 255, id 16896, offset 0, flags [none], proto unknown (59), length 20)

localhost > localhost: ipv6-nonxt 0

10:15:33.811927 IP (tos 0xc0, ttl 64, id 61788, offset 0, flags [none], proto ICMP (1), length 48)

localhost > localhost: ICMP localhost protocol 59 unreachable, length 28

10:15:51.879709 IP (tos 0x0, ttl 255, id 23040, offset 0, flags [none], proto unknown (59), length 20)

localhost > localhost: ipv6-nonxt 0

10:15:51.879777 IP (tos 0xc0, ttl 64, id 61963, offset 0, flags [none], proto ICMP (1), length 48)

localhost > localhost: ICMP localhost protocol 59 unreachable, length 28

10:16:06.725318 IP (tos 0x0, ttl 255, id 18688, offset 0, flags [none], proto unknown (59), length 20)

localhost > localhost: ipv6-nonxt 0

10:16:06.725347 IP (tos 0xc0, ttl 64, id 64323, offset 0, flags [none], proto ICMP (1), length 48)

localhost > localhost: ICMP localhost protocol 59 unreachable, length 28

Зметоювиявленняданихзакономірностейбулоствореноскрипт, якийпроводитьтестинакоженізвказанихметодівTCP-стеганографії. У даній роботі представлено скрипт, який працює із записаним у файл дампом трафіку. Надалі можлива модифікація така, що скрипт працюватиме із дампами у реальному часі. Код наведено у Додатку Б.

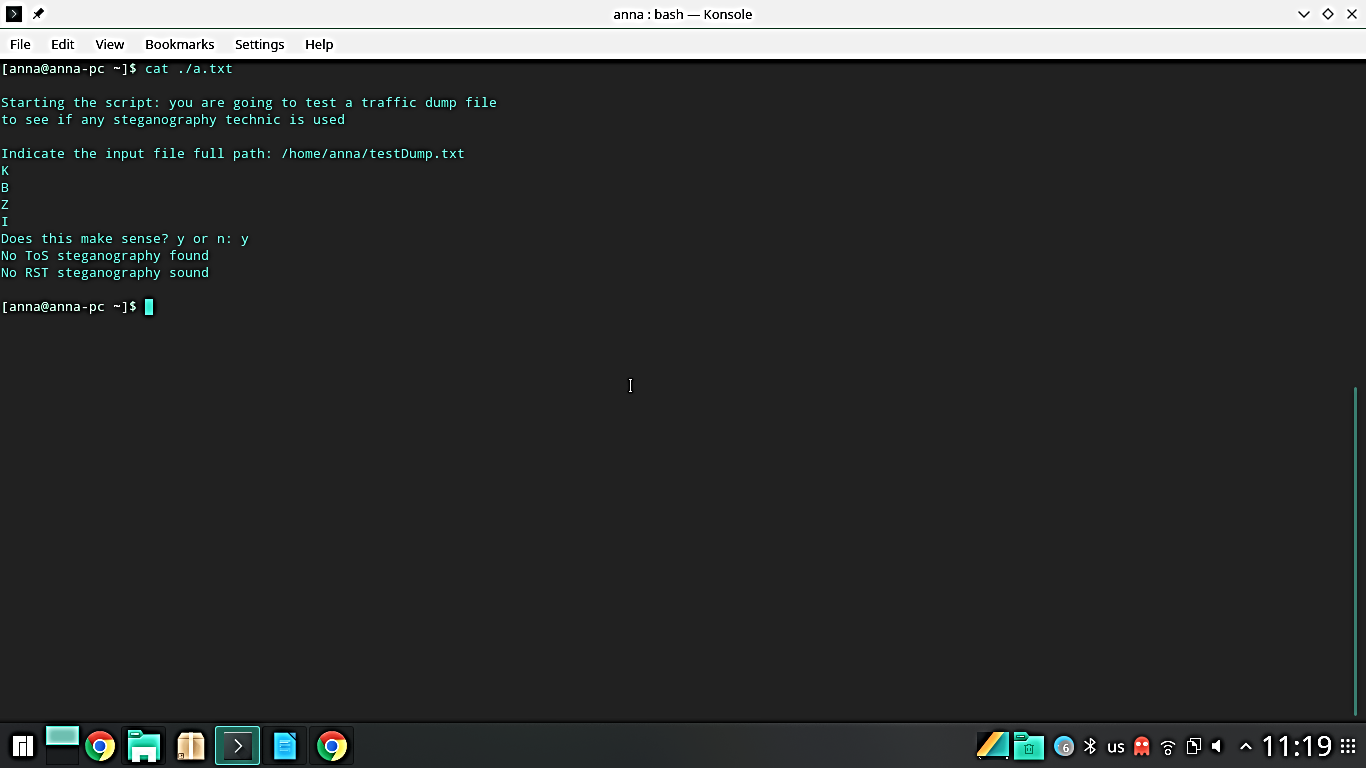
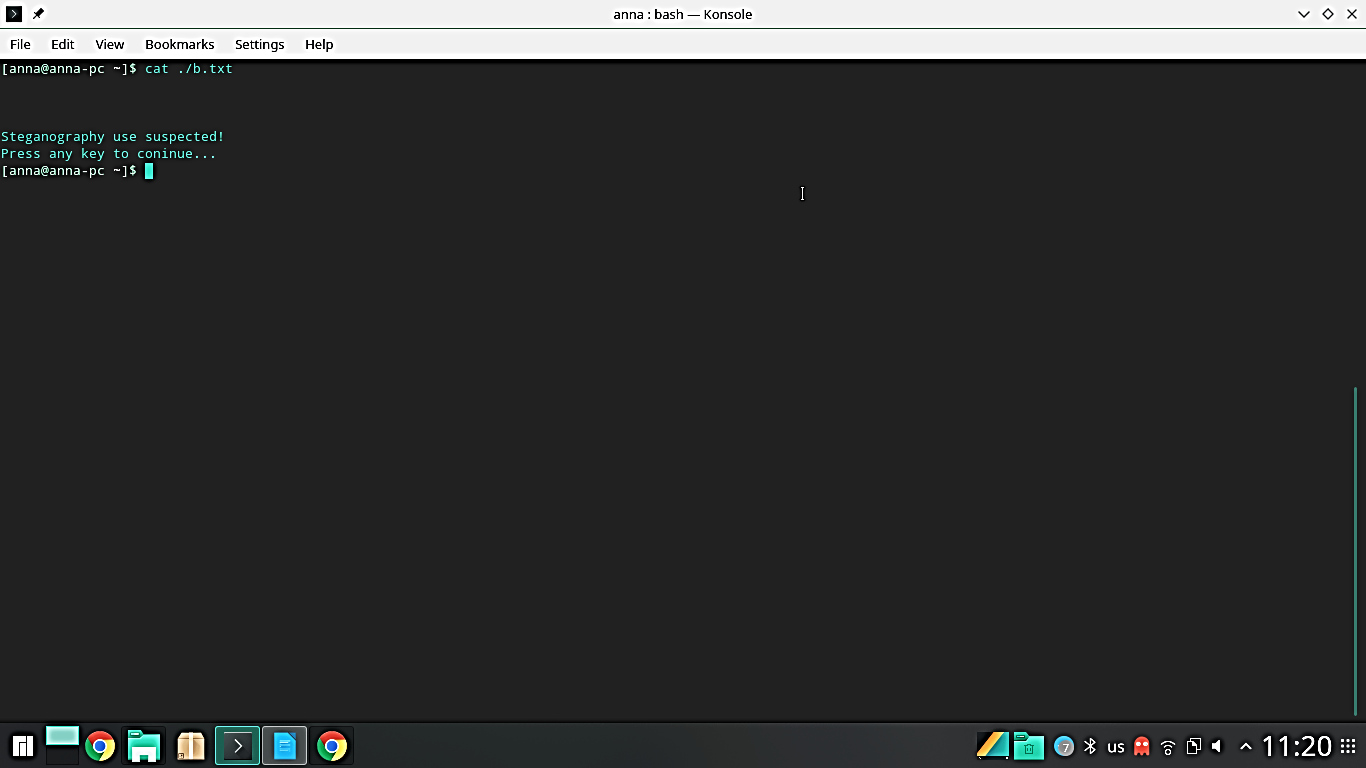


