РЕФЕРАТ

Пояснительная записка к работе содержит страниц, источников, рисунка, приложения, формул.

Главная цель работы состоит в определении криптостойкости систем, основанных на групповой математике, хаотических преобразованиях и ДНК.

Провести анализ криптосистем, построенных на разных базах, определить недостатки и преимущества каждой.

В работе рассмотрены алгоритмы построения криптосистемы на хаосе и ДНК, также проанализированы базовые методы защиты информации, которые используют групповую математику. Реализован алгоритм RSA, и дополнения, которые позволяют применять его для ДНК-криптографии, с использованием нуклеотидов.

ДНК, ХРАНЕНИЕ ДАННЫХ В ДНК, ДНК-КРИПТОГРАФИЯ, КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ, СТЕГАНОСИСТЕМЫ СТЕГАНОГРАФИЯ.

РЕФЕРАТ

Пояснювальна записка до роботи містить 56 сторінок, 17 посилань, 3 рисунка, 2 додатки, 11 формул.

Головна мета роботи полягає у визначенні криптостійкості систем, заснованих на груповій математиці, хаотичних перетвореннях і ДНК. Провести аналіз криптосистем, побудованих на різних базах, визначити недоліки та переваги кожної.

В роботі розглянуті алгоритми побудови криптосистеми на хаосі і ДНК, також проаналізовані базові методи захисту інформації, які використовують групову математику. Реалізовано алгоритм RSA, та доповнення, які дозволяють застосовувати його для ДНК-криптографії, з використанням нуклеотидів.

НЕАБЕЛЕВІ ГРУППЫ, ДНК, ЗБЕРІГАННЯ ДАННИХ У ДНК, ДНК-КРИПТОГРАФІЯ, КРИПТОГРАФІЧНІ СИСТЕМИ, ХАОТИЧНІ КРИПТОСИСТЕМИ, ВПРОВАДЖЕННЯ ХАОТИЧНИХ КРИПТОСИСТЕМ, РЕКОМЕНДАЦІЇЇ ДО РОЗРОБКИ ХАОТИЧНИХ КРИПТОСИСТЕМ.

ABSTRACT

Explanatory note for the work contains 56 pages, 17 sources, 3 figures, 2 applications, 11 formulas.

The main goal of the paper is to determine the cryptographic strength of systems based on group mathematics, chaotic transformations and DNA. Conduct an analysis of cryptosystems built on different bases, determine the disadvantages and advantages of each.

In work were considered algorithms of construction of a cryptosystem on chaos and DNA, basic methods of information protection that use group mathematics were analyzed. Implemented the RSA algorithm, and additions that allow it to be used for DNA cryptography, using nucleotides.

NON-ABELIANS GROUPS, DNA, STORAGE OF DATA IN DNA, DNA CRYPTOGRAPHY, CRYPTOGRAPHIC SYSTEMS, CHAOTIC CRYPTOSYSTEMS, INTRODUCTION OF CHAOTIC CRYPTOSYSTEMS, RECOMMENDATIONS FOR DEVELOPMENT OF CHAOTIC CRYPTOSYSTEMS.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

RSA – аббревиатура от фамилий Rivest, Shamir и Adleman

CSP – задач поиска сопряжений (Conjugacy Search Problem)

ДНК – дезоксирибонуклеи́новая кислота́

DH – Diffie-Hellman

A – аденин

T – тимин

C – цитозин

G – гуанин

Base4 – четверичная система счисления

Base3 – троичная система счисления

ПЦР – полимеразная цепная реакция

PCR – polymerase Chain Reaction

XOR – операция, исключающая “ИЛИ”

DES – data encryption standard

IDEA – international Data Encryption Algorithm

RC5 – Rivest's Cipher 5

RC4 – Rivest's Cipher 4

SEAL – software-optimized Encryption Algorithm

ЦП – центральный процессор

ОС – операционная система

ПБайт – петабайт

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 10](#_Toc534114963)

[1 ЦИФРОВА СТЕГАНОГРАФІЯ 12](#_Toc534114964)

[1.1 Предмет, термінологія, галузь використання 12](#_Toc534114965)

[1.1.1 Предмет стеганографії, основні терміни та визначення 12](#_Toc534114966)

[1.1.2 Галузі застосування стеганографії. Практичні аспекти побудови стеганосистем 16](#_Toc534114967)

[1.2 Математична модель та структурна схема стеганосистеми 24](#_Toc534114968)

[1.2.1 Структурна схема стеганосистеми 24](#_Toc534114969)

[1.2.2 Математична модель стеганосистеми 30](#_Toc534114970)

[1.3 Атаки на стегосистеми 32](#_Toc534114971)

[1.3.1 Атаки проти систем прихованої передачі повідомлень 32](#_Toc534114972)

[1.3.2 Класифікація атак на стеганосистеми 36](#_Toc534114973)

[1.3.3 Атаки, спрямовані на видалення ЦВДЗ 37](#_Toc534114974)

[1.3.4 Геометричні атаки 42](#_Toc534114975)

[1.3.5 Криптографічні атаки 43](#_Toc534114976)

[1.3.6 Атаки проти протоколу, що використовується 44](#_Toc534114977)

[1.3.7 Методи протидії атакам на системи ЦВДЗ. Статистичний стеганоаналіз та протидії 46](#_Toc534114978)

[2 ИСПОЛЬЗОВАНИЕ ДНК В КРИПТОГРАФИИ 51](#_Toc534114979)

[2.1 Хранение данных с использование ДНК 51](#_Toc534114980)

[2.2 Процесс кодирования информации 53](#_Toc534114981)

[2.3 ДНК-криптография 55](#_Toc534114982)

[2.3.1 Криптосистема ДНК с использованием замены 56](#_Toc534114983)

[2.4 Преимущество и недостатки в использовании ДНК 58](#_Toc534114984)

[ВЫВОДЫ 59](#_Toc534114985)

[ПЕРЕЧЕНЬ ССЫЛОК 60](#_Toc534114986)

# ВВЕДЕНИЕ

Благодаря междисциплинарному развитию науки об информации, физической науки и биологической науки в области криптографии появилось много новых технологий. Новые области криптографии в основном состоят из квантовой криптографии, хаотической криптографии, ДНК-криптографии и т. д. Безопасность квантовой криптографии основана на принципе неопределенности Гейзенберга. Квантовая криптография - единственная, которая может реализовать безоговорочную безопасность в настоящее время. Мэттьюс впервые применил теорию хаоса в криптографии и предложил хаотическую схему шифрования потока, основанную на пересмотренной логистической карте. С тех пор хаотическая криптография привлекла широкое внимание, большинство исследований в области хаотической криптографии сосредоточено на криптографии с секретным ключом. Криптография ДНК, которая использует вычисления ДНК, является новой ветвью криптографии в последние годы. Используя высокую плотность хранения и высокий параллелизм молекул ДНК, такая криптография может реализовать шифрование, аутентификацию, подпись и т. д.

Между тем, криптографы с нетерпением ждут применения новых трудноразрешимых математических задач в классической криптографии. В настоящее время большинство публичных криптографических примитивов основаны на высокой стойкости некоторых математических задач в очень больших конечных абелевых группах. Выдающиеся трудные задачи состоят из проблемы факторизации больших целых чисел, задачи дискретного логарифмирования над конечным полем или эллиптической кривой и т. д. Однако благодаря квантовым алгоритмам для факторизации целых чисел и решению задачи дискретного логарифмирования большинство известных криптосистем с открытым ключом будут небезопасными, когда квантовые компьютеры станут практичными. Таким образом, это неизбежная работа по разработке эффективных криптографических схем, которые могут противостоять квантовым атакам. Собственно, с 1980-х годов несколько экспертов пытались разработать новые схемы криптографии, основанные на сложных проблемах теории групп. В 1985 году Вагнер и Мадьярик предложили подход к разработке криптосистем с открытым ключом на основе групп и полугрупп с неразрешимой проблемой слов. В 1986 году, Магливерас предложил симметричную криптосистему, основанную на специальном типе факторизации бесконечных групп, названных логарифмическими сигнатурами для конечных групп перестановок. В 2000 году Ko разработал теорию криптографии на основе кос, основанную на жесткости задачи поиска сопряжения (CSP) в группах кос. В 2004 году Эйк и Кахробаи предложили новую криптосистему на основе полициклических групп. В 2005 году Шпильрайн и Ушаков предположили, что группа Томпсона может быть хорошей платформой для построения криптосистем с открытым ключом. Между тем, активная ветвь некоммутативной криптографии, основанная на жесткости проблемы групповой факторизации, добилась больших успехов в течение последних двух десятилетий.

# 

# ЦИФРОВА СТЕГАНОГРАФІЯ

## Предмет, термінологія, галузь використання

### Предмет стеганографії, основні терміни та визначення

Інформація є одним з найцінніших предметів сучасного життя. Одержання доступу до неї з появою глобальних комп’ютерних мереж стало неймовірно простим. У той же час легкість і швидкість такого доступу значно підвищили і загрозу порушення безпеки даних при відсутності засобів щодо їх захисту, а саме загрозу неавторизованого доступу до інформації.

Завдання надійного захисту авторських прав, прав інтелектуальної власності або конфіденційних даних (які в більшості випадків мають цифрової формат) від несанкціонованого доступу є однією з найдавніших і невирішених на сьогодні проблем. У зв’язку з інтенсивним розвитком і поширенням технологій, які дозволяють за допомогою комп’ютера інтегрувати, обробляти та синхронно відтворювати різні типи сигналів (так звані мультимедійні технології), питання захисту інформації, представленої в цифровому вигляді, є надзвичайно актуальним.

Переваги подання та передачі даних у цифровому вигляді (легкість відновлення, висока потенційна завадостійкість, перспективи використання універсальних апаратних і програмних рішень) можуть бути пере-креслені з легкістю, з якою можливі їх викрадення та модифікація. Тому в усьому світі назріло питання розробки методів (засобів) захисту інформації організаційного, методологічного й технічного характеру, серед них – методи криптографії та стеганографії.

Криптографічний захист інформації – система зміни останньої з метою зробити її незрозумілою для непосвячених, приховання змісту повідомлень за рахунок їх шифрування). Цей захист не вирішує згадану вище проблему повністю, оскільки наявність шифрованого повідомлення привертає увагу, і зловмисник, заволодівши криптографічно захищеним файлом, відразу розуміє про розміщення в ньому секретної інформації й переводить всю сумарну міць своєї комп’ютерної мережі на дешифрування даних.

Приховання ж самого факту існування секретних даних при їх передачі, зберіганні або обробці є завданням стеганографії – науки, що вивчає способи та методи приховання конфіденційних відомостей.

Завдання виявлення інформації при цьому відступає на другий план і вирішується в більшості випадків стандартними криптографічними методами.

Інакше кажучи, під прихованням існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні наявності іншого (прихованого ) повідомлення, але й взагалі унеможливлення виникнення будь-яких підозр на цей рахунок, оскільки в останньому випадку проблема інформаційної безпеки вертається до стійкості криптографічного коду. Таким чином, займаючи свою нішу в забезпеченні безпеки, стеганографія не заміняє, а доповнює криптографію.

Стеганографування здійснюється різними способами. Загальною ж рисою таких способів є те, що приховуване повідомлення вбудовується в об’єкт, що не привертає увагу і потім відкрито транспортується (пересилається) адресатові. Історично напрям стеганографічного приховання інформації був першим, але згодом багато в чому був витиснутий криптографією. Інтерес до стеганографії відродився в останнє десятиліття і був викликаний широким поширенням технологій мультимедіа, що цілком закономірно, беручи до уваги зазначені вище проблеми, пов’язані із захистом інформації. Не менш важливим стала поява нових типів каналів передачі інформації, що в сукупності з першим фактором дало новий імпульс розвитку та удосконаленню стеганографії, сприяло виникненню нових стеганографічних методів, в основу яких були покладені особливості подання інформації в комп’ютерних файлах, обчислювальних мережах і т. д. Це, у свою чергу, дає можливість говорити про становлення нового напряму у сфері захисту інформації – комп’ютерної стеганографії (КС) [2; 5;11; 35].

