Міністерство освіти і науки України
Вінницький національний технічний університет

В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець

КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ

Навчальний посібник

Вінниця
ВНТУ
2017

УДК 004.056.5
К

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 15 від 25.05.2017 р.)

Рецензенти:
А. Я. Кулик, доктор технічних наук, професор
С. І. Перевозніков, доктор технічних наук, професор
В. П. Майданюк, кандидат технічних наук, доцент

Хорошко, В.О.

К Комп'ютерна стеганографія: навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець. – Вінниця: ВНТУ, 2017. – 155 с.

ISBN

В посібнику розглядаються питання, що відносяться до одного з перспективних напрямків інформаційної безпеки – стеганографії. Розглядаються основні проблеми і методи стеганографії. Зокрема проведено аналіз існуючих уявлень про стеганографію та стеганографічний аналіз, наведено класифікацію стеганографічних систем та можливих атак на них.

Описані відомі методи приховування інформації у цифрових зображеннях, зокрема векторного формату, у відео файлах, а також у текстовому та звуковому середовищі. Наведено відомості про прикладні напрямки комп'ютерної стеганографії, а саме: приховані канали у комп'ютерних мережах, технології цифрових водяних знаків і цифрових відбитків.

Рекомендується для студентів, що навчаються за спеціальністю 125 «Кібербезпека», а також для фахівців, що працюють в галузі захисту інформації.

УДК 004.056.5

ЗМІСТ

ВСТУП

Стрімкий розвиток цифрових технологій та засобів телекомунікацій стимулює створення різноманітних методів захисту інформації. Відомо, що для гарантованого захисту вмісту повідомлення існує два різних по суті підходи.

Перший – це блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення. Для цієї мети використовуються криптографічні методи захисту. У криптограмах, як правило, відсутні структура і закономірності, які властиві відкритим текстам. Тому, при проведенні моніторингу мереж телекомунікацій, вони легко автоматично виділяються з інформаційного потоку.

Другий підхід полягає в тому, що повідомлення, яке передається, намагаються приховати так, що б його неможливо було знайти. Для приховування факту існування інформації застосовуються стеганографічні методи захисту, які значно знижують ймовірність її виявлення. На відміну від криптографічного захисту, коли в «зловмисника» існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати передавану інформацію в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту. Шанси знайти приховане повідомлення – невеликі, але на той випадок, якщо повідомлення все-таки буде виявлено, його можна ще додатково зашифрувати. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Стеганографія – це мистецтво і наука організації зв’язку, при якій приховується, власне, наявність самого зв’язку.

В найближчі роки інтерес до стеганографії буде підсилюватися. Основна передумова для цього сформована вже сьогодні. Це стрімкий розвиток комп’ютерної мережі загального користування Інтернет з такими невирішеними і суперечливими проблемами, як захист авторських прав, захист прав на особисту таємницю, організація електронної торгівлі, протиправна діяльність хакерів і терористів.

В посібнику проведений огляд сучасного стану порівняно нового наукового напрямку в галузі захисту інформації – комп’ютерної стеганографії. Систематизовані деякі теоретичні положення і досліджені

практичні методи стеганографічного захисту, які з'явилися в науковій літературі до 2017 року.

У двох перших розділах роботи проведений аналіз існуючих уявлень про стеганографію та стеганографічний аналіз. Зокрема, дана класифікація стеганографічних систем та можливих атак на них.

У третьому розділі систематизовані відомі підходи до стеганографічного приховування в різних типах інформаційного середовища. Описані відомі методи приховування інформації в текстовому середовищі, у звуковому середовищі, у зображеннях і відео.

В останніх трьох розділах роботи наводяться відомості про нові прикладні напрямки комп'ютерної стеганографії, а саме, приховані канали у комп'ютерних мережах, технології цифрових водяних знаків і цифрових відбитків, які останнім часом мають усе більше практичне значення.

РОЗДІЛ 1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО СТЕГАНОГРАФІЮ

Надійний захист інформації від несанкціонованого доступу є актуальною, але не вирішеною в повному обсязі проблемою. Один з перспективних напрямків захисту інформації сформував сучасні методи стеганографії.

Інформаційні технології дали друге дихання найдавнішій науці про тайнопис – *стеганографії*. Слово «стеганографія» у перекладі з грецької буквально означає *тайнопис* (steganos – таємниця, секрет; graphy - запис).

Стеганографія являє собою сукупність методів та засобів їхньої реалізації, які базуються на різних принципах і дозволяють приховувати сам факт існування секретної інформації в тому або іншому середовищі. До неї можна віднести безліч секретних засобів зв'язку, таких як невидимі чорнила, мікрофотознімки, умовне розташування знаків, таємні (приховані) канали, засоби зв'язку з плаваючими частотами, голографія і т.д.