Рис. 3.3. Результати тестування: спрацювання команди скрипта при знаходженні ознак використання стеганографії за тестами

Отже, програма видала попередження про ймовірне застосування стеганографії на основі використання поля IPID, що сигналізує про коректність роботи скрипта.

**Висновк до розділу**

Залишається багато питань, що стосуються даної роботи та є завданнями подальших досліджень та розробок. Щодо SoftTempest, то по-перше, необхідно розробити інші елементи комплексного, універсального крос-платформенного засобу захисту, які дозволять проводити виявлення даного типу атак. Загальні принципи для цього такі:

* керування випромінюванням виконується програмно, отже, програмний засіб повинен отримати доступ до файлів конфігурації монітора. Такими файлами в окремій ОС Linux можуть бути, наприклад, /libX11-xcb.so, /qt/plugins/org.kde.kwin.platforms/KWinX11Platform.so, /libQt5X11Extras.so.5.11.1, /libX11.so, /libX11-xcb.so.1, /cmake/Qt5X11Extras;
* під час атаки виконується модифікація параметрів відображення на моніторі за відомими алгоритмами, певних змінних та у певних діапазонах.

Таким чином, виявлення полягає, в першу чергу, у пошуку програмного засобу, код якого містить звертання до визначеного переліку файлів конфігурації, а в них зміну відомих параметрів у заданих діапазонах. З цієї точки зору, «слабке місце» атаки є результатом її програмного характеру та за природою характерне для програмних засобів у принципі.

По-друге, необхідно враховувати, що атакуюча сторона може використовувати складніші алгоритми дізерингу зображення. У такому випадку, необхідно додати функції, що відповідають за відповідну обробку у разі використання найбільш ймовірних технік (природньо, провести необхідні перерахунки для параметрів) та модуль, який визначатиме алгоритм і запускатиме однойменнну функцію. З математичної точки зору, необхідним буде врахувати частоту появи пікселів з окремими значеннями, їх вагові коефіцієнти, а також додаткові коефіцієнти, що враховують їх світності. У найкращому випадку, необхідно експериментально перевірити корректуючі коефіцієнти для різних паттернів дізерингу, аби отримати наочне представлення видимого виводу та виключити несподівані результати.

По-третє, необхідно розрахувати оптимальну дискретність роботи програми. Для цього необхідно буде врахувати такі параметри, як дискретність роботи власне комп’ютера, обладнання на приймаючій стороні, а також обчислювальні потужності комп’ютера-жертви. Алгоритм достатньо ресурсоємний, отже, необхідно знайти оптимум між достатньою для введення в оману приймача частотою оновлення зображення та найменшою можливою затримкою під час оновлення зображення користувача.

Окрім виявлення шляхом пошуку за файлами та змінами параметрів у заданих діапазонах, можливе також виявлення через аналіз зображення на екрані. Характерні показники, які свідчитимуть про потенційний факт проведення атаки за допомогою Soft Tempest, будуть:

* дізеринг із високим контрастом сусідніх пікселів, якого можна було б уникнути через достатність наявної палітри;
* різні пари пікселів, які дають одні й ті самі загальні значення хроматичності та світності тощо.

Пошук таких властивостей досить складний в обчисленнях, тож може виконуватись частково, ефективно доповнюючи перший запропонований метод.

Нарешті, необхідно виконати програмний продукт у зручному для користувача вигляді – розробити ергономічний інтерфейс, додати можливість видання попереджень про підозру про проведення атаки, блокування доступу до розділів файлової системи, що містять файли конфігурації, автоматизувати включення «зашумлення» та можливість його вимкнення вручну по знаходженню та нейтралізації шкідливої програмної закладки тощо.

Щодо TCP-стеганографії, у якості подальшої роботи планується розробити додатковий програмний модуль, який здійснюватиме блокування трафіку на заданому інтерфейсі від визначеного хоста при підозрі на застосування TCP-стеганографії. Також, планується додати тести, що перевіряють трафік на наявність показників щодо застосування інших відомих алгоритмів TCP-стеганографії.

**ВИСНОВКИ**

У нинішній час прогресує розвиток методів комп'ютерної стеганографії – самостійного наукового відгалуження інформаційної безпеки, що вивчає проблеми приховання даних у відкритому інформаційному середовищі, що формується обчислювальними системами та мережами.

Характерною властивістю стеганографічного підходу є те, що він не дозволяє отримати ніякої інформації про приховані компоненти. Таким чином, в рамках традиційно існуючих інформаційних потоків або інформаційного середовища з’являється можливість вирішувати деякі важливі завдання захисту інформації, а також використання відповідних алгоритмів із менш добрими (та законними) намірами.