З 1996 р. проводяться міжнародні симпозіуми із проблем приховання даних (Information Workshop on Information Hiding). Перша конференція, присвячена стеганографії, відбулася в липні 2002 р. На сьогоднішній день стеганографія є наукою, що швидко і динамічно розвивається, використовуючи при цьому методи й досягнення криптографії, цифрової обробки сигналів, теорії зв’язку та інформації.

Методи стеганографії дозволяють не тільки приховано передавати дані (так звана класична стеганографія), але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв’язку, пошуку інформації в мультимедійних базах даних і т. д. Ці обставини дозволяють у рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати деякі важливі питання захисту інформації ряду прикладних галузей.

Існує два ключових напрями використання КС: пов’язаний із цифровою обробкою сигналів (ЦОС) і непов’язаний. У першому випадку секретні повідомлення вбудовуються в цифрові дані, які, як правило, мають аналогову природу (мова, зображення, аудіо- і відеозаписи). У другому – конфіденційна інформація розміщається в заголовках файлів або пакетів даних (цей напрям не знайшов широкого застосування через відносну легкість витягання та/або знищення прихованої інформації). Переважна більшість поточних досліджень у сфері стеганографії так чи інакше пов’язана саме із ЦОС, що дозволяє говорити про цифрову стеганографію (ЦС) [5; 35].

Можна виділити принаймні дві причини популярності в наш час досліджень у сфері стеганографії: обмеження на використання криптографічних засобів у ряді країн світу та виникнення проблеми захисту прав власності на інформацію, представлену в цифровому вигляді.

Перша причина викликала велику кількість досліджень у стилі класичної стеганографії, тобто приховання властне факту передачі, а друга – не менш численні роботи у сфері так званих цифрових водяних знаків (ЦВДЗн) – спеціальних міток, приховано убудованих у зображення (або інші цифрові дані) для того, щоб мати можливість контролювати це використання.

Приховання інформації тільки на основі факту невідомості зловмисникові методу або методів, закладених в основу приховання, на сьогоднішній день є малоефективним. Ще в 1883 р. фламандський криптограф А. Керхгофс (A. Kerckhoffs) указував на той факт, що система захисту інформації повинна виконувати покладені на неї функції навіть при повній інформованості противника про її структуру та алгоритм функціонування [36].

Вся таємність системи захисту переданих повідомлень повинна втримуватися в ключі – фрагменті інформації, попередньо, як правило, розділеному між адресатами. Незважаючи на те, що цей принцип відомий уже більше 100 років, ДВТепер існують розробки, які ними зневажають. Очевидно, що вони не можуть використовуватися із серйозною метою. В основі багатьох підходів до рішення завдань стеганографії лежить загальна із криптографією методична база, яку заклав ще в середині минулого століття К. Шеннон (С. Е. Shannon) [19; 58]. Однак і ДВТепер теоретичні основи стеганографії залишаються практично непроробленими.

Беручи до уваги вищесказане, можна зробити висновок про те, що на сьогоднішній день існує актуальна науково-технічна проблема вдосконалення алгоритмів і методів проведення стеганографічного приховання конфіденційних даних або захисту авторських прав на певну інформацію.

Сьогодні немає недоліку в стеганографічних програмах як початкового, так і професійного рівня (S-Tools, Steganos Security Suite, bmpPacker та ін.). Однак захищеність їх коду (особливо це стосується програм професійного рівня) не дозволяє простежити методи, покладені в основу алгоритмів їх дії. Розміщені ж в Internet-ресурсах численні тексти програм через свою низьку інформативність мало чим допомагають, тому що компіляція запропонованих текстів виконується програмою так, що її алгоритм вкрай важко простежити, оскільки остання видає вже готовий результат – заповнений стеганоконтейнер, і практично не існує можливості заздалегідь установити достатність рівня приховання конфіденційної інформації в цьому контейнері.

Таким чином, зовсім 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.

### Галузі застосування стеганографії. Практичні аспекти побудови стеганосистем

Цифрова стеганографія як наука народилася буквально в останні роки. На думку авторів, вона містить у собі такі напрями:

* вбудовування інформації з метою її прихованої передачі;
* вбудовування цифрових водяних знаків (ЦВДЗн) (watermarking);
* вбудовування ідентифікаційних номерів (fingerprinting);
* вбудовування заголовків (captioning).

ЦВДЗн можуть застосовуватися, в основному, для захисту від копіювання та несанкціонованого використання. У зв’язку з бурхливим розвитком технологій мультимедіа гостро встало питання захисту авторських прав і інтелектуальної власності, представленої в цифровому вигляді. Прикладами можуть бути фотографії, аудіо- та відеозаписи та ін. Переваги, які дають подання та передача повідомлень у цифровому вигляді, можуть виявитися перекресленими з легкістю, з якою можливі їх викрадення або модифікація. Тому розробляються різні засоби захисту інформації, організаційного та технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в захисті об’єкта невидимих міток – ЦВДЗн. Розробки в цій сфері ведуть найбільші фірми в усьому світі. Оскільки методи ЦВДЗн почали розроблятися зовсім недавно (першою статтею на цю тему була робота [51]), то тут є багато неясних проблем, що вимагають свого вирішення.

Назву цей метод одержав від усім відомого способу захисту цінних паперів, у тому числі грошей, від підробки. Термін "digital watermarking" був уперше застосований у роботі [51]. На відміну від звичайних водяних знаків ЦВДЗн можуть бути не тільки видимими, але й, як правило, невидимими. Невидимі ЦВДЗн аналізуються спеціальним декодером, що виносить рішення про їх коректність. ЦВДЗн можуть містити деякий автентичний код, інформацію про власника або яку-небудь керуючу інформацію. Найбільш придатними об’єктами захисту за допомогою ЦВДЗн є нерухливі зображення, файли аудіо- й відеоданих.

Технологія вбудовування ідентифікаційних номерів виробників має багато загального з технологією ЦВДЗн. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний вбудований номер (звідси й назва – дослівно "відбитки пальців"). Цей ідентифікацій-ний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то "відбитки пальців" швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту й т. д. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній потенційний зловмисник.

Оскільки цифрова стеганографія є молодою наукою, то її термінологія не до кінця сформувалася. Основні поняття стеганографії були погоджені на Першій міжнародній конференції з приховання даних [21]. Проте навіть саме поняття "стеганографія" трактується по-різному. Так, деякі дослідники розуміють під стеганографією тільки приховану передачу інформації. Інші відносять до стеганографії такі додатки, як наприклад, метеорний радіозв’язок, радіозв’язок із псевдовипадковою перебудовою радіочастоти, широкосмуговий радіозв’язок. Неформальне визначення того, що таке цифрова стеганографія, могло б виглядати в такий спосіб: "наука про непомітне і надійне приховання одних бітових послідовностей в інших, що мають аналогову природу". Під це визначення саме підпадають всі чотири вищенаведені напрями приховання даних, а додатка радіозв’язку – немає. Крім того, у визначенні міститься дві головні вимоги до стеганографічному перетворення: непомітність і надійність, або стійкість до різного роду перекручування. Згадування про аналогову природу цифрових даних підкреслює той факт, що вбудовування інформації виконується в оцифровані безперервні сигнали. Таким чином, у рамках цифрової стеганографії не розглядаються питання впровадження даних у заголовки IP-пакетів і файлів різних форматів, у текстові повідомлення.

Яким б різними не були напрями стеганографії, пропоновані ними вимоги багато в чому збігаються, як це буде показано далі. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВДЗн полягає в тому, що в першому випадку зловмисник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більше того, у зловмисника на законних підставах може бути пристрій виявлення ЦВДЗн (наприклад, у складі DVD-програвача).

Під словом "непомітний" у нашому визначенні цифрової стеганографії мається на увазі обов’язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що висуває до системи передачі досить важко формалізовані вимоги.

Завдання вбудовування і виділення повідомлень із іншої інформації виконує стеганосистема. Стеганосистема складається з таких основних елементів, наведених на рис. 1.1:

прекодер – пристрій, призначений для перетворення приховуваного повідомлення до виду, зручного для вбудовування в сигнал-контейнер;

контейнером називається інформаційна послідовність, у якій ховається повідомлення;

стеганокодер – пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі; пристрій виділення убудованого повідомлення;

стеганодетектор – пристрій, призначений для визначення наявності стегаповідомлення;

декодер – пристрій, що відновлює приховане повідомлення. Цей вузол може бути відсутнім, це буде пояснено далі.

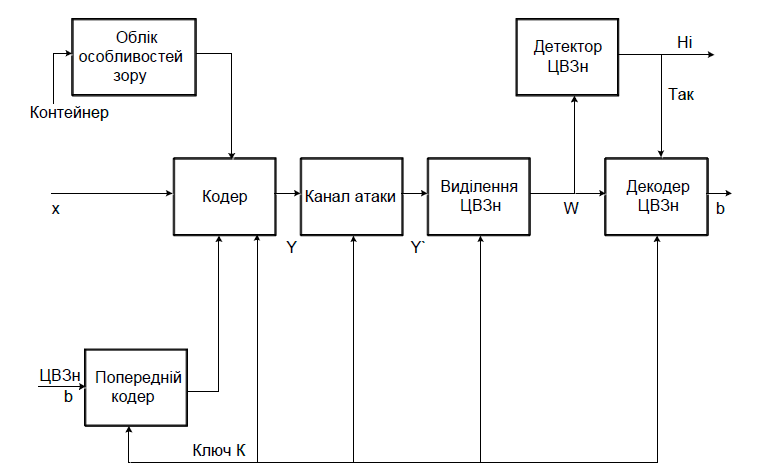


Рисунок 1.1 – Структурна схема типової стеганосистеми ЦВЗн

На рис. 1.2 наведена класифікація систем цифрової стеганографії. Стеганосистема утворює стеганоканал, по якому передається заповнений контейнер. Цей канал уважається підданим впливам з боку порушників. Згідно з Г. Сіммонсом [63], у стеганографії звичайно розгля- дається така постановка завдання ("проблема ув’язнених").

Двоє ув’язнених, Аліса і Боб бажають конфіденційно обмінюватися повідомленнями, незважаючи на те, що канал зв’язку між ними контролює охоронець Віллі. Для того щоб таємний обмін повідомленнями був можливий, передбачається, що Аліса і Боб мають деякий відомий обом секретний ключ. Дії Віллі можуть полягати не тільки в спробі виявлення прихованого каналу зв’язку, але й у руйнуванні переданих повідомлень, а також їх модифікації та створенні нових, помилкових повідомлень. Відповідно можна виділити три типи порушників, яким повинна протистояти стеганосистема: пасивний, активний і злочинний порушники. Помітимо, що пасивний зловмисник може бути лише в стеганосистемах прихованої передачі даних. Для систем ЦВДЗ характерні активні та злочинні порушники.

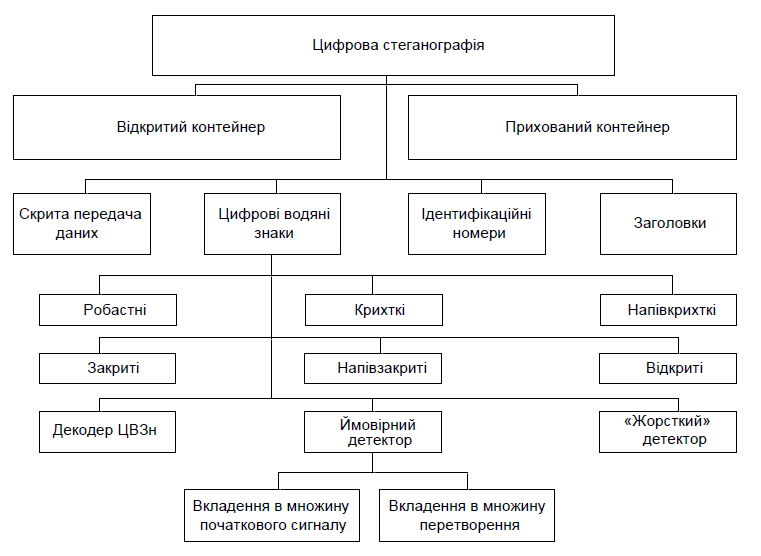


Рисунок 1.2 – Класифікація систем цифрової стеганографії

Для того щоб стеганосистема була надійною, необхідне виконання при її проектуванні ряду вимог.