В даний час розвиваються методи комп'ютерної стеганографії – самостійного наукового напрямку інформаційної безпеки, що вивчає проблеми створення компонент приховуваної інформації у відкритому інформаційному середовищі, яке може бути сформовано обчислювальними системами та мережами. Особливістю стеганографічного підходу є те, що він не передбачає прямого оголошення факту існування захищуваної інформації. Ця обставина дозволяє в рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати деякі важливі задачі захисту інформації ряду прикладних галузей.

1.1 З історії стеганографії

Історія стеганографії нараховує тисячоріччя [1-3]. Приховування факту існування таємного повідомлення завжди представлялося доцільним для його захисту, а існування різних технічних, хімічних, фізичних та психологічних методів такого приховування забезпечувало можливість його реалізації.

Місцем зародження стеганографії вважається Єгипет, хоча «стеганографічними повідомленнями» можна назвати і наскальні малюнки древніх людей.

Перше згадування в літературі про стеганографію відноситься до древньої Греції. У ті часи текст наносився на дерев’яні дощечки, покриті

воском. З розповідей Геродота відомо: для передавання повідомлення про те, що цар персів Ксеркссс планує захопити Грецію, використовувалася звичайна дощечка із секретним повідомленням під шаром воску. Варті дощечка з посланням була пред'явлена як заготівля для листа і не викликала підозри.

Інший вдало використовуваний метод полягав у тім, що для передавання таємного послання використовували голову раба: посильного голили наголо і повідомлення наносили у вигляді татуювання на його голову. Після того як волосся відростало, повідомлення не можна було виявити, а щоб його прочитати, досить було знову поголитися «під Котовського».

У Китаї листи писали на смужках шовку. Тому для приховування повідомлень смужки з текстом листа згорталися в кульки, покривалися воском і потім ковтались посильними.

Темне середньовіччя породило не тільки інквізицію. Посилення стеження привело до розвитку як криптографічних, так і стеганографічних методів. Саме в середні віки вперше було застосовано спільне використання шифрів і стеганографічних методів.

У XV столітті абат Тритемія (*J.Trithemio*, 1462-1516), що займався криптографією і стеганографією, описав багато різних методів прихованого передавання повідомлень, які у 1499 році були об'єднані в книгу «Steganographia» (рис. 1.1).

Гаспар Скотт (*G.Schott*, 1608-1666) запропонував метод приховування повідомлень у нотному записі [4], де кожній ноті відповідає певна буква (рис. 1.2). Природно, одержати благозвучну мелодію в такому випадку було утруднено.

З початку XVIII століття основним споживачем стеганографії стає розвідка (а пізніше - революціонери-підпільники). Шифр – це мова розвідників: вони зазвичай змушені вести свої таємні розмови пошепки. Успіх розвідника залежить від уміння залишатися непоміченим, а зашифровані повідомлення, що надсилаються їм у явній формі, негайно привертають увагу «сторонніх». Тому, замість звичайних способів секретного зв'язку, розвідкою використовуються найбільш витончені способи: коди, що мають вигляд звичайних відкритих текстів; невидимі

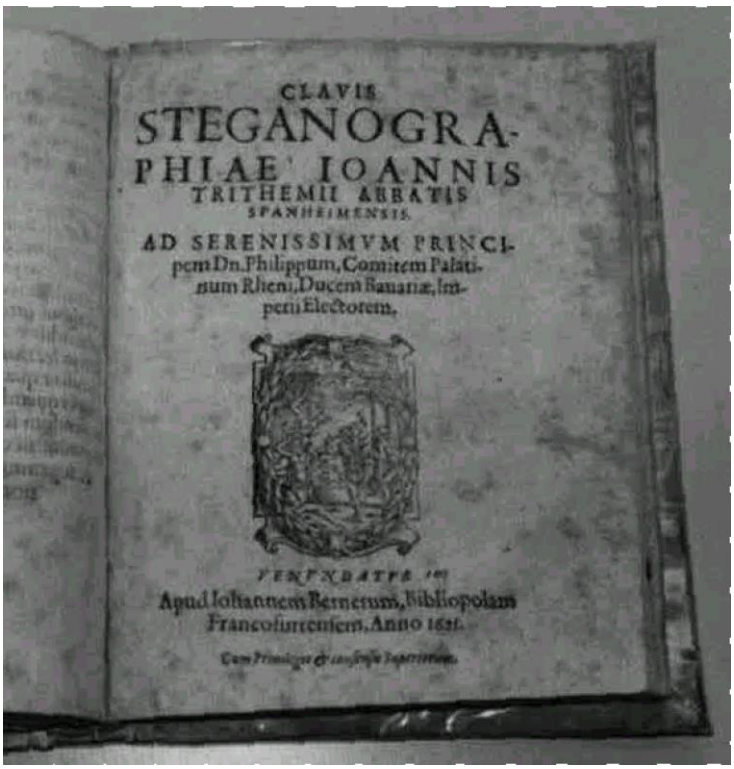


Рисунок 1.1 – Книга абата Тритемія «Steganographia»
(зберігається в музеї фірми Crypto AG, Швейцарія)