В результаті виконаної роботи був проведений огляд стеганографічних рішень, які можуть використовуватися для організації кібератак на інформаційно-телекомунікаційні системи.

В процесі виконання роботи були досягнуті такі поставлені завдання:

* проведено аналітичний огляд відомих методів стеганографії, проаналізовано теоретичну базу систем, в яких вони реалізовані;
* аналітично проаналізовано атаку, що базується на використанні технології «SoftTempest», відомі приклади реалізації та наявні методи протидії;
* аналітично проаналізовано атаку, в основі якої лежить TCP-стеганографія, різноманітні її модифікація, а також наявні методи протидії;
* формалізовано вимоги до алгоритмів виявлення вищезазначених атак та засобів протидії ним;
* розроблено методи та засоби виявлення факту проведення вищезазначених атак на систему;
* запропоновано методи та засоби захисту систем та інформації у них від вищезазначених атак;
* виконано програмну реалізацію даних засобів у формі програмних рішень.

Особливість та складність роботи полягає у незвичайному використані апарату кількох механізмів одночасно. Об’єктом вивчення є атаки, які можна описати за допомогою класичної постановки задачі стеганографії, яка зазвичай розглядається у контексті захисту, а не навпаки. Таким чином, і розглядати дані атаки, у тому числі протидію ним, необхідно з точки зору позицій стеганографії, а особливо її теоретичного апарату.

Обрані для дослідження стеганографічні алгоритми включають у себе використання особливостей таких напрямків у сфері захисту інформації, як ПЕМВН та використання протоколів передавання даних у мережі, що наразі здатні створити одні з найбільш небезпечних каналів витоку інформації, а також таких, що найшвидше змінюються та модернізуються.

Результати даної роботи можуть бути корисними для організації захисту інформації в інформаційно-комунікаційних системах, оскільки атаки, що є об’єктом вивчення, можуть застосовуватися у різних сферах. У якості прикладу можна навести корпоративний шпіонаж, а саме викрадення конфіденційної інформації шляхом її виведення із системи прихованим каналом передавання у файлах (чи інших носіях), які не викликають підозри. Таким чином, термін виявлення факту витоку може розтягнутися на невизначений час, аж до моменту, коли власник інформації понесе значні збитки.