Безпека системи повинна повністю визначатися таємністю ключа. Це означає, що зловмисник може повністю знати всі алгоритми роботи стеганосистеми та статистичні характеристики множин повідомлень і контейнерів, і це не дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері.

Знання зловмисником факту наявності повідомлення в якому- небудь контейнері не повинне допомогти йому при виявленні повідомлень в інших контейнерах.

Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення у візуально незначущі множини сигналу. Однак ці ж множини використовують і алгоритми стиску. Тому, якщо зображення буде надалі піддаватися стиску, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися у візуально значущі множини, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра.

Стеганосистема ЦВДЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не утримує. У деяких додатках таке виявлення може привести до серйозних наслідків. Наприклад, помилкове виявлення ЦВДЗ на DVD-диску може викликати відмову від його відтворення плеєром.

Повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна, в основному, для стеганосистем прихованої передачі інформації). У третьому розділі введемо поняття прихованої пропускної здатності й розглянемо шляхи її досягнення.

Стеганосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВДЗ, тобто складний стеганокодер і простий стеганодекодер.

До ЦВДЗ висуваються такі вимоги [5; 11; 55]:

ЦВДЗ повинен легко (обчислювально) витягатися законним користувачем;

ЦВДЗ повинен бути стійким або нестійким до навмисних і випадкових впливів. Якщо ЦВДЗ використовується для підтвердження дійсності, то неприпустима зміна контейнера повинна призводити до руйнування ЦВДЗ (тендітний ЦВДЗ). Якщо ж ЦВДЗ містить ідентифікаційний код, логотип фірми тощо, то він повинен зберігатися при максимальних перекручуваннях контейнера, що звичайно, не приводять до істотних перекручувань вихідного сигналу. Наприклад, у зображенні можуть бути відредаговані колірна гама або яскравість, в аудіозаписі – посилене звучання низьких тонів і т. п. Крім того, ЦВДЗ повинен бути працездатним стосовно афінних перетворень зображення, тобто його поворотів, масштабування. При цьому треба розрізняти стійкість самого ЦВДЗ і здатність декодера правильно його виявити. Скажемо, при повороті зображення ЦВДЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатки, коли ЦВДЗ повинен бути стійким стосовно одних перетворень і нестійким стосовно інших. Наприклад, може бути дозволене копіювання зображення (ксерокс, сканер), але накладена заборона на внесення в нього яких-небудь змін.

Повинна бути можливість додавання до стега додаткового ЦВДЗ. Наприклад, на DVD-диску є мітка про допустимість однократного копіювання. Після здійснення такого копіювання необхідно додати мітку про заборону подальшого копіювання. Можна було б, звичайно, видалити перший ЦВДЗ і записати на його місце другий, однак це суперечить припущенню про важке видалення ЦВДЗ. Кращим виходом є додавання ще одного ЦВДЗ, після якого перший не буде братися до уваги. Однак наявність декількох ЦВДЗ на одному повідомленні може полегшити атаку з боку зловмисника, якщо не почати спеціальних заходів.

У цей час технологія ЦВДЗ перебуває в початковій стадії свого розвитку. Як показує практика, повинно пройти років 10 – 20 для того, щоб новий криптографічний метод почав широко використовуватися в суспільстві. Напевно, аналогічна ситуація буде спостерігатися й зі стеганографією. Однією із проблем, пов’язаних зі ЦВДЗ, є різноманіття вимог до них, залежно від додатка. Розглянемо докладніше основні множини застосування ЦВДЗ.

Спочатку розглянемо проблему піратства, або необмеженого неавторизованого копіювання. Наприклад, Аліса продає своє мультимедійне повідомлення Пітеру. Хоча інформація могла бути зашифрована під час передачі, ніщо не перешкодить Пітеру зайнятися її копіюванням після розшифрування. Отже, у цьому випадку потрібен додатковий рівень захисту від копіювання, що не може бути забезпечений традиційними методами. Існує можливість впровадження ЦВДЗ, що дозволяє відтворення та забороняє копіювання інформації.

Важливою проблемою є визначення дійсності отриманої інформації, тобто її автентифікація. Звичайно для автентифікації даних використовуються засоби цифрового підпису. Однак ці засоби не зовсім підходять для забезпечення автентифікації мультимедійної інформації. Справа в тому, що повідомлення, постачене електронним цифровим підписом, повинне зберігатися й передаватися абсолютно точно, "бітів у бітів". Мультимедійна ж інформація може незначно спотворюватися як при зберіганні (за рахунок стиску), так і при передачі (вплив одиночних або пакетних помилок у каналі зв’язку). При цьому її якість залишається припустимою для користувача, але цифрової підпис працювати не буде. Одержувач не зможе відрізнити справжнє, хоча і трохи перекручене повідомлення, від помилкового. Крім того, мультимедійні дані можуть бути перетворені з одного формату в іншій. При цьому традиційні засоби захисту цілісності працювати також не будуть. Можна сказати, що ЦВДЗ здатно захистити саме зміст аудіо-, відеоповідомлення, а не його цифрове подання у вигляді послідовності бітів. Крім того, важливим недоліком цифрового підпису є те, що його легко видалити із завіреного ним повідомлення, після чого прилаштувати до нього новий підпис. Видалення підпису дозволить зловмиснику відмовитися від авторства, або ввести в оману законного одержувача щодо авторства повідомлення. Система ЦВДЗ проектується таким чином, щоб виключити можливість подібних порушень. Як видно з рис. 1.3 застосування ЦВДЗ не обмежується додатками безпеки інформації.



Рисунок 1.3 – Потенційні множини застосування стеганографії

Основні множини використання технології ЦВДЗ можуть бути об’єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації та прихований зв’язок.

Популярність мультимедіа-технологій викликало множину досліджень, пов’язаних з розробкою алгоритмів ЦВДЗ для використання в стандартах MP3, MPEG-4, JPEG2000, захисту DVD- дисків від копіювання.

1.2 Математична модель та структурна схема стеганосистеми

1.2.1 Структурна схема стеганосистеми

У загальному випадку стеганосистема може бути розглянута як система зв’язку [24]. Узагальнена структурна схема стеганосистеми наведена на рис. 1.4.

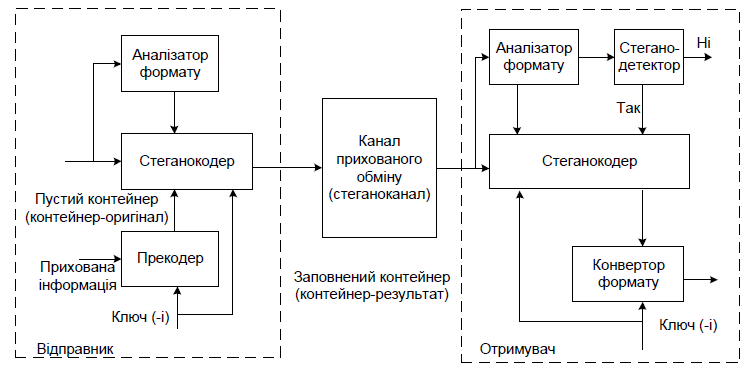


Рисунок 2.1 – Структурна схема стеганосистеми як системи зв’язку

Основними стеганографічними поняттями є повідомлення і контейнер.

Повідомлення m M – це секретна інформація, наявність якої необхідно приховати, – множина всіх повідомлень.

Контейнером с С називається несекретна інформація, яку можна використовувати для приховання повідомлення , – множина всіх контейнерів, причому q >> n. Як повідомлення та контейнер можуть виступати як звичайний текст, так і файли мультимедійного формату

Порожній контейнер (або так званий контейнер-оригінал) – це контейнер с, що не містить прихованої інформації. Заповнений контейнер (контейнер-результат) – контейнер с, що містить приховану інформацію m (сm). Одна з вимог, що при цьому висувається: контейнер-результат не повинен візуально відрізнятися від контейнера-оригіналу. Виділяють два основних типи контейнера: потоковий і фіксований.

Потоковий контейнер становить послідовність бітів, що безупинно змінюються. Повідомлення вбудовується в нього в реальному масштабі часу, тому в кодері заздалегідь невідомо, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути убудовано кілька повідомлень. Інтервали між убудованими бітами визначаються генератором псевдовипадкової послідовності (ПВП) із рівномірним розподілом інтервалів між відліками.

Основна проблема полягає у виконанні синхронізації, визначенні початку та кінця послідовності. Якщо в даних контейнера існують біти синхронізації, заголовки пакетів тощо, то прихована інформація може випливати відразу ж після них. Складність організації синхронізації є перевагою з погляду забезпечення прихованості передачі. На жаль, на сьогоднішній день практично відсутні роботи, присвячені розробці стеганосистем з потоковим контейнером.

Як приклад перспективної реалізації потокового контейнера можна навести стеганоприставку до звичайного телефону. При цьому під прикриттям пересічної, несуттєвої телефонної розмови можна передавати іншу розмову, дані та ін. Не знаючи секретного ключа, не можна не тільки довідатися про зміст прихованої передачі, але й про самий факт її існування.

У фіксованому контейнері розміри і характеристики останнього заздалегідь відомі. Це дозволяє виконувати вкладення даних оптимальним (у визначеному змісті) чином. Далі будуть розглядатися переважно фіксовані контейнери (надалі – контейнери).

Контейнер може бути вибраним, випадковим або нав’язаним. Вибраний контейнер залежить від убудованого повідомлення, а в граничному випадку є його функцією. Такий тип контейнера більше характерний саме для стеганографії. Нав’язаний контейнер з’являється, коли особа, що надає контейнер, підозрює про можливу приховану переписку і бажає їй запобігти. На практиці ж найчастіше мають справу з випадковим контейнером.

Приховання інформації, що переважно має великий обсяг, висуває істотні вимоги до контейнера, розмір якого повинен щонайменше в кілька разів перевищувати розмір даних, що вбудовуються. Зрозуміло, що для збільшення прихованості зазначене співвідношення повинне бути як можна більшим.

Перед тим як виконати вкладення повідомлення в контейнер, його необхідно перетворити в певний зручний для впакування вид. Крім того, перед упакуванням у контейнер, для підвищення захищеності секретної інформації останню можна зашифрувати досить стійким криптографічним кодом. У багатьох випадках також бажана стійкість отриманого стегаповідомлення до перекручувань (у тому числі і злочинних).

У процесі передачі звук, зображення або яка-небудь інша інформація, використовувана як контейнер, може піддаватися різним трансформаціям (у тому числі з використанням алгоритмів із втратою даних): зміна обсягу, перетворення в інший формат і т. п., тому для збереження цілісності убудованого повідомлення може знадобитися використання коду з виправленням помилок (завадостійке кодування).

Початкову обробку приховуваної інформації виконує наведений на рис. 2.1 прекодер. Як одну з найважливіших попередніх обробок повідомлення (а також і контейнера) можна назвати обчислення його узагальненого перетворення Фур’є. Це дозволяє здійснити вбудовування даних у спектральній множині, що значно підвищує їх стійкість до перекручувань.

Слід зазначити, що для збільшення таємності вбудовування попередня обробка досить часто виконується з використанням ключа.

Упакування повідомлення в контейнер (з урахуванням формату даних, що представляють контейнер) виконуються за допомогою стегакодера. Вкладення відбувається, наприклад, шляхом модифікації найменших значущих бітів контейнера. Взагалі, саме алгоритм (стратегія) внесення елементів повідомлення в контейнер визначає методи стеганографії, які, у свою чергу, діляться на визначені групи, наприклад, залежно від того, файл якого формату був обраний як контейнер.