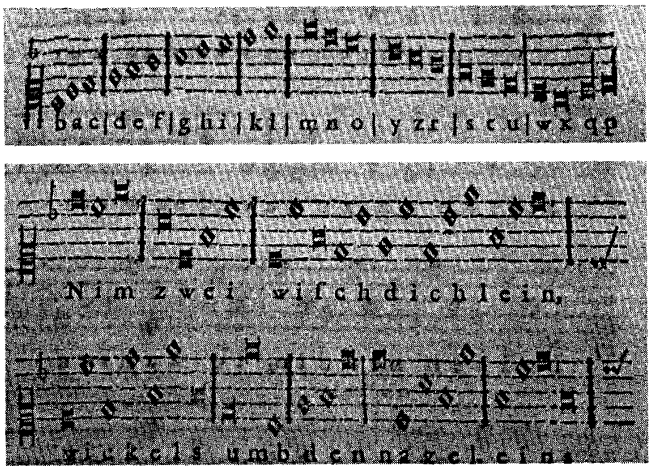


Рисунок 1.2 – Зразок стеганограми за методом Г. Скотта (1660 р.)

чорнила; послання мікроскопічно малих розмірів та ін. Таким чином, застосовуються методи приховування самого факту відправлення повідомлення.

Щоб позбавити іноземних розвідників можливості користуватися цими методами, при відділеннях поштового і телеграфного зв'язку створювалися потужні фільтрувальні державні організації, у завдання яких входило

виявлення та припинення таємного листування. Ці фільтри, що безперешкодно пропускають усі нешкідливі повідомлення, являють собою органи цензури. У демократичних країнах вона є породженням війни, а в диктаторських – тиранії.

Цензура веде свій родовід від «чорних кабінетів» XVIII століття. Основною задачею «чорних кабінетів» було перехоплення, перлюстрація і дешифрування листування. Крім криптографів, у штат «чорних кабінетів» входили й інші фахівці, у тому числі і хіміки.

Наявність фахівців-хіміків була викликана активним використанням так званих невидимих чорнил – дуже популярної форми маскування повідомлень. Це воістину древній винахід. Плиній Старший у своїй книзі «Природна історія» (I ст. до н.е.) розповідає, як можна використовувати сік рослин сімейства молочаїв як симпатичних чорнил. Для цієї ж мети використовувалося також молоко, оцет, фруктові соки та сеча, які сутеніють при нагріванні. Незважаючи на давню популярність і слабку стійкість, такий вид тайнопису настільки зручний, що застосовувався навіть під час II світової війни.

Наприклад, якщо для тайнопису використовується залізний купорос, то текст буде невидимий доти, поки його не оброблять розчином ціанату калію, після чого утвориться берлінська лазур – речовина, що має дуже красивий колір. Мистецтво виготовлення гарного чорнила для тайнопису полягає в тому, щоб знайти речовину, яка реагувала б з мінімальною кількістю хімікалій (найкраще лише з одним).

Прикладом використання симпатичного тайнопису може слугувати цікавий історичний епізод. Повсталими дворянами в Бордо був арештований францисканський чернець Берто, що був агентом кардинала Мазаріні. Повсталі дозволили Берто написати лист знайомому священикові в місто Блей. Однак наприкінці цього листа релігійного змісту чернець зробив приписку, на яку ніхто не звернув увагу: «Посилаю Вам очну мазь; натріть нею очі і Ви будете краще бачити». Так він зумів переслати не тільки приховане повідомлення, але й вказав спосіб його виявлення. У результаті чернець Берто був врятований.

Основні труднощі при застосуванні симпатичних чорнил пов’язані з неможливістю забезпечення швидкої обробки величезної кількості інформації, яку необхідно передавати. Один із способів стеганографування інформації великого об’єму полягав у тому, що спеціальним розчином відзначалися необхідні букви в якій-небудь газеті. У звичайних умовах ці

відмітки були невидимі, але при обробці ультрафіолетовими променями вони починали фосфоресціювати.