# **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Штонда Р. М. и др. Аналіз методів цифрової стеганографії зображень //Сучасні інформаційні технології у сфері безпеки та оборони. – 2014. – №. 3. – С. 78-81.
2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография //теория и практика/ГФ Конахович, АЮ Пузыренко.—Киев: МК-Пресс. – 2006.
3. Busted alleged Russian spies used stegnography to conceal communications [Electronic resource] – Access: <https://www.darkreading.com/risk/busted-alleged-russian-spies-used-steganography-to-conceal-communications/d/d-id/1133884>
4. Zorz, Z. Zeus retrieves attack list hidden in sunset and cat images [Electronic resource] – Access: <https://www.helpnetsecurity.com/2014/03/04/zeus-retrieves-attack-list-hidden-in-sunset-and-cat-images/>
5. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія: монографія //Х.: ХНЕУ. – 2008.
6. Dumitrescu D., Stan I. M., Simion E. Steganography techniques //IACR Cryptology ePrint Archive. – 2017. – Т. 2017. – С. 341.
7. Romanova A., Toliupa S. Perspective steganographic solutions and their application //Proceedings of the VII Inter University Conference Engineer of XXI Century. – 2017. – Т. 2. – С. 269-278.
8. Yang H., Kot A. C. Data hiding for text document image authentication by connectivity-preserving //Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. – IEEE, 2005. – Т. 2. – С. ii/505-ii/508 Vol. 2.
9. Різуненко А. О. ТЕОРІЯ ТА ПРАКТИКА ЦИФРОВОЇ ОБРОБКИ ЗОБРАЖЕНЬ //Полтава: РВВ ПУСКУ. – 2009.
10. Чеховский С. Современные методы скрытой передачи информации путем программного управления излучением компьютера. – 2003.
11. Mohammadi F. G., Abadeh M. S. A survey of data mining techniques for steganalysis //Recent Advances in Steganography. – IntechOpen, 2012.
12. Андрущенко Д. М. Система для исследования стойкости робастных стеганографических алгоритмов //Восточно-Европейский журнал передовых технологий. – 2013. – №. 6 (12). – С. 41-44.
13. Юдін О. К., Руслана З., Фролов О. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів //Радиоэлектроника и информатика. – 2015. – №. 3.
14. Singh H. Analysis of Different Types of Steganography //International Journal of Scientific Research in Science, Engineering and Technology. – 2016. – Т. 2. – №. 3. – С. 578-582.
15. Ferreira A. M. an overview on hiding and detecting stego-data in video streams //University of Amsterdam. System & Network Engineering–Research Project II. – 2015.
16. Wai E. N. C., Khine M. A. Modified Linguistic Steganography Approach by Using Syntax Bank and Digital Signature //International Journal of Information and Education Technology. – 2011. – Т. 1. – №. 5. – С. 410.
17. Грибунин В. Г. и др. Стеганография, цифровые водяные знаки и стеганоанализ. – 2009.
18. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом : дис. – –СПб.: СПбГУТ, 2014.–176 с, 2014.
19. Carvajal-Gámez B. E. et al. Steganography in Different Colour Models Using an Energy Adjustment Applying Wavelets //Recent Advances in Steganography. – IntechOpen, 2012.
20. Sajedi H. RABS: Rule-Based Adaptive Batch Steganography //Recent Advances in Steganography. – IntechOpen, 2012.
21. Зайцева А. В. Методика построения энтропийных стеганографических систем защиты сообщений в информационных сетях : дис. – автореф. дис.… к. т. н МГТУ им. НЭ Баумана, Москва, 2014.
22. Yalman Y., Akar F., Erturk I. Contemporary Approaches to the Histogram Modification Based Data Hiding Techniques //Recent Advances in Steganography. – IntechOpen, 2012.
23. Зорин Е. Л., Чичварин Н. В. Информационная безопасность САПР/PLM, применяющих облачные технологии //Вопросы кибербезопасности. – 2014. – №. 4 (7).
24. Фисун Ю. С., Юнов С. В. Стеганографическое сокрытие данных в аудиосигналах. – 2017. – С. 14-17.
25. Aoki N. Lossless Steganography for Speech Communications //Recent Advances in Steganography. – IntechOpen, 2012.
26. Wai E. N. C., Khine M. A. Syntactic bank-based linguistic steganography approach //2011 International Conference on Information Communication and Management IPCSIT. – 2011. – Т. 16.
27. Chang C. Y., Clark S. Linguistic steganography using automatically generated paraphrases //Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics. – Association for Computational Linguistics, 2010. – С. 591-599.
28. Lemström K., Tarhio J., Takala T. Color dithering with n-best algorithm //Proceedings of Fourth International Conference in Central Europe on Computer Graphics and Visualization, Plzen, Czech Republic. – 1996. – С. 162-170.
29. Дизеринг [Electronic resource] – Wikipedia – Access: <https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%B7%D0%B5%D1%80%D0%B8%D0%BD%D0%B3>
30. Dithering [Electronic resource] – Access: <https://webstyleguide.com/wsg2/graphics/dither.html>
31. Helland, T. Image dithering: eleven algorithms and source code [Electronic resource] – Access: [http://www.tannerhelland.com/4660/dithering-eleven-algorithms-source-code](http://www.tannerhelland.com/4660/dithering-eleven-algorithms-source-code/)
32. Romanova A., Toliupa S. Steganography methods used in attacks on information and communication systems //Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. – 2018. – Т. 8.
33. Лыков Ю. В., Сягаева О. А. Концепция построения защищенных видеосистем //Радиотехника. – 2013. – №. 173. – С. 208-215.
34. Пархоменко И.И., Язиванова М.В.Способыпредотвращения утечки  информации с компьютерных систем через технологию  Soft TEMPEST [Електронний ресурс] – Режим доступу: [http://www.rusnauka.com/31\_ONBG\_ 2011/ Informatica/4\_96679.doc.htm](http://www.rusnauka.com/31_ONBG_%202011/%20Informatica/4_96679.doc.htm)
35. Чеховский С. А. Електромагнітні випромінювання комп'ютерних систем і захист інформації //Захист інформації. – 2003. – Т. 5. – №. 3 (16). – С. 18-29.
36. Kuhn M. G., Anderson R. J. Soft tempest: Hidden data transmission using electromagnetic emanations //International Workshop on Information Hiding. – Springer, Berlin, Heidelberg, 1998. – С. 124-142.
37. Kuhn M. G. Electromagnetic eavesdropping risks of flat-panel displays //International Workshop on Privacy Enhancing Technologies. – Springer, Berlin, Heidelberg, 2004. – С. 88-107.
38. Kuhn M. G. Optical time-domain eavesdropping risks of CRT displays //Proceedings 2002 IEEE Symposium on Security and Privacy. – IEEE, 2002. – С. 3-18.
39. Suzuki Y. et al. Countermeasure technique for preventing information leakage caused by unintentional PC display emanations //Proceedings of International Symposion on EMC 2009. – 2009. – С. 9-12.
40. Антясов И. С., Сафонов А. В., Соколов А. Н. Программно-техническая реализация технологии «Мягкий» ПЭМИН //Вестник УрФО. Безопасность в информационной сфере. – 2015. – №. 3. – С. 8-11.
41. Kuhn M. G. Compromising emanations: eavesdropping risks of computer displays :дис. – University of Cambridge, 2002.
42. Таликин Т. А. TCP СТЕГАНОГРАФИЯ //Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. – С. 210.
43. Szczypiorski K. HICCUPS: Hidden communication system for corrupted networks //International Multi-Conference on Advanced Computer Systems. – 2003. – С. 31-40.
44. Murdoch S. J., Lewis S. Embedding covert channels into TCP/IP //International Workshop on Information Hiding. – Springer, Berlin, Heidelberg, 2005. – С. 247-261.
45. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет //Труды объединённой научной конференции" Интернет и современное общество". – 2012. – С. 348-354.
46. Mandal D. Covert Channel over ICMP. – 2011.
47. Lucena N. B., Lewandowski G., Chapin S. J. Covert channels in IPv6 //International Workshop on Privacy Enhancing Technologies. – Springer, Berlin, Heidelberg, 2005. – С. 147-166.
48. Fisk G. et al. Eliminating steganography in Internet traffic with active wardens //International Workshop on Information Hiding. – Springer, Berlin, Heidelberg, 2002. – С. 18-35.
49. Kreibich C., Handley M., Paxson V. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics //Proc. USENIX Security Symposium. – 2001. – Т. 2001.
50. Ahsan K., Kundur D. Practical data hiding in TCP/IP //Proc. Workshop on Multimedia Security at ACM Multimedia. – 2002. – Т. 2. – №. 7.
51. Recommendation ITU-R BT.709-6 (06/2015) Parameter values for the HDTV standards for production and international programme exchange [Electronic resource] – Access: <http://www.itu.int/dms_pubrec/itu-r/rec/bt/R-REC-BT.709-6-201506-I!!PDF-E.pdf>
52. Bayer B. E. An optimum method for two-level rendition of continuous tone pictures //IEEE International Conference on Communications, June, 1973. – 1973. – Т. 26.
53. Кошкіна Н. В. Спектральні методи комп’ютерної стеганографії та методи стеганоаналізу з навчанням і класифікацією. – 2016.
54. Иванников А. Д. и др. Цифровая стеганография: шифрование, зашита //Информационные технологии. – 2004. – №. 8. – С. 1-32.
55. Kahn D. The Codebreakers: The comprehensive history of secret communication from ancient times to the internet. – Simon and Schuster, 1996.
56. Азаров О. Д. и др. Основи комп’ютерної стеганографії. – 2003.
57. Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. — К.: «Центр учбової літератури», 2018. — 558 с., іл.
58. Anna Romanova, Sergiy Toliupa. Dmitry Malyarenko steganographyas a means of attacking information systems. МатеріалиІІміжнародноїнауково-практичноїконференції “Проблемикібербезпекиінформаційно- телекомунікаційнихсистем” (PCSIТS). – Київ. - 2019. – с. 122-123.
59. Toliupa S., NakonechnyiV., Romanova A.,Dmitry Malyarenko. Steganographyand cibernetic space. Науково-практичнаконференція. «Кібербезпекау системі національної безпеки України: проблеми та перспективи розвитку». Маріуполь. 2019. – с. 78-79.
60. Толюпа С., Єсипенко О., Маляренко Д. Застосування математичної теорії ігор при побудові систем управління інформаційною безпекою. Матеріали допо-відей. VІ Міжнародна науково-практична конференція «Інформаційні технології та взаємодії» (IT&I 2019). – с. 313-317.