У більшості стеганосистем для впакування та витягнення повідомлень використовується ключ, що визначає секретний алгоритм, який визначає порядок внесення повідомлення в контейнер. За аналогією із криптографією, тип ключа спричиняє існування двох типів стеганосистем :

з секретним ключем – використовується один ключ, що визначається до початку обміну стеганограмою або передається захищеним каналом;

з відкритим ключем – для впакування та розпакування повідомлення використовуються різні ключі, які відрізняються таким чином, що за допомогою обчислень неможливо одержати один ключ із іншого, тому один із ключів (відкритий) може вільно передаватися по незахищеному каналу. Як секретний алгоритм може бути використаний генератор псевдовипадкової послідовності бітів. Якісний генератор ПВП, орієнтований на використання в системах захисту інформації, повинен відповідати певним вимогам. Перелічимо деякі з них.

Криптографічна стійкість – відсутність у зловмисника можливості передбачити наступний бітів на підставі відомих йому попередніх з імовірністю, відмінною від 1/2. На практиці криптографічна стійкість оцінюється статистичними методами. Національним інститутом стандартів і технологій США (НІСТ) розроблений посібник із проведення статистичних випробувань генераторів ПВП, орієнтованих на використання в задачах криптографічного захисту інформації.

Статистичні властивості – ПВП за своїми статистичними властивостями не повинна істотно відрізнятися від істинно випадкової послідовності.

Великий період формованої послідовності.

Ефективна апаратно-програмна реалізація. Статистично (криптографічно) безпечний генератор ПВП повинен відповідати таким вимогам:

жоден статистичний тест не визначає в ПВП ніяких закономірностей, іншими словами, не відрізняє цю послідовність від істинно випадкової;

при ініціалізації випадковими значеннями генератор породжує статистично незалежні псевдовипадкові послідовності.

Як основа генератора може використовуватися, наприклад, лінійний рекурентний регістр. Тоді адресатам для забезпечення зв’язку повинне повідомлятися початкове заповнення цього регістра. Числа, породжувані генератором ПВП, можуть визначати позиції модифікованих відліків у випадку фіксованого контейнера або інтервали між ними у випадку потокового контейнера.

Слід зазначити, що метод випадкового вибору величини інтервалу між убудованими бітами не є досить ефективним за двома причинами. По-перше, приховані дані повинні бути розподілені по всьому контейнеру, тому рівномірний розподіл довжини інтервалів (від найменшого до найбільшого) може бути досягнуто тільки приблизно, оскільки повинна існувати впевненість у тому, що все повідомлення убудоване (тобто помістилося в контейнер). По-друге, довжина інтервалів між відліками шуму (у багатьох моделях сигнал-контейнер розглядається як адитивний шум) розподілена не за рівномірним, а за експонентним законом. Генератор ПВП із експонентним розподілом інтервалів складний у реалізації. Приховувана інформація заноситься відповідно до ключа в ті біти, модифікація яких не приводить до істотних перекручувань контейнера. Ці біти утворять так званий стеганошлях. Під "істотним" мається на увазі перекручування, що приводить до зростання ймовірності виявлення факту наявності прихованого повідомлення після проведення стеганоаналізу.

Стеганографічний канал – канал передачі контейнера-результату (взагалі, існування каналу як, власне кажучи, і одержувача – найбільш узагальнений випадок, оскільки заповнений контейнер може, наприклад, зберігатися у "відправника’’, що поставив перед собою мету обмежити неавторизований доступ до певної інформації. У цьому випадку відправник виступає в ролі одержувача). Під час перебування в стеганографічному каналі контейнер, що містить приховане повідомлення, може піддаватися навмисним атакам або випадковим перешкодам.

У стеганодетекторі визначається наявність у контейнері (можливо вже зміненому) прихованих даних. Ця зміна може бути обумовлена впливом помилок у каналі зв’язку, операцій обробки сигналу, навмисних атак порушників. Як вже відзначалося вище, у багатьох моделях стеганосистем сигнал-контейнер розглядається як адитивний шум. Тоді завдання виявлення й виділення стеганоспілкування є класичним для теорії зв’язку. Але такий підхід не враховує двох факторів: невипадкового характеру контейнера й вимог зі збереження його якостей. Ці моменти не зустрічаються у відомій теорії виявлення й виділення сигналів на тлі адитивного шуму. Очевидно, що їх облік дозволить побудувати більш ефективні стеганосистеми.

Розрізняють стеганодетектори, призначені тільки для виявлення факту наявності убудованого повідомлення, і пристрої, призначені для виділення цього повідомлення з контейнера, – стеганодекодери.

Отже, у стеганосистемі відбувається об’єднання двох типів інформації таким чином, щоб вони по-різному сприймалися принципово різними детекторами. У якості одного з детекторів виступає система виділення прихованого повідомлення, у якості іншого – людина.

Алгоритм вбудовування повідомлення в найпростішому випадку складається із двох основних етапів:

Вбудовування в стегакодері секретного повідомлення в контейнер- оригінал.

Виявлення (виділення) у стеганодетекторі (декодері) прихованого зашифрованого повідомлення з контейнера-результату.

1.2.2 Математична модель стеганосистеми

Виходячи із цього, слід розглянути математичну модель стеганосистеми. Процес тривіального стеганографічного перетворення описується залежностями:



(2.1)



(2.2)

де

* множина контейнерів-результатів (стеганограм).

Залежність (2.1) описує процес приховання інформації, залежність (2.2) – витягнення прихованої інформації. Необхідною умовою при цьому є відсутність "перетинання" [11], тобто, якщо , причому , а , , то .

Крім того, необхідно, щоб потужність множини . При цьому обидва адресати (відправник і одержувач) повинні знати алгоритм прямого (Е) і зворотного (D) стеганографічних перетворень.

Отже, у загальному випадку стеганосистема – це сукупність  
 контейнерів (оригіналів і результатів), повідомлень і перетворень, які їх пов’язують.

Для більшості стеганосистем множина контейнерів C вибирається таким чином, щоб у результаті стеганографичного перетворення (2.1) заповнений контейнер і контейнер-оригінал були подібні, що формально може бути оцінене за допомогою функції подоби [11; 46; 51].

Визначення 1.1. Нехай C – непуста множина, тоді функція   
є функцією подоби на множині С, якщо для яких-небудь справедливо, що у випадку та при при .

Стеганосистема може вважатися надійною, якщо для всіх m ∈ M і c ∈ C, причому як контейнер с повинен обиратися такий, котрий раніше не використовувався. Крім того, неавторизована особа не повинна мати доступ до набору контейнерів, використовуваних для секретного зв’язку.

Вибір визначеного контейнера із набору можливих контейнерів С може здійснюватися довільно (так званий сурогатний метод вибору контейнера) або шляхом обрання найбільш придатного, котрий менше інших зміниться під час стеганоперетворення (селективний метод). В останньому випадку контейнер обирається відповідно до правила:

Також слід зазначити, що функції прямого (E) і зворотного (D) стеганографічних перетворень в загальному випадку можуть бути довільними (але, звичайно, відповідають одна одній), однак на практиці вимоги до стійкості прихованої інформації накладають на зазначені функції визначені обмеження. Так, у переважній більшості випадків, , або   
 – тобто незначно модифікований контейнер (на величину δ) не повинен приводити до зміни прихованої в ньому інформації.

1.3 Атаки на стегосистеми

1.3.1 Атаки проти систем прихованої передачі повідомлень

Повернемося до розглянутої в попередніх лекціях стеганосистеми, призначеної для прихованої передачі повідомлень. Дослідимо докладніше можливості зловмисника Віллі за протидією Алісі й Бобу. Як відзначалося, зловмисник може бути пасивним, активним і злочинним. Залежно від цього він може створювати різні загрози.

Пасивний зловмисник може лише виявити факт наявності стегаканалу й, можливо, читати повідомлення. Чи зможе він прочитати повідомлення після його виявлення залежить від стійкості системи шифрування, і це питання, як правило, не розглядається в стеганографії. Якщо у Віллі є можливість виявити факт наявності прихованого каналу передачі повідомлень, то стеганосистема звичайно вважається нестійкою. Хоча існують і інші точки зору на стійкість стеганосистем. Здійснення виявлення стегаканалу є найбільш трудомістким завданням, а захист від виявлення вважається основним завданням стеганографії, за визначенням. Діапазон дій активного зловмисника значно ширше. Сховане повідомлення може бути їм вилучено або зруйновано. У цьому випадку Боб і, можливо, Аліса довідаються про факт втручання. У більшості випадків це суперечить інтересам Віллі (наприклад, за юридичними мотивами). Інша справа – видалення або руйнування цифрового водяного знака, які можуть розглядатися як основні загрози в цій множині.

Дії злочинного зловмисника найнебезпечніші. Він здатний не тільки руйнувати, але й створювати помилкові стеги. Історія протистояння розвідки й контррозвідки знає чимало прикладів, коли реалізація цієї загрози приводила до катастрофічних наслідків. Ця загроза актуальна й стосовно систем ЦВЗ. Маючи здатність створювати водяні знаки, зловмисник може створювати копії контента, що захищається, створювати помилкові оригінали й т. д. У багатьох випадках зловмисник може створювати помилкові стеги без знання ключа.

Для здійснення тієї або іншої загрози зловмисник застосовує атаки.

Найбільш проста атака – суб’єктивна. Віллі уважно розглядає зображення (слухає аудіозапис), намагаючись визначити "на око", чи є в ньому приховане повідомлення. Ясно, що подібна атака може бути проведена лише проти зовсім незахищених стеганосистем . Проте вона, напевно, найпоширеніша на практиці, принаймні, на початковому етапі розкриття стеганосистеми. Первинний аналіз також може містити в собі такі заходи [5; 11]:

* Первинне сортування стега за зовнішніми ознаками.
* Виділення стега з відомим алгоритмом вбудовування.
* Визначення використаних стегаалгоритмів.
* Перевірка достатності обсягу матеріалу для стеганоаналізу.
* Перевірка можливості проведення аналізу по окремих випадках.
* Аналітична розробка стегаматеріалів. Розробка методів розкриття стеганосистеми.
* Виділення стега з відомими алгоритмами вбудовування, але невідомими ключами та ін.

Із криптоаналізу нам відомі такі різновиди атак на шифровані повідомлення [5; 7; 11]:

* атака з використанням тільки шифртексту;
* атака з використанням відкритого тексту;
* атака з використанням обраного відкритого тексту;
* адаптивна атака з використанням відкритого тексту;
* атака з використанням обраного шифртексту.

За аналогією із криптоаналізом у стегааналізі можна виділити такі типи атак [23; 27]:

Атака на основі відомого заповненого контейнера. У цьому випадку у зловмисника є один або трохи стегів. В останньому випадку передбачається, що вбудовування прихованої інформації здійснювалося Алісою тим самим способом. Завдання Віллі може полягати у виявленні факту наявності стегаканалу (основною), а також у його витягненні або визначенні ключа. Знаючи ключ, зловмисник одержить можливість аналізу інших стегаповідомлень.

Атака на основі відомого збудованого повідомлення. Цей тип атаки більшою мірою характерний для систем захисту інтелектуальної власності, коли як водяний знак використовується відомий логотип фірми. Завданням аналізу є одержання ключа. Якщо відповідному схованому повідомленню заповнений контейнер невідомий, то завдання вкрай важко розв’язуване.

Атака на основі обраного прихованого повідомлення. У цьому випадку Віллі має можливість пропонувати Алісі проаналізувати повідомлення яке пропонується для передачі у стеганосистемі.

Адаптивна атака на основі обраного прихованого повідомлення. Ця атака є частковим випадком попередньої атаки. У цьому випадку Віллі має можливість вибирати повідомлення для нав’язування Алісі адаптивно, залежно від результатів аналізу попередніх стегів.

Атака на основі обраного заповненого контейнера. Цей тип атаки більш характерний для систем ЦВЗ. Стегааналітик має детектор стега у вигляді "чорного ящика" і трохи стегів. Аналізуючи детектировані приховані повідомлення, зловмисник намагається розкрити ключ.

У Віллі може бути можливість застосувати ще три атаки, що не мають прямих аналогій у криптоаналізі.

Атака на основі відомого порожнього контейнера. Якщо він відомий Віллі, то шляхом порівняння його з передбачуваним стегом він завжди може встановити факт наявності стегаканалу. Незважаючи на тривіальність цього випадку, у ряді робіт приводиться його інформаційно-теоретичне обґрунтування. Набагато цікавіше сценарій, коли контейнер відомий приблизно, з деякою погрішністю (як це може мати місце при додаванні до нього шуму).