Для боротьби з тайнописом під час ІІ світової війни американські цензори «смугували» листи з метою виявити наявність у них невидимого чорнила [3]. Лаборант водив по листу декількома щітками, закріпленими в одному затискачі і змоченими в розчинах різних проявників. Ці проявники мали різні властивості і реагували навіть на виділення людини, так що після обробки на папері з'являлися відбитки пальців і краплі поту. Листи також проходили перевірку в інфрачервоних і ультрафіолетових променях. Наприклад, написаний крохмалем текст, невидимий при денному або електричному світлі, починав світитися під впливом ультрафіолету. Інфрачервоні промені допомагали розрізняти кольори, які не можна було розрізнити при звичайному освітленні, наприклад зелені написи на зеленій поштовій марці.

Інші широко розповсюджені методи класичної стеганографії використовували незначні розходження в написанні рукописних символів, маленькі проколи певних надрукованих символів і безліч інших способів приховування істинного змісту таємного повідомлення у відкритому листуванні.

Для прикладу, у XVII столітті сер Джон Тревеніон, що очікував неминучої страти від рук прихильників Кромвеля, одержав листа, який був ретельно вивчений його тюремниками, перш ніж його передали йому в руки. Прочитавши в цьому листі кожну третю букву після кожного розділового знака, він довідався, що «у східній стіні каплиці відкривається одна панель». Під час вечерні Тревеніон утік.

Інший приклад. У період ІІ світової війни полонені німецькі офіцери-підводники у своїх листах додому посилали таємні повідомлення, роблячи невеликі пропуски після кожної значимої букви. Один пильний англійський цензор помітив, що ці маленькі пропуски трапляються в найнеприродніших місцях, навіть у середині складів. Виявилося, що у своїх прихованих посланнях німці повідомляли про тактику, що застосовувалася англо-американськими союзниками в боротьбі з німецькими підводними човнами, а також про їхні технічні недоліки.

У міру того, як поліпшувалися методи виявлення повідомлень, розроблялися і нові технології, що могли передавати більше інформації і важче виявлялися. Наприклад, у воєнні часи цензура вживала надзвичайних заходів і забороняла постачання великих партій квітів,

публікацію кросвордів і приватних оголошень, вбачаючи в них засоби передавання секретних повідомлень. Цензори дійшли навіть до того, що переписували листи, перефразовували текст і переклеювали на конвертах марки, були навіть скасовані шахові матчі за допомогою листування. З листів вимазували навіть кросворди, тому що в цензорів бракувало часу розгадувати їх, щоб перевірити, чи не містять вони таємні послання. З поштових відправлень вилучалися газетні вирізки, тому що вони могли містити секретний текст. Не дозволялося пересилати поштою табелі успішності учнів. Один раз у нью-йоркському цензурному відділенні перевели всі стрілки в призначеній для відправлення партії годинників, побоюючись, що їхнє положення може містити в собі якесь повідомлення.

Особливе місце в історії стеганографії займають фотографічні мікрокрапки. Суть ідеї така: фотографія розвідувального повідомлення стискувалася до розміру крапки і наклеювалася в тексті якого-небудь невинного листа замість чорнильної крапки. У розвідувальному центрі фотографію-мікрокрапку збільшували і отримували донесення від свого агента. Завдяки цій технології стало можливим приховане передавання великих об’ємів даних, включаючи креслення та фотографії. Іноді в одному листі було до 20 мікрокрапок.

Активне використання мікрокрапок фахівцями німецької розвідки почалося незадовго до II світової війни й успішно застосовувалося практично до її закінчення. Лише в серпні 1941 р. один лаборант уперше раптово помітив слабке світіння на поверхні конверта, знайденого у людини, яку підозрювали в зв’язках з німецькою розвідкою. У результаті була виявлена перша мікрокрапка, замаскована під розділовий знак машинописного шрифту. Найперша з виявлених мікрокрапок містила розпорядження німецькому агентові з’ясувати, «де в США здійснюються уранові випробування». У такий же спосіб через океан переправлялися вкрадені технічні креслення та схеми.

Мікрокрапки дозволили німцям вирішити проблему передавання великої кількості інформації. Директор ФБР Едгар Гувер назвав мікрокрапки «*ворожим шедевром шпигунства»*.

Основним визначальним моментом у стеганографії є стеганографічне перетворення. Донедавна стеганографія, як наука, в основному вивчала окремі методи приховування інформації і способи їхньої технічної реалізації. Розмаїтість принципів, закладених у стеганографічних методах, власне кажучи гальмувала розвиток стеганографії як окремої наукової

дисципліни і не дозволила їй сформуватися у вигляді деякої науки зі своїми теоретичними положеннями і єдиною концептуальною системою, яка забезпечила б формальне одержання якісних та кількісних оцінок стеганометодів. У цьому історія розвитку стеганографії різко відрізняється від розвитку криптографії.