# **Додаток А**

Лістінг коду програмного забезпечення, що реалізує алгоритм протидії атаці із використанням Soft Tempest

#include <stdio.h>

#include <stdlib.h>

#include <jpeg.h>

#include <png.h>

// necessary library depends on the image format

// compilation command needs gcc softTempest.c -lpng -o softTempest.exe

// libjpeg.so

// libpng.so and so on

struct pixels

{

int red;

int green;

int blue;

};

int \* getImage (FILE \*); // this is a prototype for some function that gets an image and returns an array of clear pixel colour structures

// includes memory allocation for data structure

void reverseImage (int \*) // this function gets new values and makes them into a new file with correct headers

void giveImage(FILE \*); //this is a prototype for a function that will pass the constructed image to the screen (both functions depend on the format type)

int \* processImage(struct pixels \*, struct pixels \*); //this function calculates new values for a 2x2 pixel block (is implemented in main())

int main ()

{

FILE \*inputfile, \*outputfile;

char filename [100];

int n = 0;

int \*ptr;

printf ("Input the name of the image file: \n");

scanf ("%s", filename);

inputfile = fopen(filename, "r");

while(fscanf(filename, "%s") != EOF)

{

ptr = processImage(\*(getImage(inputfile) + n), \*(getImage(inputfile) + n + 1));

n++;

reverseImage(ptr);

}

printf ("Enter the output file name: /n");

scanf ("%s", filename);

outputfile = fopen(filename, "r");

giveImage(outputfile);

return 0;

}

int \* processImage (struct pixels \* rgb1, struct pixels \* rgb2)

{

double l1, l2, l12, r12, g12, b12;

struct pixel \* rgb12;

struct pixels value1 = (int\*)malloc(sizeof(int)\*3);

struct pixels value2 = (int\*)malloc(value1 + sizeof(int)\*3);

value1.red = rgb1->red;

value1.green = rgb1->green;

value1.blue = rgb1->blue;

value2.red = rgb2->red;

value2.green = rgb2->green;

value2.blue = rgb2->blue;

l1 = 0.2126 \* value1.red + 0.7152 \* value1.green + 0.0722 \* value1.green;

l2 = 0.2126 \* value2.red + 0.7152 \* value2.green + 0.0722 \* value2.green;

r12 = (value1.red + value2.red) / 2;

g12 = (value1.green + value2.green) / 2;

b12 = (value1.blue + value2.blue) / 2;

l12 = 0.2126 \* r12 + 0.7152 \* g12 + 0.0722 \* b12;

if ((r12 \* 10) % 10 == 0)

{

value1.red = (int)r12;

value2.red = (int)r12;

}

else

{

value1.red = (int)(r12 + 0.5);

value2.red = (int)(r12 - 0.5);

}

if ((g12 \* 10) % 10 == 0)

{

value1.green = (int)g12;

value2.green = (int)g12;

}

else

{

value1.green = (int)(g12 + 0.5);

value2.green = (int)(g12 + 0.5);

if ((b12 \* 10) % 10 == 0)

{

value1.blue = (int)b12;

value2.blue = (int)b12;

}

else

{

value1.blue = (int)(b12 + 0.5);

value2.blue = (int)(b12 - 0.5);

}

return \* value1;

free(value1);

free(value2);

# **Додаток Б**

Лістінг коду програмного забезпечення, яке реалізує метод виявлення атаки із використанням TCP-стеганографії

#!/bin/bash

# echo $SHELL just in case

# This script takes a traffic dump file as an input

# then, it contains steganograohy test which are performed one-by-one

# it is highly unlikely that two steganography technics are used at once

# thus, if one flag goes off, the script gives alert and aborts

clear

echo

echo Starting the script: you are going to test a traffic dump file

echo to see if any steganography technic is used

echo

echo

read -p "Indicate the input file full path: " FILE

checkFlag=0

tcpRst () {

local n=1

while read line

do

if [[$line==\*[R.]\*]]

then

if [[$((line+1))#\*//0x????:]]

then

checkFlag=1

fi

fi

n=$((n+1))

done < $1

}

tos () {

local n=1

while read line

do

if [[$line==\*IP\*]]

then

tosVar=${line#\*0x}

tosVar=${tosVar%%,\*}

fi

if ! [[$tosVar==0]]

then

checkFlag=1

fi

n=$((n+1))

done < $1

}

ipId () {

local n=1

while read line

do

if [[$line==\*id\*]] && [[$line==\*tos 0x0\*]]

then

ipid=${line#\*id }

ipid=${ipid%%,\*}

ipid=$((ipid/256))

printf "\x $(printf %x $ipid)"

fi

n=$((n+1))

done < $1

read -p "Does this make sense? y or n: " a

if [[a=='y']]

then

checkFlag=1

fi

}

ipFragm () {

local n=1

while read line

do

if [[$line==\*DF\*]]

then

fragm=${line#\*offset }

fragm=${fragm%%,\*}

fi

if ! [[fragm==0]]

then

checkFlag=1

fi

n=$((n+1))

done <$1

}

tcpUrg () {

local n=1

while read line

do

if ! [[$line==\*[U]\*]] && [[$line==\*urg\*]]

then

urg=${line#\*urg}

urg=${urg%%,\*}

fi

if ! [[urg==0]]

then

checkFlag=1

fi

n=$((n+1))

done < $1

}

tcpTime () {

local n=1

while read line

do

if [[$line==\*:??:\*]]

then

stamp=${line##\*:}

stamp=${stamp%% IP\*}

$array[n-1]=stamp

fi

n=$((n+1))

done < $1

diff=$((array[n-1]-array[0]))

sort $array | uniq -c >> /home/dima/count.txt

count=0

while read list

do

count++

done < /home/dima/count.txt

# example file name, might be modified to get from command line

if [[$((count / diff)) < 0.85]]

checkFlag=1

fi

}

tos $FILE 2>/dev/null

if[[checkFlag==1]]

then

terminal -e /home/dima/alert.sh

exit

fi

echo No ToS steganography found

echo

tcpRst $FILE 2>/dev/null

if[[checkFlag==1]]

then

terminal -e /home/dima/alert.sh

exit

fi

echo No RST steganography found

echo

ipId $FILE 2>/dev/null

if[[checkFlag==1]]

then

terminal -e /home/dima/alert.sh

exit

fi

echo No IP ID steganography found

echo

ipFragm $FILE 2>/dev/null

if[[checkFlag==1]]

then

terminal -e /home/dima/alert.sh

exit

fi

echo No IP Fragmentation steganography found

echo

tcpUrg $FILE 2>/dev/null

if[[checkFlag==1]]

then

terminal -e /home/dima/alert.sh

exit

fi

echo No TCP URG steganography found

echo

tcpTime $FILE 2>/dev/null

if[[checkFlag==1]]

then

terminal -e /home/dima/alert.sh

exit

fi

echo No TCP timestamp steganography found

echo

echo Program executed successfully!