Атака на основі обраного порожнього контейнера. У цьому випадку Віллі здатний змусити Алісу користуватися запропонованим їй контейнером. Наприклад, запропонований контейнер може мати більші однорідні множини (однотонні зображення), і тоді буде важко забезпечити таємність впровадження.

Атака на основі відомої математичної моделі контейнера або його частини. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі. Наприклад, допустимо, що біти усередині відліку зображення корельовані. Тоді відсутність такої кореляції може служити сигналом про наявне приховане повідомлення. Завдання повідомлення полягає у тому, щоб не порушити статистики контейнера. Впроваджуючий й атакуючий можуть мати у своєму розпорядженні різні моделі сигналів, тоді в протиборстві, що інформаційно приховує, переможе той, що має кращу модель.

Розглянуті вище атаки мають одну особливість: вони не змінюють стегаповідомлення, що посилаються Алісою, а також не спрямовані на протидію роботи декодера Боба. У цьому полягає їхня позитивна сторона: дії Віллі навряд чи здатні насторожити Алісу й Боба. Порівняння працездатності стеганосистем виробляється звичайно стосовно деяких стандартних тестів. У якості одного з них є атака, заснована на застосуванні алгоритму стиску JPEG (досить неефективна атака). Набагато більше подання про достоїнства того або іншого стегаалгоритму можна одержати, комплексно використовуючи різні атаки. Загальнодоступна в Internet програма Stirmark дозволяє більш повно аналізувати працездатність стегаалгоритмів. За твердженням творців програми на сьогоднішній день не існує загальновідомого стегаалгоритму, стійкого до їх комплексних атак.

Тому розроблювачами надається велике значення забезпеченню завадостійкості впровадження ЦВЗ. Це досягається, як правило, розширенням спектра прихованого повідомлення або застосуванням завадостійких кодів. Системи з розширенням спектра широко застосовуються у зв’язку для завадостійкої передачі сигналів. Але чи є вони досить завадостійкими для застосування у ЦВЗ? Виявляється, далеко не завжди. Розглянемо пропоновані дослідниками методи атак і протидії їм.

### 1.3.2 Класифікація атак на стеганосистеми

Можлива різна класифікація атак на стеганосистеми. Розглянемо атаки, специфічні для систем ЦВЗ. Можна виділити наступні категорії атак проти таких стеганосистем [28; 29; 44;56]:

1. Атаки проти збудованого повідомлення – спрямовані на видалення або псування ЦВДЗ шляхом маніпулювання стега. Вхідні в цю категорію методи атак не намагаються оцінити й виділити водяний знак. Прикладами таких атак можуть бути лінійна фільтрація, стиск зображень, додавання шуму, вирівнювання гістограми, зміна контрастності й т. д.

2. Атаки проти стегадетектора – спрямовані на те, щоб утруднити або унеможливити правильну роботу детектора. При цьому водяний знак у зображенні залишається, але губиться можливість його прийому. У цю категорію входять такі атаки, як афінні перетворення (тобто масштабування, зсуви, повороти), усікання зображення, перестановка пікселів і т. д.

3. Атаки проти протоколу використання ЦВЗ – в основному пов’язані зі створенням помилкових ЦВДЗ, помилкових стегів, інверсією ЦВДЗ, додаванням декількох ЦВДЗ.

4. Атаки проти самого ЦВДЗ – спрямовані на оцінювання й витягнення ЦВДЗ зі стегаповідомлення, по можливості без перекручування контейнера. У цю групу входять такі атаки, як атаки змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації [56] та ін.

Треба відмітити, що розглянута класифікація атак не є єдино можливою й повною. Крім того, деякі атаки (наприклад, видалення шуму) можуть бути віднесені до декількох категорій. У роботі [44] була запропонована інша класифікація атак, що також має свої достоїнства й недоліки.

Відповідно до цієї класифікації всі атаки на системи вбудовування ЦВДЗ можуть бути розділені на чотири групи:

1) атаки, спрямовані на видалення ЦВДЗ;

2) геометричні атаки, спрямовані на перекручування контейнера;

3) криптографічні атаки;

4) атаки проти використовуваного протоколу вбудовування й перевірки ЦВДЗ.

1.3.3 Атаки, спрямовані на видалення ЦВДЗ

До цієї групи відносяться такі атаки, як очищення сигналів-контейнерів від шумів, перемодуляція, стиснення з втратами (квантування), усереднення і колізії. Ці атаки засновані на припущенні про те, що ЦВДЗ є статистично описуваним шумом. Очищення від шуму полягає в фільтрації сигналу з використанням критеріїв максимальної правдоподібності або максимуму апостеріорної імовірності. В якості фільтра, що реалізує критерій максимальної правдоподібності, може використовуватися медіа (для ЦВДЗ, що має розподіл Лапласа) або усереднюючий (для гаусівського розподілу) фільтр, який застосовують у програмному пакеті StirMark. За критерієм максимуму апостеріорної ймовірності найкращим буде адаптивний фільтр Вінера (у випадку, якщо в якості моделі контейнера використовується нестаціонарний гаусівський процес), а також порогові методи очищення від шуму (м’які і жорсткі пороги) (модель – узагальнений гаусівський процес), які мають багато спільного з методами стиснення з втратами.

Стиснення з втратами та очищення сигналів від шумів значно зменшують пропускну здатність стегаканалу, особливо для гладких галузей зображення, коефіцієнти перетворення яких можуть бути "обнулені" без помітного зниження якості відновленого зображення.

Перемодуляція – порівняно новий метод, який є специфічним саме для атак на ЦВДЗ. Атака перемодуляції була вперше запропонована в роботі [56]. У даний час відомі її різні варіанти, залежно від використовуваного в стеганосистемі декодера. У побудові атаки є свої нюанси для стеганосистеми М-ї модуляції, стеганосистеми, що використовують коди завадостійкості, які використовують кореляційний декодер. У будь-якому випадку вважається, що ЦВДЗ впроваджений у зображення з застосуванням широкосмугових сигналів і розмножений на всі зображення. Оскільки оцінюваний декодером ЦВДЗ корельований з істинним, з’являється можливість обману декодера. Атака будується таким чином. Спочатку ЦВДЗ "пророкує" шляхом вирахування фільтрованої версії зображення з захищеного зображення (застосо-вується медіанний фільтр). "Пророкований" ЦВДЗ піддається ВЧ-фільтрації, урізається, множиться на два і віднімається з вихідного зображення. Крім того, якщо відомо, що при впровадженні ЦВДЗ множився на деяку маску для підвищення непомітності вбудованості, то атакуючий оцінює цю маску і домножує на неї ЦВДЗ. В якості додаткової засоби в "обмані" декодера вважається ефективним вбудовування в високочастотні множини зображення (де спотворення непомітні) шаблонів, які мають не гаусівський розподіл. Таким чином буде порушено оптимальність лінійного кореляційного детектора.

Така атака буде ефективною лише проти високочастотного ЦВДЗ, тому реальні ЦВДЗ будуються так, щоб їх спектр відповідав спектру вихідного зображення. Справа в тому, що достовірна оцінка виходить лише для високочастотних компонент ЦВДЗ. Після її вирахування низькочастотна компонента ЦВДЗ залишається незмінною і дає в детекторі позитивний кореляційний відгук. Високочастотна ж складова дасть негативний відгук, що в сумі дасть нуль, і ЦВДЗ не буде виявлено. В якості другої протидії цій атаці було запропоновано виконання попередньої низькочастотної фільтрації.

У роботі [37] наведена модифікація цього алгоритму, що полягає в застосуванні фільтра Вінера замість медіанного і більш інтелектуального способу знаходження коефіцієнта множення. Він вибирається так, щоб мінімізувати коефіцієнт взаємної кореляції між ЦВДЗ і стегом. Крім того, додається ще один крок: накладення випадкового шуму. Ця атака не працює проти адаптивно вбудованого ЦВДЗ, оскільки у ній передбачається, що ЦВДЗ і стег є стаціонарним гаусівським процесом з нульовим середнім. Ясно, що це припущення не виконується також і для реальних зображень. Тому С. Волошиновським та іншими запропонована атака, в якій сигнали моделюються як не стаціонарний гаусівський або узагальнений стаціонарний гаусівський процес [38]. Коефіцієнт множення ЦВДЗ вибирається виходячи з локальних властивостей зображення. Замість накладення випадкового шуму запропоновано додавати відліки зі знаком, протилежним знаку відліку ЦВДЗ (в припущенні, що ЦВДЗ є послідовністю біполярних символів). Це ще більше ускладнює роботу кореляційного детектора. Звичайно, знаки потрібно змінювати не у всіх, а тільки у частині відліків оцінюваного ЦВДЗ, наприклад, випадково.

До інших атак цієї групи відносяться атаки усереднення і змови. У разі наявності великої кількості копій стега з різними ЦВДЗ або з різними ключами впровадження можна виконати їх усереднення. Наприклад, кадри відеосигналу можуть мати різні ЦВДЗ. Якщо ЦВДЗ мав нульове середнє, то після усереднення він буде відсутній у зображенні.

Атака шляхом статистичного усереднення наведена в [56]. Зловмисник може спробувати оцінити ЦВДЗ і вирахувати його з зображення. Такий вид атак особливо небезпечний у випадку, коли атакуючий може отримати певний узагальнений ЦВДЗ, наприклад, деякий , не залежних сильно від вихідного зображення .

Атакуючий може виявити ЦВДЗ шляхом усереднення декількох зображень. Наприклад, у нього є . Тоді їх сума буде досить близька до якщо N велике, а зображення статистично незалежні.

Протидією подібної атаки може бути випадкове використання одного із двох ЦВДЗ з ймовірностями й . Тоді вищенаведена атака дасть лише .

Однак атака може бути поліпшена в тому випадку, якщо в атакуючого є якісь припущення про те, який ЦВДЗ із двох убудований у дане зображення. Тоді всі зображення можуть бути розподілені на два класи: 1 й 2. Нехай – ймовірність того, що зображення віднесене до невірного класу. Тоді усереднення по великій кількості зображень класу 1 дає . Аналогічне усереднення по зображень класу 2 дає.

Обчислення зваженої різниці дає

Отже, для будь-якого , що атакує, може оцінити суму й різницю та , звідки він може одержати та .

При атаці змови є кілька однакових копій, що містять різні ЦВДЗ, а для атаки з кожної копії вибираються якісь частини, які в сукупності й утворять атаковану множину. Атаки на основі "змови" описані, наприклад, у роботах [28; 29]. Чим більше утримуючих стеги копій є в зловмисника, тим вище ймовірність того, що близьке до вихідного реконструйоване зображення не буде містити стеги. У стегасистемах із закритим ключем така атака не настільки ефективна в силу того, що атакуючий не може перевірити, чи містять апроксимації ЦВДЗ, що в нього виходять. Це підвищує безпеку стеганосистем із закритим ключем. Захищеність від цієї атаки можна також підвищити за рахунок спеціальної побудови стега.

Ще одна ефективна атака на ЦВДЗ називається мозаїчною [29]. Ця атака спрямована на пошукові системи, що відслідковують незаконно розповсюджувані зображення. Зображення розбивається на кілька частин, так що пошукова система ЦВДЗ не виявляє. Internet-браузер демонструє фактично кілька шматочків зображення, близько розташованих один від одного, так що в цілому зображення виглядає неспотвореним. Для протидії такій атаці ЦВДЗ повинен виявлятися навіть у малих частинах зображення. Це дуже складна вимога, навіть більш важка, ніж робастність до обрізання країв зображення, тому що в останньому випадку атакуючий обмежений необхідністю збереження якості зображення. Напевно, більш здійсненним було б створення інтелектуальних пошукових систем, здатних "зібрати" зображення зі шматочків і перевірити наявність у ньому ЦВДЗ.