До кінця XIX століття стеганографія і криптографія розвивалися в рамках єдиної науки про тайнопис. Після формулювання голландським офіцером Кірхгофсом (*A.Kerckhoffs*) знаменитого правила про те, що стійкість криптографічного алгоритму повинна визначатися виключно стійкістю ключа, криптографія, як окрема наука, відокремилася від стеганографії. За останні десятиліття криптологія із сукупності спеціальних методів перетворилася в наукомістку дисципліну, що базується на фундаментальних дослідженнях з теорії ймовірності, математичної статистики, чисел, алгебраїчних полів, що дозволило їй вирішити ряд важливих для практичного застосування задач. Наприклад, визначення стійкості зашифрованих повідомлень стосовно можливих засобів криптоаналізу, а також цілий ряд інших задач, рішення яких дозволяє одержувати досить чіткі кількісні характеристики засобів криптографічного захисту інформації.

В основі багатьох підходів до вирішення задач стеганографії лежить загальна з криптографією методична база, закладена К. Шеноном (*C.E. Shannon*) у теорії тайнопису [5]. Однак дотепер теоретичні основи стеганографії залишаються практично неопрацьованими.

1.2 Стеганографія сьогодні

Інтерес, що спостерігається в наш час, до стеганографії як сукупності методів приховування інформації виник у великій мірі завдяки інтенсивному впровадженню та широкому поширенню засобів обчислювальної техніки в усі сфери діяльності людини. У рамках обчислювальних мереж виникли досить широкі можливості з оперативного обміну різною інформацією у вигляді текстів, програм, звуку, зображень між будь-якими учасниками мережних сеансів незалежно від їхнього територіального розміщення. Це дозволяє активно застосовувати всі переваги, що їх дають стеганографічні методи захисту.

Стеганографічні методи знаходять усе більше застосування в оборонній і комерційній сферах діяльності в силу їхньої легкої адаптації

при вирішенні задач захисту інформації, а також відсутності явно виражених ознак засобів захисту, використання яких може бути обмежене або заборонене (як, наприклад, криптографічних засобів захисту).

Сьогодні стеганографічні технології активно використовуються для вирішення таких основних задач:

– захисту конфіденційної інформації від несанкціонованого доступу;

– захисту авторських прав на деякі види інтелектуальної власності;

– подолання систем моніторингу і керування мережними ресурсами;

– камуфляжу програмного забезпечення;

– створення прихованих від законного користувача каналів витоку чутливої інформації .

Використання стеганографічних систем є найбільш ефективним при вирішенні проблеми *захисту конфіденційної інформації*. Так, наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 бітів у стереорежимі дозволяє приховати за рахунок заміни молодших розрядів на приховуване повідомлення близько 10 Кбайт інформації. При цьому зміна значень відліків складає менше 1%. Така зміна практично не виявляється при прослуховуванні файлу більшістю людей. Приховування впроваджуваних даних, які у більшості випадків мають великий об’єм, висуває серйозні вимоги до контейнера: розмір контейнера в декілька разів повинен перевищувати розмір даних, що вбудовуються.

Крім прихованого передавання повідомлень, стеганографія є одним із найперспективніших напрямків для автентифікації і маркування авторської продукції з метою захисту авторських прав на цифрові об’єкти від піратського копіювання. На комп’ютерні графічні зображення, аудіо продукцію, літературні твори (програми в тому числі) наноситься спеціальна мітка, що залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням. Мітка містить приховану інформацію, що підтверджує авторство. Прихована інформація покликана забезпечити захист інтелектуальної власності. Як впроваджувану інформацію можна використовувати дані про автора, дату і місце створення твору, номери документів, що підтверджують авторство, дату пріоритету і т.п. Такі спеціальні відомості можуть розглядатися як докази при розгляді спорів про авторське право або для доказу нелегального копіювання. Чи треба говорити, яке це має значення при тому широкому

злодійстві, що відбувається в Інтернеті. Основні вимоги, які висуваються до цифрових водяних знаків, є надійність і стійкість до перекручувань. Цифрові водяні знаки мають невеликий об'єм, однак, враховуючи зазначені вище вимоги, для їхнього вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень. Більш докладно питання, пов'язані з захистом авторських прав на цифрові об'єкти, будуть розглянуті в *розділах 5* і *6*, де мова йтиме про цифрові водяні знаки і цифрові відбитки пальця.

Як і будь-які інші інструменти, стеганографічні методи вимагають до себе дбайливого відношення, тому що вони можуть бути використані як з метою захисту, так і в протизаконних цілях.