#!/bin/bash

# This is the alert message

# in case any flag goes off

clear

echo

echo

echo

echo Steganography use suspected!

# echo The suspected technic is

read -n 1 -s -p "Press any key to continue..." KEY

# kill -25 $PPID

# **Додаток В**

У роботі [7, с. 17] міститься опис напрямків розвитку стеганографії, що вивчаються менше, та її методів, які застосовуються значно рідше за інші, незважаючи на високі показники за вимогами стеганосистем та загальну перспективність. Така непопулярність може бути зумовлена різними причинами, з яких найімовірнішими є:

* відносна складність побудови системи, необхідність використання вузькоспеціалізованого обладнання та складних алгоритмів;
* для деяких з методів – висока вартість побудови системи;
* вимога до специфічних знань та навичок; деякі з цих методів є багатодисциплінарними, що спричиняє складність пошуку спеціалістів, які розумілися б на багатьох сферах науки, або ж підбору ефективної команди вузьких спеціалістів.

**Інтернет речей та кібер-фізичні системи**

Кібер-фізична система (CPS) – це механізм, який контролюється за допомогою комп'ютерних алгоритмів, тісно інтегрованих з Інтернетом та його користувачами. Прикладами таких систем є автономні автомобільні системи, медичний моніторинг, інтелектуальні електромережі, автопілотні системи в авіоніці тощо.

Інтернет речей (IoT) – це мережа фізичних пристроїв, транспортних засобів та інших об’єктів із вбудованою електронікою, датчиками, програмним забезпеченням і мережевим підключенням, які дозволяють їм виконувати збір та обмін даними. Наближено це можна розглядати як об’єкт класу кібер-фізичних систем.

Мережева стеганографія використовує елементи керування протоколами зв'язку та їх функціональність, аби приховати всередині інформацію. Модифікації можуть бути здійснені або через єдиний мережевий протокол (застосований до ProtocolDataUnit (блоку протокольних даних), часової кореляції між PDU або обидва способи) або декілька протоколів одночасно (міжпротокольна стеганографія). Такі способи мережевої стеганографії можуть бути застосовані також до вищезгаданих систем. Вважається, що феномен IoT значно розширить свій вплив протягом наступних кількох років. Як перспективний приклад комплексної мережі, він вимагає уваги фахівців зі стеганографії. Фактично, інформація циркулює всередині IoT так само, як і в будь-якій іншій системі. Таким чином, оптимальні та найбільш відповідні методи приховування даних у протоколах зв'язку повинні бути відповідно модифіковані та підлаштовані під використання в IoT.

Більше того, оскільки елементи IoT вміщують велику кількість різноманітних датчиків і програмного забезпечення, останні також можуть бути використані для приховування даних. Наприклад, приховані повідомлення можуть кодуватися в невикористовуваних регістрах компонентів CPS/IoT або у значеннях станів їх датчиків.

**Використання потокових контейнерів**

За типом доступу до даних можна виділити фіксовані та потокові контейнери [2, с. 7]. Більшість методів використовують перші для приховування інформації. Такий контейнер є постійною попередньо визначеною послідовністю бітів, яку стеганограф отримує всю одночасно. На противагу цьому, потоковий контейнер є послідовністю бітів, яка безперервно змінюється, як-от у телефонній розмові. Повідомлення вбудовується в реальному часі так, що кінцевий розмір контейнера не відомий заздалегідь. Інтервали між вбудованими бітами генеруються генератором псевдовипадкових послідовностей (PRS generator) і рівномірно розподіляються між відліками [2, с. 7].

Існує лише кілька наукових праць, присвячених цьому типу стеганографії, не кажучи вже про приклади його реальної практичної реалізації. Незважаючи ні на що, вона може бути успішно застосована як ефективний засіб інформаційної безпеки. Існує ряд рішень для зашифрованого безпечного спілкування в реальному часі. Але що як ми зможемо, наприклад, зробити конфіденційну телефонну розмову не тільки незрозумілою, але й такою, що вона здаватиметься цілком невинними балачками? Рішенням може стати стенографічна телефонна приставка. Це стосується і відеоконференцій. Сторонній спостерігач побачить лише середньостатистичну бесіду, якщо він не має доступу до реальних аудіо, відео чи будь-яких інших вбудованих даних.

Непопулярність стеганографії із потоковими котейнерами можна пояснити, розглянувши основні проблеми її використання. Перш за все, ніколи не відомо, чи буде розмір контейнера достатнім для приховання усього повідомлення, оскільки довжина першого (і, ймовірно, останнього, також) є невизначеною. Ця властивість створює і перевагу теж, оскільки один файл-контейнер може бути достатньо ємним, аби вмістити кілька повідомлень. У будь-якому випадку, якимось чином повинна бути реалізована синхронізація з контейнером, тому одним з найбільших питань є те, як визначити початок і кінець вбудованої послідовності всередині нього. Проблема стає більш серйозною щодо відеозв'язку. Рішення було б надзвичайно складним, оскільки необхідно синхронізувати потік зображення (як відкритого, так і прихованого), повний звуковий потік, та зображення і звук відповідно.

У майбутньому, рішення може полягати у використанні спеціальних вбудованих бібліотек. Вони складатимуться зі структурованих груп слів однакової довжини, які в ідеальному випадку мали б схожість вимови. Такі групи повинні бути згруповані в семантичні словники, щоб вони формували прості, але логічно і семантично структуровані речення. Лінгвістичні засоби для цього добре розвинені і схожі з тими, що формують синонімічні словники та додатки машинного перекладу. Слова й речення можуть бути суміщені з контейнером за допомогою бітів синхронізації, заголовків пакетів та/або інших засобів поділу інкапсульованих даних; приховане повідомлення може бути вбудовано після них і синхронізовано з використанням базових властивостей контейнера.

Ситуація із відеозв'язком була б значно складнішою. Якщо тільки зміст даної розмови є конфіденційним, то проблема полягає в тому, щоб стеганографічно зашифрувати звук і синхронізувати його з реальним відеозображенням. З іншого боку, якщо особи учасників розмови також складають таємницю, то повинні бути передбачені інші методи. Стеганографічне рішення не обов’язково повинно бути універсальним. Можна розробити систему, що складається як з криптографічних, так і стеганографічних модулів і передбачає різні сценарії відповідно до конкретної ситуації.