Цікава і практично значуща атака запропонована в роботі [57]. Вона заснована на оцінюванні ЦВДЗ, але не в множині вихідного зображення, а у його гістограмі. Атака особливо ефективна проти систем неадаптивних систем ЦВДЗ, але може бути використана й для оцінювання адаптивно впровадженого ЦВДЗ.

Пояснити атаку можна на такому прикладі. Нехай ЦВДЗ , а у вихідному зображенні є ізольоване значення піксела. Наприклад, значення 200 зустрічається 300 разів, а значення 199 та 201 – жодного разу. Тоді після впровадження ЦВДЗ значення 199 і 201 зустрінуться приблизно 150 разів, а значення 200 – жодного разу. Це і є демаскуюча ознака. Як показано на прикладі в роботі [57], цей метод може бути застосований і у випадку наявності на гістограмі зображення декількох ненульових значень, розділених трьома і більше нулями.

Для успішного використання гістограмної атаки запропоновано виконувати попереднє згладжування зображення-контейнера. Тоді зменшується діапазон значень кольорів й з’являється багато нульових ланцюжків. Утім, ефективність атаки підвищується в результаті згладжування не для всіх зображень.

У роботі [57] показано також, як гістограмна атака підсилюється при наявності декількох зображень, тобто у випадку її комбінування з атакою змови.

1.3.4 Геометричні атаки

На відміну від атак видалення, геометричні атаки прагнуть не видалити ЦВДЗ, а змінити його шляхом внесення просторових або часових перекручувань. Геометричні атаки математично моделюються як афінні перетворення з невідомим декодеру параметром. Усього є шість афінних перетворень: масштабування, зміна пропорцій, повороти, зсуви і усікання. Ці атаки приводять до втрати синхронізації в детекторі ЦВДЗ і можуть бути локальними або глобальними, тобто застосованими до всього сигналу. При цьому можливо вирізання окремих пікселів або рядків, перестановка їх місцями, застосування різних перетворень і т. д. Подібні атаки реалізовані в програмах Unsign (локальні атаки) і Stirmark (локальні та глобальні атаки).

Існують і більш "інтелектуальні" атаки на застосовуваний метод синхронізації ЦВДЗ. Основна ідея цих атак полягає в розпізнаванні методу синхронізації і руйнуванні його шляхом згладжування піків в амплітудному спектрі ЦВДЗ. Атаки ефективні в припущенні про те, що у якості механізмів синхронізації використовуються періодичні шаблони. При цьому для забезпечення синхронізації можуть використовуватися два підходи: вбудовування піків у спектральній множині, або періодичне впровадження послідовності ЦВДЗ. В обох випадках у спектрі утворяться піки, які руйнуються в розглянутій атаці. Після руйнування можна застосовувати інші геометричні атаки: синхронізації вже немає.

Сучасні методи вбудовування ЦВДЗ робастні до глобальних атак. У них застосовуються спеціальні методи відновлення синхронізації, що мають багато загального із застосовуваними в техніці зв’язку. Робастність досягається за рахунок використання інваріантних до зсуву галузей [40], застосування опорного ЦВДЗ [6], обчислення автокореляційної функції ЦВДЗ.

Якщо забезпечення робастності до глобальних геометричних атак є більш-менш вирішеним завданням, то забезпечення стійкості до локальних змін зображення є відкритим питанням. Ці атаки засновані на тому, що людське око мало чутливе до невеликих локальних змін картинки.

1.3.5 Криптографічні атаки

Криптографічні атаки названі так тому, що вони мають аналоги у криптографії. До них відносяться атаки з використанням оракула, а також злом за допомогою "грубої сили".

Атака з використанням оракула дозволяє створити незахищене ЦВДЗ зображення при наявності в зловмисника детектора. У роботі [49] досліджується стійкість ЦВДЗ на основі розширення спектра до атаки при наявності детектора у вигляді "чорного ящика". Метод полягає в експериментальному вивченні поводження детектора для з’ясування того, на які зображення він реагує, а на які – ні. Наприклад, якщо детектор виносить "м’які" рішення, тобто показує ймовірність наявності стега в сигналі, то атакуючий може з’ясувати, які невеликі зміни в зображенні впливають на поводження детектора. Модифікуючи зображення піксел за пікселем, він може взагалі з’ясувати, який алгоритм використовує детектор. У випадку детектора з "жорстким" рішенням атака здійснюється біля границі, де детектор міняє своє рішення з "є присутнім" на "відсутній".

Приклад атаки на детектор з жорстким рішенням:

1. На основі наявного зображення, що містить стеганоповідомлення, створюється тестове зображення. Тестове зображення може бути створено різними шляхами, модифікуючи вихідне зображення ДВТи, доки детектор не покаже відсутності ЦВДЗ. Наприклад, можна поступово зменшувати контрастність зображення, або піксел за пікселем заміняти дійсні значення якимись іншими.

2. Атакуючий збільшує або зменшує значення якого-небудь піксела ДВТи, доки детектор не виявить ЦВДЗ знову. У такий спосіб з’ясовується, збільшив або зменшив значення даного піксела ЦВДЗ.

3. Крок 2 повторюється для кожного піксела в зображенні.

4. Знаючи, наскільки чутливий детектор до модифікації кожного піксела, атакуючий визначає піксели, модифікація яких не приведе до істотного погіршення зображення, але порушить роботу детектора.

5. Дані піксели віднімаються з вихідного зображення.

Чи можлива побудова стеганоалгоритму, стійкого до подібної атаки, поки невідомо.

Відомо різновид вищенаведеної атаки для ймовірнісного детектора. Також, як і раніше, атака починається з побудови тестового зображення на границі ухвалення рішення детектором. Потім вибирається випадкова двійкова послідовність, і її елементи додаються до пікселей тестового зображення. Якщо детектор виносить рішення про наявність, то ця послідовність вважається ЦВДЗ. В іншому випадку – ЦВДЗ вважається протилежним цій послідовності. Далі виконується випадкова перестановка елементів у послідовності, і процес повторюється. Повторивши цю процедуру кілька разів і додавши всі проміжні результати, одержимо досить гарну оцінку ЦВДЗ. Можна показати, що точність оцінювання , де J – кількість спроб, N – кількість пікселів у вихідному зображенні. Звідси виходить, що при фіксованій точності оцінювання кількість спроб лінійно залежить від кількості пікселів у зображенні. Також може бути показано, що кількість спроб пропорційна квадрату ширини зони ухвалення рішення. Таким чином, розроблювач ймовірнісного детектора повинен компромісно вибрати між такими параметрами: великою величиною зони ухвалення рішення, тобто безпекою, малим значенням верхнього порога зони, тобто малою ймовірністю помилкового виявлення стега, і більшим значенням нижнього порога зони, тобто малою ймовірністю помилкового невиявлення стега. У цілому з роботи [2] та інших слідує, що система ЦВДЗ на основі розширення спектра не повинна мати загальнодоступного детектора.

1.3.6 Атаки проти протоколу, що використовується

У роботах [8; 10; 26] показано, що багато стеганосистем ЦВДЗ чутливі до так званої інверсної атаки. Ця атака полягає в наступному. Зловмисник заявляє, що в захищеному зображенні частина даних є його водяним знаком. Після цього він створює помилковий оригінал, віднімаючи цю частину даних. У помилковому оригіналі присутній дійсний ЦВДЗ. З іншого боку, у захищеному зображенні присутній проголошений зловмисником помилковий ЦВДЗ. Настає нерозв’язна ситуація. Звичайно, якщо в детектора є вихідне зображення, то власник може бути виявлений. Але, як показано у роботі [8], далеко не завжди. У роботах [8; 10; 26] наведені методи захисту від подібної атаки. У них показано, що стійкий до подібної атаки ЦВДЗ повинен бути незворотним. Для цього він робиться залежним від зображення за допомогою односпрямованої функції.

У роботі [23] та інших досліджуються атаки на системи захисту від копіювання. У ряді випадків набагато простіше не видаляти ЦВДЗ, а перешкодити його використанню за призначенням. Наприклад, можливе впровадження додаткових ЦВДЗ так, що стає не зрозуміло, який з них ідентифікує справжнього власника контента.

Іншою відомою атакою на протокол використання ЦВДЗ є атака копіювання. Ця атака полягає в оцінюванні ЦВДЗ у захищеному зображенні і впровадженні оціненого ЦВДЗ в інші зображення. Метою може бути, наприклад, протидія системі імітозахисту або автентифікації.

Одним з недоліків стеганосистеми, застосовуваної для захисту від копіювання, є те, що детектор здатний виявити ЦВДЗ тільки коли відео-сигнал візуально прийнятний. Однак можна піддати сигнал скреблюванню, одержати шумоподібний сигнал, потім без перешкод незаконно скопіювати його. У відеоплеєр у цьому випадку вбудовується дескремблер, що і відновлює незаконно зроблену копію. Апаратна реалізація скремблера і дескремблера досить проста і іноді використовується для захисту, наприклад, програм кабельного телебачення. Можливим захистом проти такого підходу є дозвіл копіювання тільки визначеного формату даних.

1.3.7 Методи протидії атакам на системи ЦВДЗ. Статистичний стеганоаналіз та протидії

У найпростіших стеганосистемах ЦВДЗ при вбудовуванні використовується псевдовипадкова послідовність, що є реалізацією білого гаусівського шуму і невраховуючої властивості контейнера. Такі системи практично нестійкі до більшості розглянутих вище атак. Для підвищення робастності стеганосистем можна запропонувати ряд поліпшень.

У робастній стеганосистемі необхідний правильний вибір параметрів псевдовипадкової послідовності. Відомо, що при цьому системи з розширенням спектра можуть бути досить робастними стосовно атак типу додавання шуму, стиску й т. п. Вважається, що ЦВДЗ повинен виявлятися при досить сильній низькочастотній фільтрації (7×7 фільтр із прямокутною характеристикою). Отже, база сигналу повинна бути велика, що знижує пропускну здатність стеганоканалу. Крім того, вико-ристовувана як ключ ПВП повинна бути криптографічно безпечною.

Причина нестійкості систем ЦВДЗ з розширенням спектра до подібних атак пояснюється тим, що послідовність, яка звичайно використовується для вкладання, має нульове середнє.

Після усереднення великої кількості реалізацій ЦВДЗ видаляється. Є відомим спеціальний метод побудови водяного знака, націлений проти подібної атаки. При цьому коди розробляються таким чином, щоб при будь-якому усередненні завжди залишалася не дорівнююча нулю частина послідовності (статична компонента). Більш того, по ній можливе відновлення решти послідовності (динамічна компонента). Недоліком запропонованих кодів є те, що їх довжина збільшується експонентно зі зростанням кількості розповсюджуваних захищених копій. Можливим виходом із цього становища є застосування ієрархічного кодування, тобто призначення кодів для групи користувачів. Деякі аналогії тут є з системами стільникового зв’язку з кодовим поділом користувачів (CDMA).

Різні методи протидії пропонувалися для вирішення проблеми прав власності. Перший спосіб полягає в побудові незворотного алгоритму ЦВДЗ. ЦВДЗ повинен бути адаптивним до сигналу і вбудовуватися за допомогою односпрямованої функції, наприклад, геш-функції. Геш- функція перетворює 1 000 бітів вихідного зображення V в бітову послідовність , де [35]. Далі, залежно від значення використовується дві функції убудовування ЦВДЗ. Якщо , то використовується функція , якщо , то функція , де -й коефіцієнт зображення; – -й бітів вбудованого повідомлення. Передбачається, що такий алгоритм формування ЦВДЗ запобіжить фальсифікації. У роботі [26] на прикладі показано, що для того, щоб цей алгоритм був незворотним, всі елементи повинні бути позитивними. i i w

Другий спосіб вирішення проблеми прав власності полягає у вбудовуванні в ЦВДЗ деякої часової позначки, що надається третьою, довіреною стороною. У разі виникнення конфлікту особа, яка має на зображенні більш ранню часову позначку, вважається справжнім власником.