Наприклад, наприкінці 2001 року під пильною увагою преси виявилися додаткові відомості про те, що один з найнебезпечніших терористів світу Усама бен Ладен і члени його угруповання широко використовують мережу Інтернет для передавання повідомлень з організації терористичних акцій. При цьому злочинці широко використовують новітні досягнення стеганографії для передавання повідомлень через чати та електронні дошки оголошень. Розпізнати подібну інформацію в загальному потоці повідомлень практично неможливо не тільки в силу їхнього незначного об'єму в загальній масі, але і через витонченість способів, використовуваних при приховуванні цих повідомлень. Уряди деяких країн уживають заходи з метою приборкання такої погрози, намагаючись ввести обмеження на поширення програм, пов'язаних із криптографічними та стеганографічними методами. Однак стеганографічні методи успішно застосовуються для *протидії системам моніторингу* і керування мережними ресурсами промислового шпигунства. З їхньою допомогою можна протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери керування локальних або глобальних обчислювальних мереж.

Нерідко методи стеганографії використовують для *камуфлювання програмного забезпечення*. У тих випадках, коли використання програм незареєстрованими користувачами є небажаним, воно може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховане у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

І, нарешті, стеганографічний підхід використовується при створенні прихованого каналу витоку чутливої інформації від санкціонованих

користувачів. Деякі приклади створення прихованих каналів будуть розглянуті в *розділі 4*.

1.3 Класифікація стеганографічних методів

В сучасній стеганографії, в цілому, можна виділити такі напрямки: технологічну стеганографію й інформаційну стеганографію (рис. 1.3).

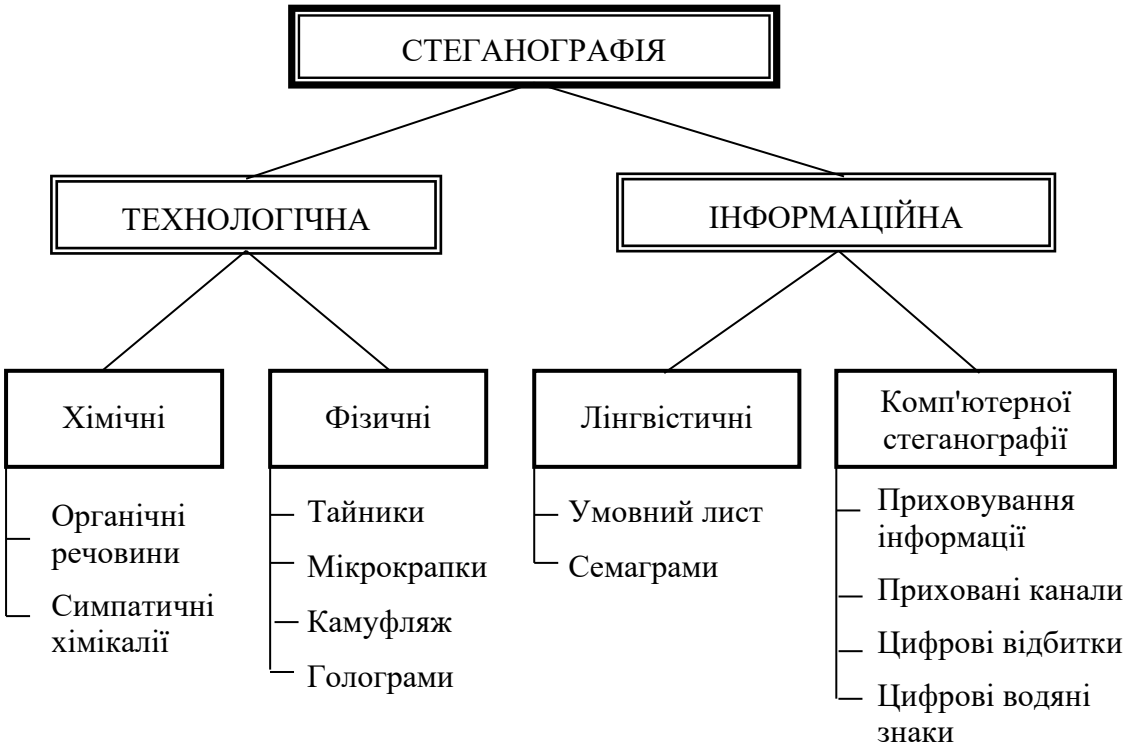


Рисунок1.3 – Класифікація методів стеганографічного захисту

До методів технологічної стеганографії відносяться методи, що базуються на використанні хімічних або фізичних властивостей різних матеріальних носіїв інформації.

Хімічні методи стеганографії зводяться майже винятково до застосування невидимих чорнил. Невидимі чорнила бувають двох видів: органічні рідини і симпатичні хімікалії. Перші, до яких відносяться сеча, молоко, оцет і фруктові соки, стають видимими в результаті незначного нагрівання. Симпатичні чорнила – це хімічні розчини, безбарвні після висихання, але такі, що утворюють видимі сполуки після обробки іншими хімікаліями (реагентами).