Найбільшою проблемою залишається значна затримка, яка є неприйнятною в режимі реального часу. Знову ж таки, щодо цього у криптографії вже існують розроблені рішення, які можна модифікувати відносно стеганографії та адаптувати до задачі.

**Семантичні та синтаксичні методи**

Ці два класи методів відносяться до стеганографії з текстовими контейнерами. Замість використання властивостей цифрового формату, вони працюють із самою мовою. Це є перевагою в порівнянні із першим типом. Тоді як середньостатистичний читач може не знати про приховане повідомлення, що існує у відкритому тексті, текстовий редактор може автоматично змінювати кількість пробілів або здійснювати інші дії, які можуть зіпсувати вбудовані дані [2, с. 7]. Насправді, будь-яке переформатування призведе до того самого результату.

Синтаксичні та семантичні методи, на противагу до вищезазначеного, використовують не представлення тексту, а працюють із самим текстом. Перший тип використовує той факт, що в більшості мов існують деякі додаткові правила пунктуації та граматики. Будь-яка мова дотримується конкретних правил, але всеодно не є абсолютно жорсткою структурою і тому надає велику кількість мовних можливостей. Наприклад, в українській мові двокрапка і тире в деяких випадках можуть замінювати один одного. Така властивість може бути використана для кодування бітового секретного повідомлення – “0” для одного знака пунктуації та “1” для іншого. Більш складним методом може бути використання граматичних подібностей у різних конструкціях речень, таких як зміна послідовності деяких слів.

Прикладом семантичної стеганографії є використання таблиць синонімів для кодування секретних бітів. Якщо два слова, скажімо, «однак» і «але», то одне з них може кодувати «0», а інше «1». Якщо є більше синонімів, можливо контекстних, то 4 слова можуть кодувати 2 біти, 6 слів 3 біта інформації тощо. Середня швидкість передачі даних при використанні цих методів становить вже значно більше, ніж кілька біт на кілобайт тексту, як у лінгвістичній стеганографії.

Основні проблеми з такими лінгвістичними методами очевидні. По-перше, існує значна залежність від мови. По-друге, вони вимагають великих обсягів вихідного тексту у якості контейнера, що не зовсім ефективно. Нарешті, навіть якщо деякі правила пунктуації є неоднозначними, їх навмисне і суперечливе використання може бути виявлене цензором або редактором.

Логічно запропонувати використання більш складних методів мовної стеганографії. Кожна мова може бути проаналізована для створення спеціальних таблиць синтаксичної відповідності. Наприклад, для англійської та інших германських мов необов'язковим є використання активних чи пасивних конструкцій, а також складених підметів та додатків. Речення можна легко і природньо трансформувати, використовуючи еквівалентні конструкції, які, швидше за все, не викличуть підозри. Переваги такого рішення численні. Однією з них є висока стійкість до різних атак (вони схожі на одноразові блокноти). Інша полягає в тому, що здатність вбудовування набагато вища, ніж у базових семантичних методів. Питанням залишається лише алгоритм вибору вихідного текстового матеріалу. Ймовірно, найкращим варіантом є створення спеціальних бібліотек текстів, відсортованих за темою. Таким чином, багато тем можна охопити таким чином, щоб приховане повідомлення не було виявлено.

У роботі [7, с. 17] пропонується створення багатоцільового комплексу лінгвістичної стеганографії. Безумовно, це вимагатиме якісної та глибокої лінгвістичної роботи. Необхідно знайти оптимальний підхід, який, за можливості, зменшить залежність рішень від мови. В іншому випадку, такий додаток повинен розроблятися для окремої мови або, принаймні, групи мов із тією ж лінгвістичною парадигмою. Таким чином, завдання полягає в групуванні мов у кожній сім'ї за допомогою подібних тенденцій у використанні граматики. Наступний крок полягає у створенні таблиць відповідності для граматичних конструкцій та стилістичних виразів, які можна взаємозамінювати. Нарешті, бібліотеки текстових матеріалів повинні надавати контейнери ненав’язливого вигляду з якомога більшою кількістю варіантів, описаних у вигляді таблиць.

**Біохімічна стеганографія**

Більшість сучасних стеганографічних систем використовують тільки цифрові контейнери, такі як файли різної природи, бінарні послідовності тощо [17, с. 9]. Однак для стеганографії існують й інші сфери інтересу, оскільки навколишнє середовище може забезпечити значну різноманітність контейнерів нецифрової природи.

Ми оточені мільярдами організмів, кожна клітина яких містить молекули ДНК. Вони є центральним сховищем інформації у клітині. Біологічні та квантові обчислення вважаються двома найбільш перспективними технологіями, над якими наразі працює світова наукова спільнота. І оскільки на даний момент криптографія в основному працює над проблемами факторизації, що не захистить повідомлення від атак із використанням квантових комп'ютерів, біохімія представляє нову сферу потенційних рішень інформаційної безпеки.

ДНК-стеганографія – це процес приховування повідомлення, кодованого за допомогою молекул ДНК, серед великої кількості найрізноманітніших ДНК видових геномів. Внаслідок різноманітності ДНК-коду з-поміж різних видів, випадково обраний організм має випадковий ДНК-код. Така характеристика робить ці молекули потенційно ефективними контейнерами. Ще однією безсумнівною перевагою є їхній маленький розмір, оскільки величезна кількість інформації може бути закодована в контейнері, який навіть не розпізнати людським оком без належного посилення. ДНК також є цілісною структурою із високими показниками стійкості до можливих біохімічних атак.

Проте, незважаючи на очевидні перспективи використання ДНК як засобу біохімічної стеганографії, до цих пір більша частина уваги приділялася ДНК-криптографії.

Молекула ДНК являє собою послідовність з чотирьох нуклеотидів – аденіну (А), цитозину (С), гуаніну (G) та тиміну (Т), які згруповані в триплекси, так звані кодони, і утворюють дві антипаралельні ланцюги. Додаткові ланцюги ДНК можуть самостійно утворюватися шляхом формування водневих зв'язків між основами (парування основ) кожного лангцюга, так що A поєднується тільки з T, а G тільки з C. Чотири різні основи означають 4n можливих різних n-мерів, які кодують генетичну інформацію за допомогою різних амінокислот. Іншою макромолекулою, яку потенційно можна використати, є молекула РНК. Вона схожа на молекулу ДНК, за винятком того, що основою є інший 5-атомний цукор – рибоза, а урацил (U) замінює тимін.