Один із принципів побудови робастної ЦВДЗ полягає в адаптації його спектра. У ряді робіт показано, що огинаюча спектра ідеального ЦВДЗ повинна повторювати огинаючу спектра контейнера. Спектральна щільність потужності ЦВДЗ, звичайно ж, набагато менше. При такій огинаючій спектра вінеровський фільтр дає найгіршу оцінку ЦВДЗ з можли- вих: дисперсія значень помилки досягає дисперсії значень заповненого контейнера. На практиці адаптація спектра ЦВДЗ можлива шляхом локального оцінювання спектра контейнера. З іншого боку, методи вбудовування ЦВДЗ в множини перетворення досягають цієї мети за рахунок адаптації в множини трансформанти.

Для захисту від атак типу афінного перетворення можна використовувати додатковий (опорний) ЦВДЗ. Цей ЦВДЗ не несе в собі інформації, але використовується для "реєстрації" виконуваних зловмисником перетворень. У детекторі ЦВДЗ є схема попереднього деформування, що виконує зворотне перетворення. Тут є аналогія з використовуваними у зв’язку тестовими послідовностями. Однак у цьому випадку атака може бути спрямована саме проти опорного ЦВДЗ. Іншою альтернативою є вкладення ЦВДЗ у візуально значущі множини зображення, які не можуть бути вилучені з нього без суттєвої його деградації. Нарешті, можна розмістити стеги в інваріантних до перетворення коефіцієнтах. Наприклад, амплітуда перетворення Фур’є інваріантна до зсуву зображення (при цьому змінюється тільки фаза).

Іншим методом захисту від подібних атак є блочний детектор. Модифіковане зображення розбивається на блоки розміром 12×12 або 16×16 пікселів, і для кожного блоку аналізуються всі можливі спотворення. Тобто піксели в блоці піддаються повороту, перестановці і т. д. Для кожної зміни визначається коефіцієнт кореляції ЦВДЗ. Перетворення, після якого коефіцієнт кореляції виявився найбільшим, вважається реально виконаним зловмисником. Таким чином з’являється можливість як би звернути внесені зловмисником спотворення. Можливість такого підходу ґрунтується на припущенні про те, що зловмис-ник не буде значно спотворювати контейнер (це не в його інтересах).

Основним завданням стеганоаналізу є визначення факту наявності прихованого повідомлення у ймовірному контейнері (мовлення, відео, зображення). Вирішити це завдання можливо шляхом вивчення статистичних властивостей сигналу. Наприклад, розподіл молодших бітів сигналів має, як правило, шумовий характер (помилки квантування). Вони несуть найменшу кількість інформації про сигнал і можуть використовуватися для впровадження прихованого повідомлення. При цьому, можливо, зміниться їх статистика, що й послужить для атак ознакою наявності прихованого каналу.

Для непомітного вбудовування даних стеганокодер повинен вирішити три завдання: виділити підмножину бітів, модифікація яких мало впливає на якість, вибрати із цієї підмножини потрібну кількість бітів відповідно до розміру прихованого повідомлення і виконати їх редагування. Якщо статистичні властивості контейнера не змінилися, то впровадження інформації можна вважати успішним. Оскільки розподіл незначущих бітів найчастіше близький до білого шуму, вбудовані дані повинні мати той самий характер. Це досягається за рахунок попереднього шифрування повідомлення або його стиснення.

Стеганоаналітік на основі вивчення сигналу завжди може виділити підмножину незначущих бітів, роблячи ті ж припущення, що і стеганограф. Далі він повинен перевірити відповідність їх статистики передбачуваній. При цьому, якщо аналітик має у своєму розпорядженні кращу модель даних, ніж стеганограф, вкладення буде виявлено. Тому по-справжньому гарні моделі сигналів різного характеру, ймовірно, тримаються в секреті, і ви не зустрінете їх у відкритих публікаціях. Можна лише дати рекомендації загального характеру. При побудові моделі треба враховувати:

– неоднорідність послідовностей відліків;

– залежність між бітами у відліку (кореляцію);

– залежність між відліками;

– нерівномірність умовних розподілів у послідовності відліків;

– статистику довжин серій (послідовностей з однакових бітів).

Відповідність статистики, що реально спостерігається очікуваній зазвичай перевіряється за допомогою критерію Хі-квадрат. Перевірка може здійснюватися на рівні монобітів, дібітів і т. д. Можливі й більш складні тести, аналогічні застосовуються при тестуванні криптографічних безпечних програмних датчиків випадкових чисел. Як показано в одній з робіт на прикладі звукових файлів, критерій Хі-квадрат дозволяє виявити модифікацію всього лише 10 % незначущих бітів. Там же показана ефективність для стеганоаналізу і ще більш простого критерію

,

де – кількість переходів зі значення біта i в значення j. Застосування тесту довжин серій базується на такому факті: у випадковій послідовності серій великої довжини (>15) зустрічаються значно рідше, ніж у незначущих бітах реальних сигналів. Тому вбудовування випадкового сигналу може бути помічено після застосування цього тесту.

Таким чином, протидія статистичного стеганоаналізу повинна полягати в побудові математичних моделей сигналів-контейнерів, пошуку на їх основі "дозволених" для модифікації галузей та впровадження у них прихованої інформації, чия статистика невідрізняється від статистики контейнера.

# ИСПОЛЬЗОВАНИЕ ДНК В КРИПТОГРАФИИ

Размеры «цифровой вселенной» должны были превысить 16 зеттабайт к 2017 году. Значительная доля этих данных хранится в виде архивов. К примеру, компания Facebook недавно построила отдельный дата-центр для «холодного» хранения 1 эксабайта данных. Такое же количество информации способно уместиться в 1 мм3 ДНК. Сохранение данных в ДНК проходит в три этапа: преобразование цифровых данных в последовательность нуклеотидов ДНК, синтез молекул ДНК и, непосредственно, хранение данных. Чтобы данные считать, необходимо выделить требуемую последовательность из молекулы ДНК и преобразовать её в первоначальный вид. Время на проведение синтеза и секвенирования уменьшается экспоненциально как показано на рисунке 2.1 [8].

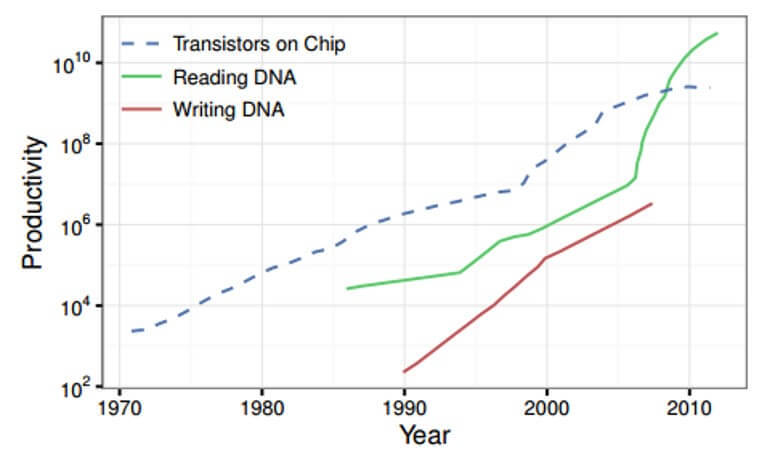


Рисунок 2.1 – Рост продуктивности использования ДНК

## 2.1 Хранение данных с использование ДНК

Молекула ДНК хранит информацию в четверичной системе счисления, по количеству нуклеотидов. Это компактный контейнер с плотностью записи в тысячи раз больше, чем у существующих носителей. Однако, чтобы технология перешла от научных испытаний к коммерческому использованию, требуется решить ряд проблем. Одна из них — специфика цифровой информации, в которой одни и те же биты могут многократно повторяться. Если многократно повторять один и тот же нуклеотид в молекуле ДНК, то это негативно влияет на стабильность кластера и информация может быть потеряна, даже при использовании избыточного дублирования и коррекции ошибок.  
 Исследователи из Европейского института биоинформатики  опубликовали работу с описанием способа, как можно существенно повысить стабильность ДНК. Попросту, они предлагают отказаться от четверичной системы (Base-4) в пользу троичной (Base-3), а четвёртый нуклеотид использовать в служебных целях для разбиения длинных цепочек согласно рисунка 2.2 [9].

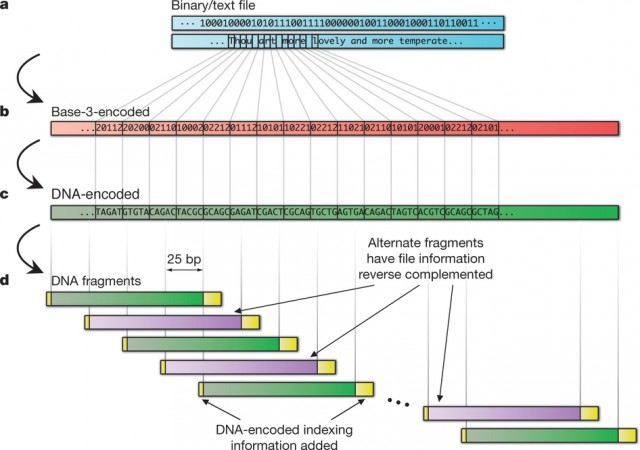
. 

Рисунок 2.2 – Процесс записи данных в ДНК

Во время эксперимента исследователи записали в ДНК почти мегабайт информации, в том числе все 154 сонета Шекспира в формате .txt, видеоролик с записью выступления Мартина Лютера Кинга продолжительностью 26 секунд, обложку журнала Bioinformatics Institute в формате .jpeg, научную работу с описанием структуры ДНК в формате .pdf, а также ещё один файл с описанием процесса кодирования. В общей сложности всё уместилось в 739 килобайт.  
При переходе с Base-4 на Base-3 мы теряем 25% информационной ёмкости, но даже в таком варианте учёные сообщают об информационной плотности записи 2,2 петабайта на 1 грамм биологического материала. Эксперимент показал надёжность считывания информации 100%. Теоретически, эта схема способна масштабироваться в пределах, превышающих объёмы всей существующей цифровой информации, пишут авторы исследования.

Исходя из нынешнего технологического прогресса в области синтеза и секвенирования, носители ДНК для записи информации должны появиться в открытой продаже в течение десяти лет. Хотя ДНК позволяет хранить информацию тысячелетиями, первые коммерческие носители будут продаваться с гарантией до 50-ти лет, считают исследователи.

## 2.2 Процесс кодирования информации

ДНК содержит четыре типа нуклеотидов: аденин (A), цитозин (С), гуанин (G) и тимин (T). Нить ДНК представляет собой линейную последовательность этих нуклеотидов. Таким образом, у нас есть четыре кодовых   
символа (A, C, G и T), поэтому очевидным подходом к хранению двоичных данных будет их кодирование в четверичной системе счисления, например, 0=A, 1=C, 2=G, и 3=T, на основе этих данных, в приложении А, представлен реализованный алгоритм шифрования основанный на RSA с использованием нуклеотидов. Однако стоит учитывать, что синтез и секвенирование подвержены ошибкам. Вероятность ошибок можно снизить, если закодировать двоичную информацию не в четверичной, а в троичной   
системе счисления, как показано на рисунке ниже. Чтобы избежать неэффективного преобразования исходных двоичных данных в троичную систему счисления, используется код Хаффмана. Пример такого преобразования показан на рисунке 2.3.

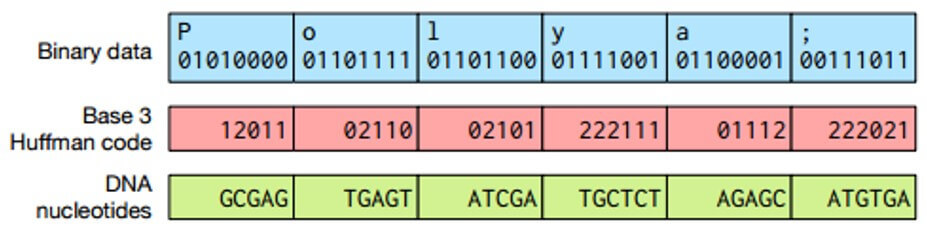


Рисунок 2.3 – Процесс преобразование слова в нуклеотиды ДНК

Каждая из трех цифр соотносится с нуклеотидом ДНК в соответствии с рисунком 2.4, причем нуклеотиды в цепочке не повторяются, что приводит к снижению ошибки секвенирования.