До фізичних методів можна віднести мікрокрапки, різного виду схованки і методи камуфляжу. В даний час фізичні методи становлять

інтерес в галузі дослідження різних носіїв інформації з метою запису на них даних, які б не виявлялися звичайними методами зчитування. Особливий інтерес виявляється до стандартних носіїв інформації засобів обчислювальної, аудіо- і відеотехніки. Крім цього, з'явився цілий ряд нових технологій, які базуються на традиційній стеганографії, використовують останні досягнення мікроелектроніки (голограми, кінеграми).

До інформаційної стеганографії можна віднести методи лінгвістичної і комп'ютерної стеганографії.

Лінгвістичні методи стеганографії діляться на дві основні категорії: умовний лист і семаграми.

Існують три види умовного листа: жаргонний код, пустковий шифр і геометрична система.

У жаргонному коді зовні невинне слово має зовсім інше реальне значення, а текст складається так, щоб виглядати якомога більш безневинно і правдоподібно. Спочатку він може містити лише згадування про обопільно відомі події й осіб: «Я відвідав людину, з якою Ви обідали на минулому тижні», а далі може йти відрізок тексту, зрозумілий тільки адресатові. Наприклад, один злочинець повідомляє про арешт іншого: «Ця людина потрапила в лікарню», де замість слова «в'язниця» використовується слово «лікарня».

Іншим видом умовного листа є пустковий шифр. При його застосуванні в тексті мають значення лише деякі визначені букви або слова. Наприклад, читається кожне п'яте слово або перша буква кожного слова, у той час як всі інші букви або слова служать у якості «пусткових» для приховання значимого тексту. Пусткові шифри звичайно виглядають ще більш штучно, ніж жаргонний код.

Третім видом умовного листа є геометрична форма. При її застосуванні слова, що мають значення, розташовуються на сторінці у визначених місцях або в точках пересікання геометричної фігури заданого розміру.

Другу категорію лінгвістичних методів складають семаграми - таємні повідомлення, у яких шифропозначення – це будь-які символи, крім букв і цифр. Ці повідомлення можуть бути передані, наприклад, у малюнку, що містить крапки і тире для читання за кодом Морзе.

Стеганографічні методи в своїй проекції на інструментарій та середовище, яке реалізується на основі комп'ютерної техніки і програмного забезпечення в рамках окремих обчислювальних або

керувальних систем, корпоративних або глобальних обчислювальних мереж, складають предмет вивчення порівняно нового наукового напрямку інформаційної безпеки - ***комп'ютерної стеганографії*** [6,7].

У рамках комп'ютерної стеганографії розглядаються питання, пов'язані з приховуванням інформації, що зберігається на носіях або передається мережами телекомунікацій, з організацією прихованих каналів у комп'ютерних системах і мережах, а також з технологіями цифрових водяних знаків і відбитка пальця.

Існують певні відмінності між технологіями цифрових водяних знаків і відбитка пальця, з одного боку, і власне стеганографічними технологіями приховування секретної інформації для її наступного передавання або збереження. Найголовніша відмінність – це те, що цифрові водяні знаки і відбитки мають на меті захист самого цифрового об'єкта (програми, зображення, музичного файлу й ін.), куди вони впроваджуються, і забезпечують доказ прав власності на даний об'єкт.

При використанні методів комп'ютерної стеганографії повинні враховуватися такі умови:

– противник може мати повне уявлення про стеганографічну систему і деталі її реалізації. Єдиною інформацією, яка повинна залишатися йому невідомою, – це ключ, за допомогою якого можна встановити факт присутності прихованого повідомлення і його зміст;

– якщо противникові якимсь чином вдалося довідатися про факт існування прихованого повідомлення, то це не повинно дозволити йому витягти подібні повідомлення з інших стеганограм доти, поки ключ зберігається в таємниці;

– потенційний противник повинен бути позбавлений яких-небудь технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

У подальших розділах будуть обговорені основні теоретичні положення комп'ютерної стеганографії і розглянуті деякі методи приховування даних в інформаційному середовищі, яке може бути підтримано обчислювальними системами і мережами.

1.4 Питання для самоконтролю знань

1. Дайте означення стеганографії.

2. Чим стеганографія відрізняється від криптографії?

3. Назвіть місця зародження а також першого згадування про стеганографію.

4. Назвіть найбільш відомі історичні факти приховування передавання секретних повідомлень.

5. Які актуальні задачі сучасності можуть вирішуватись завдяки стеганографічним технологіям?

6. Наведіть класифікацію стеганографічних методів.

7. Які існують методи інформаційної стеганографії?

8. Які існують види умовного листа?

9. Що таке семаграми?

10. Розкрийте поняття “комп’ютерна стеганографія”.

11. Які умови повинні враховуватись під час використання методів комп’ютерної стеганографії?