Отже, як ми кодуємо інформацію всередині біомолекулярної структури? Повідомлення може бути зашифровано в ланцюзі ДНК, кожен символ кодується кодоном, визначеним у спеціально розробленій таблиці (техніка нагадує використання одноразових блокнотів). Наприклад, "A" може бути закодовано послідовністю CGA, "B" – CCA і так далі. Потім секретне повідомлення представляється послідовністю кодонів. Існує навіть ряд готових амінокислот, що можуть бути використані без модифікацій: аланін – GCT, GCC, GCA, GCG; аспарагін – GAT, GAC; фенілаланін – ТТТ, ТТК.

Потім ланцюжок фланкують послідовностями праймерів полімеразної ланцюгової реакції (ПЛР) і приховують шляхом змішування серед численних додаткових «відволікаючих» ланцюгів ДНК. Полімеразна ланцюгова реакція (ПЛР) являє собою процес, під час якого ПЛР-праймери та "ключі" праймерів F і R в ДНК стають комплементарними. Потім їх приховують у мікроточці. Знаючи секретний ключ і послідовності праймерів, користувач може вирізнити необхідний ланцюг із використанням відомих способів розділення ДНК (гібридизація з елементами, комплементарними до ланцюгів, що утворюють секретний ключ, може бути поміщена на тверду основу на магнітних кульках або на підготовленій поверхні; цей крок можна поєднати з етапами ампліфікації та/або ПЛР) і зчитати повідомлення [7, с. 17].

Проблема такого підходу полягає в тому, що ймовірнісний розподіл амінокислот у природі не є таким самим, як у секретному повідомленні. Таємні ланцюжки повинні бути такими, щоб їх не можна було відрізнити від "відволікаючих" ланцюгів ДНК, та ентропія повинна бути такою ж, як і в будь-якій молекулі ДНК – між 1,2 і 2. Зазначені вимоги створюють необхідність використання, з-поміж іншого, моделей реальних молекул ДНК. Однією з найновітніших корректуючих методик є використання секвенування (визначення послідовності нуклеотидів у фрагменті ДНК). Завдяки досягненням науковців, у відкритому доступі вже є чимало секвенованих геномів – 55 геномів бактерій, геном дріжджів та інших стандартних лабораторних об'єктів є лише деякими з них. Ще одне запропоноване рішення полягає в тому, щоб моделювати «відволікаючі» ланцюги так, що їх розподіл імітуватиме розподіл відкритого тексту повідомлення. Один з найпростіших способів зробити це – синтезувати молекулу ДНК, характеристики якої залежать тільки від відкритого тексту та секретного ключа. Також можливе стиснення відкритого тексту. Якщо результуючий розподіл відкритого тексту можна апроксимувати нормальним розподілом, то випадкової «відволікаючої» послідовності може бути достатньо для забезпечення необхідного рівня безпеки. Використання замісної випадкової комбінації послідовних геномів (наприклад, екзотичних організмів) також може бути рішенням для поліпшення характеристик системи.

Роботу TOMONORI KAWANO: Run-length encoding graphic rules, biochemically editable designs and steganographical numeric data embedment for DNA-based cryptographical coding system (Commun Inteqr Biol. March 2013: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3609851/) присвячено системам кодування довжини серії (run-length encoding, RLE) у біохімічній стеганографії, хоча і зазначено, що використання таких систем на практиці все ще ставить більше питань, ніж надає відповідей.

Зважаючи на усе вищезазнечене, будь-яка потенційна атака на систему на основі ДНК-стеганографії не буде успішною, якщо носитиме суто обчислювальний характер. Тим не менше, шляхи протидії біохімічним атакам є важливим питанням, на яке слід звернути увагу в подальшому розвитку даного напряму.

Сучасні технології ДНК-стеганографії все ще перебувають на стадії лабораторних досліджень і зосереджені на експериментах. Можливе пояснення відсутності очікуваної діяльності в цій галузі полягає в тому, що дана область надзвичайно багатопрофільна, вона вимагає знань як у біології, так і в математиці, теорії інформації та криптографії, і тому вимагає від дослідників з усіх сфер пошуку шляхів ефективного співробітництва. Можливими сферами для реалізації цих технологій є контроль проти підробок, контроль ідентифікації та доступу персоналу, маркування для протидії крадіжкам та аутентифікація продукції. Всі вони є засобами забезпечення прибутку в бізнесі і, таким чином, привабливими для промислового виробництва та сфери обслуговування. Відомо лише кілька прикладів використання ДНК-стеганографії у якості свого роду водяних знаків. У 2000 році під час Олімпійських ігор в Сіднеї Австралійський олімпійський комітет використовував технологію відстеження ДНК для захисту ліцензованих олімпійських товарів від підробок [7, с. 17].

**Стеганоаналіз**

Наразі, можна вирізнити такі перспективні напрямки розвитку методологічної бази стеганографічного аналізу:

* + 1. Розробка ймовірнісно-статистичних методів розпізнавання, застосування елементів штучного інтелекту для оцінки надійності стеганографічних перетворень та розробки детекторів (фільтрів) для аналізу інформаційних потоків з метою виявлення та знищення прихованих каналів зв'язку. У цьому випадку перевірка наявності прихованої інформації визначається певною оцінкою з використанням статистичних критеріїв (послідовна кореляція, ентропія зображення, дисперсія LSB тощо). Рішення, розроблені для даної мети, повинні не тільки забезпечувати низький рівень помилок у розпізнаванні вхідних повідомлень (особливо при використанні шифрування даних), але й мати можливість виявляти повідомлення, вбудовані з використанням різних стеганографічних методів. Порівняно із додатками, призначеними для стеганографічно прихованих даних, кількість і якість стеганоаналітичних систем наразі достатньо низькі.
    2. Аналіз конкретних стеганографічних програмних рішень для відновлення алгоритмів приховування та розробки методу оптимального аналізу. Основною складністю є знову ж таки велика кількість специфічних алгоритмів, що вимагають індивідуального підходу, а також значні обчислювальні потужності.
    3. Розробка технології автоматизованих активних і шкідливих атак для того, щоб передбачувана стеганограма спотворювалася без можливості відновлення, аби спровокувати її повторну передачу в іншому контейнері, що підтвердить існування прихованого каналу [2, с. 7].