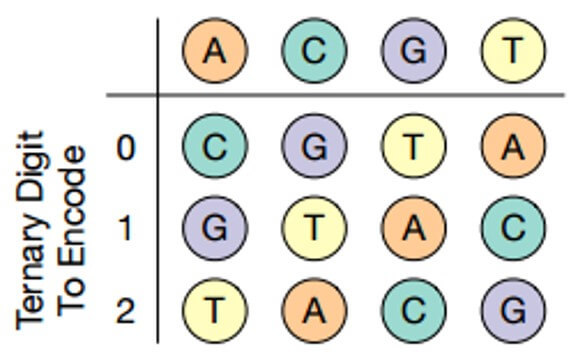


Рисунок 2.4 – Кодирования нуклеотидов

Чтобы обеспечить возможность произвольного доступа к данным, ученые организовали перевод ключей в уникальные последовательности праймеров. Праймеры – это короткие синтетические нити, определяющие начало и конец области, которую необходимо амплифицировать. Праймеры обеспечивают произвольный доступ с помощью полимеразной цепной реакции, которая генерирует множество копий ДНК. Цепи конкретного объекта имеют общий праймер, а разные цепи с одним и тем же праймером различаются по адресам.  «Контролируя последовательности, которые используются как праймеры для полимеразной цепной реакции (ПЦР), мы можем указать, какие нити в решении будут проходить амплификацию. Для того чтобы считать значение ключа в решении, мы просто проводим ПЦР, используя соответствующий этому ключу праймер», – говорят ученые.

## 2.3 ДНК-криптография

ДНК криптография – это новое поле, основанное на исследованиях в ДНК вычислений и новых технологиях, таких как PCR (Polymerase Chain Reaction),. ДНК-вычисления обладают высоким уровнем вычислительной способности и способны хранить огромное количество данные. Грамм ДНК содержит 1021 основание ДНК, что эквивалентно 108 терабайтам данных. В криптографии ДНК мы используем существующую биологическую информацию из общедоступных баз данных ДНК для кодирования открытого текста. Криптографический процесс может использовать разные методы. В методах одноразовых блокнотов описаны наиболее эффективные алгоритмы безопасности. В случае одноразового блокнота, открытый текст комбинируется с секретным случайным ключом или нашим блокнотом, который используется только один раз. Блокнот сочетается с открытым текстом, используя типичное модульное сложение или операцию XOR. Скорость алгоритма должна быть довольно высокой. Биологический фон: ДНК является аббревиатурой для дезоксирибонуклеиновой кислоты, которая является зародышевой плазмой всех стилей жизни. ДНК является своего рода биологической макромолекулой и состоит из нуклеотидов. Как уже выше упоминалось, каждый нуклеотид содержит одно основание и существует четыре типа оснований: аденин (А) и тимин (Т) или цитозин (С) и гуанин (G), соответствующий четырем типам нуклеотидов. Одноцепочная ДНК построена с ориентацией: один конец называется 5 ', а другой конец называется 3'. Обычно ДНК существует как двухцепочные молекулы в природе. Две взаимодополняющие нити ДНК удерживаются вместе, образуя структуру двойной спирали. Структура двойной спирали была обнаружена Уотсоном и Криком; Таким образом, комплементарная структура называется комплементарностью Уотсона Крика. Их открытие является одним из величайших научных открытий 20-го века. Развитие ДНК-криптографии, выигрывает от развития ДНК-вычислений (также называемых молекулярными вычислениями или биологическими вычислениями). С одной стороны, криптография всегда имеет некоторые отношения с соответствующей вычислительной моделью более или менее. С другой стороны, некоторые биологические технологии используются в ДНК-криптографии.

### 2.3.1 Криптосистема ДНК с использованием замены

В одноразовой системе замещения используется группа двоичного сообщения открытого текста и группа таблиц, определяющая случайное отображение на зашифрованный текст. Входная цепочка имеет длину и разбивается на незашифрованные слова фиксированной длины. Таблица отображает все возможные строки незашифрованного текста с фиксированной длиной в соответствующие строки зашифрованного текста, так что существует уникальное обратное отображение.

Шифрование происходит путем замены каждого слова открытого текста ДНК соответствующим шифрованным словом ДНК. Отображение реализуется с использованием длинного ДНК-блокнота, состоящего из множества сегментов, каждый из которых указывает на одно слово с открытого текста для шифрования словосочетаний. Слово с открытым текстом действует связывания праймера, который затем удлиняется. Это приводит к формированию текстовой пары открытого текста и зашифрованного текста.

Идеальная одноразовая библиотека будет содержать огромное количество блокнотов, и каждый из них обеспечит совершенно уникальное, случайное отображение из незащищенных слов в зашифрованные слова.

Повторяющийся блок состоит из: одного слова последовательности , из набора слов, соответствующих шифру или кодовой книге и префикса . Приметим, что включает в себя уникальную подпоследовательность, которая предотвращает атаки частотного анализа путем сопоставления нескольких экземпляров одного и того же открытого текста сообщения с различными зашифрованными словами. Кроме того, этот префикс может быть необязательно использован для кодирования положение слова в сообщении.

Каждая пара последовательностей однозначно связывает текстовое слово с шифровым словом.

Последовательность стопоров запрещает расширение растущей цепи ДНК за границу парного шифрованного слова. Используя эту тему, создается библиотека уникальных цепочек кодовых книг. Каждая отдельная цепочка из этой библиотеки кодовой книги задает конкретный уникальный набор парных слов[10].

Одноразовый блокнот состоит из цепочки ДНК длиной , содержащей копииповторяющегося шаблона: шифрованное слово длиной , слово открытого текста длиной и стопорной последовательности длины . Заметим, что длина слова растет логарифмически по всей длине блокнота. Определенно ; и = , где фиксированные целочисленные константы и . Каждый повторитель задает единую пару сопоставления, и ни одно слово из кодовой книги или текстовое слово не будет использоваться более одного раза в любом блокноте. Поэтому, учитывая шифрованное слово , мы уверены, что оно отображает только одно слово с открытым текстом и наоборот. Последовательность стоппера действует как «пунктуация» между повторяющимися звеньями, так что ДНК-полимераза не сможет продолжать копирование нити матрицы (блокнота). Стоппер – последовательности состоят из последовательности идентичных нуклеотидов, которые действуют для прекращения копирования цепи ДНК-полимеразой, учитывая отсутствие комплементарного нуклеотидтрифосфата в пробирке. Например, последовательность TTTT будет действовать в качестве точки остановки, если полимеризационной смеси не хватает своего комплементарного основания.

Экспериментальная осуществимость зависит от следующих факторов: размер лексикона, который представляет собой число пар слов открытого текста-зашифрованного текста, размер каждого слова, количество одноразовых ДНК, блокноты, которые могут быть созданы в цикле синтеза, и длина каждого сообщения, которое должно быть зашифровано. Если бы используемый лексикон состоял из слов английского языка, его размер находился бы в диапазоне от 10 000 до 25 000 словных пар. Если по экспериментальным причинам требуется меньший лексикон, тогда используемые слова могут представлять собой более малый набор, такой как ASCII-символы, что приводит к размеру словаря 128.

## 2.4 Преимущество и недостатки в использовании ДНК

В будущем такие системы потенциально позволят сохранить огромное количество данных на микроскопических носителях. Представьте себе «флешку» объемом 100 мм3, способную хранить порядка 100 000 ПБайт данных. Однако пока что самым крупным препятствием к внедрению подобных технологий остается время. Расшифровка и чтение молекулы ДНК занимает многие часы. Поэтому такой тип хранилищ вряд ли подойдет для содержания часто используемых данных, однако способен перевернуть наше представление о долговременных хранилищах в дата-центрах. Также на сегодняшний день стоимость кодирования информации в ДНК оценивается примерно в [$12400 за мегабайт](http://mashable.com/2013/01/23/dna-replace-hard-drive/), стоимость считывания — $220 за 1 МБ, что является явным недостатком. Еще одним минусом является то, что необходимы специальные емкости для хранения ДНК, во избежание ее распада и потери данных.

# СТЕГАНОГРАФІЯ З ВИКОРИСТАННЯМ ДНК

# ВЫВОДЫ

В данной работе были проанализированы криптосистемы, основанные на неабелевых группах, были рассмотрены алгоритмы обмена ключами реализованные на модулярной арифметике, так же эти алгоритмы были представлены на абелевых группах, что дает большую стойкость, за счет сложности нахождения сопряжений между группами и подгруппами.

Анализ ДНК-криптографии показал, что использование ее на данном этапе развития не целесообразно за счет потребление больших вычислительных средств и дороговизны всей процедуры, также большим минусом является то, что процесс записи и извлечения занимает большое время, примерно в 5 раз больше, чем с использованием алгоритмах в групповой математике. Положительной стороной есть то, что технологии развиваются чрезвычайно быстро и через несколько лет данный вид защиты информации может быть реализован без больших финансовых и вычислительных трудностей.

Криптосистемы, основанные на хаосе, являются чрезвычайно чувствительными к выбору параметров, и для их создания был сформирован ряд правил, которые не являются необходимыми, но есть желательными. Для построения успешной такой криптосистемы были определены два свойства: путаницу и различие. Путаница используется для усложнения понимания алгоритма связи ключа с шифротекстом, различие – должно минимизировать количество шаблонов в самой криптосистеме.

# ПЕРЕЧЕНЬ ССЫЛОК

1. A.G. Myasnikov, V.Shpilrain and A. Ushakov, Group-Based Cryptography Advanced Courses in Mathematics, CRM Barcelona, 415, 2007.
2. P.Dehornoy, Braid-Based Cryptography Cont. Math., 360, 2004, 5–34.
3. W. Magnus, A. Karass and D. Solitar Combinatorial Group Theory, Wiley Interscience,New York, 527, 1968.
4. G. Baumslag, B.Fine, and X.Xu, Cryptosystems Using Linear Groups Appl. Alg. in Engineering, Communication and Computing 17, 290, 2006, 205-217.
5. K.Ko, J.Lee, J.H. Cheon, J.W. Han, J.Kang, C.Park, New Public-Key Cryptosystem Using Braid Groups , Advances in Cryptology - CRYPTO 2000 Santa Barbara CA , Lecture Notes in Computer Science, Springer 1880, 2000, 166-183.
6. D.Kahrobaei and B.Khan, A Non-Commutative Generalization of the ElGamal Key Exchange using Polycyclic Groups Proceeding of IEEE, GLOBECOM, 2006.
7. V.Shpilrain and A. Ushakov, The Conjugacy Search Problem in Public Key Cryptography; Unnecessary and Insufficient Applicable Algebra in Engineering, Communication and computing, 17, 2006 285-289.
8. «Заложено природой»: Система хранения данных на основе ДНК [Электронный ресурс] // URL: <https://m.habrahabr.ru/company/1cloud/blog/306656/> (дата обращения: 11.05.2017).
9. Надёжное хранение информации в ДНК (2,2 петабайта на грамм) [Электронный ресурс] // URL: <https://geektimes.ru/post/166889/> (дата обращения: 21.05.2017).
10. DNA Data cryptography [Электронный ресурс] // URL: <https://www.slideshare.net/mayukhmaitra/dna-cryptography> (дата обращения: 25.05.2017).
11. Alvarez, G. & Li, S. “Breaking cryptography with chaos at the physical level,” arXiv:nlin.CD/0403029, 215, 2004.
12. Cerm´ak, J. “Digital generators of chaos,” Phys. Lett. 525, 1996, 151–160.
13. Stinson, D. R. [1995] Cryptography: Theory and Practice (CRC Press).
14. Schneier, B. [1996] Applied Cryptography – Protocols, algorithms, and souce code in C second edn. (John Wiley & Sons, Inc., New York, USA).
15. Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. Handbook of Applied Cryptography (CRC Press), 1997.
16. Fog, A. [2000] “How to optimize for the Pentium family of microprocessors,” Online document, <http://www.codingnow.com/2000/download/pentopt.htm>.
17. Fridrich, J. “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurc. Chaos 8, 1465, 1998, 1259–1284.

ДОДАТОК А

ДОДАТОК Б