РОЗДІЛ 2 ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

2.1 Деякі узагальнені термінологічні поняття

Незважаючи на те, що стеганографія як спосіб приховування секретних даних відома вже протягом тисячоріч, комп'ютерна стеганографія – молодий напрямок, що розвивається. Роком становлення комп'ютерної стеганографії як науки можна вважати 1996 рік, коли на міжнародному семінарі *InfoHiding-96* була введена єдина термінологія [8]. Нижче наведемо деякі означення (більш докладний список означень наведений у *Короткому словнику стеганографічних термінів*).

Стеганографічна система (стегосистема) – сукупність засобів та методів, які використовуються для формування прихованого каналу передавання інформації. Узагальнена модель стегосистеми показана на рис. 2.1. Як дані може використовуватися будь-яка інформація: текст, звук, зображення, Web-сторінки і т.п. Далі для позначення приховуваної інформації будемо використовувати саме термін *повідомлення*, хоча повідомленням може бути як текст або зображення, так і, наприклад, аудіодані.

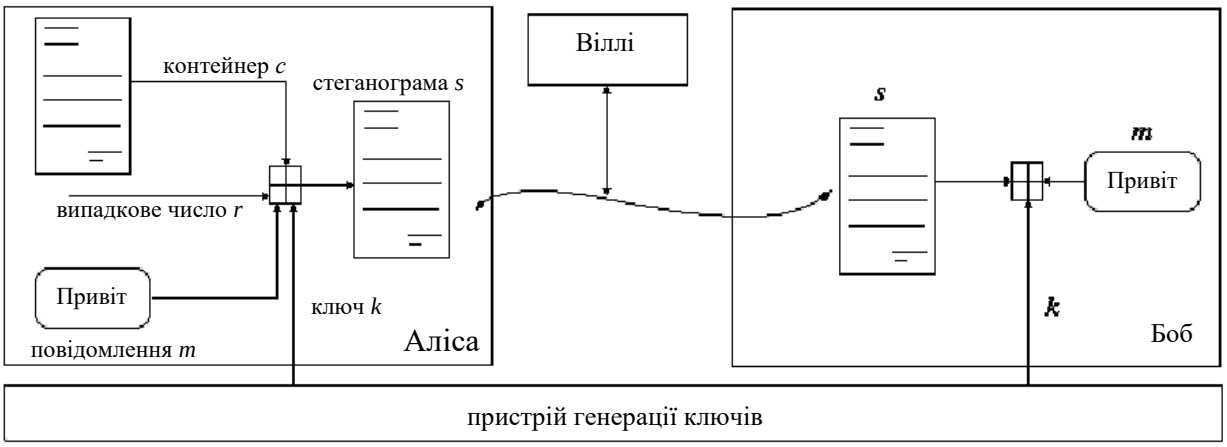


Рисунок 2.1 – Узагальнена схема стеганографічного зв'язку

Контейнер – будь-яка інформація, призначена для приховування таємних повідомлень. *Порожній контейнер* – контейнер без вбудованого повідомлення; *заповнений контейнер* (стеганоконтейнер), що містить вбудовану інформацію.

Вбудоване (приховане) *повідомлення* – повідомлення, що вбудовується в контейнер.

Стеганографічний канал – канал передавання прихованого повідомлення.

Стегоключ – секретний ключ, необхідний для приховування інформації. У залежності від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) у стегосистемі може бути один або кілька стегоключів.

2.2 Узагальнена модель стегосистеми

Модель стеганографічної системи була запропонована Сіммонсом (*G.J.Simmons*) під час вивчення так званої проблеми про «тюремника» [9]. Суть проблеми полягає в тому, що двоє ув'язнених (Аліса і Боб) бажають обмінятися секретними повідомленнями без втручання тюремника (Віллі), який контролює їхній канал зв'язку. При цьому є ряд припущень, що роблять цю проблему більш-менш вирішуваною. Перше припущення, яке полегшує вирішення задачі, полягає в тому, що ув'язнені (Аліса і Боб) перед арештом можуть заздалегідь розділити деякі секретні дані (наприклад, ключ). Інше припущення, навпаки, ускладнює вирішення проблеми, тому що тюремник має право не тільки читати повідомлення, але й модифікувати (змінювати) його.

Більшість стегосистем реалізовано за схемою, яка показана на рис. 2.1. Аліса під час пересилання Бобу секретного повідомлення m випадковим чином (використовуючи датчик r) вибирає безпечне, що не викликає ні в кого підозри, повідомлення c, яке називається *контейнером*. В обраний контейнер вбудовується секретне повідомлення m, використовуючи ключ k, який називається *стегоключем*. Таким чином, при побудові стеганограми s Аліса змінює початковий вигляд контейнера c. Це повинно бути виконано дуже обережно, щоб третя особа, перехопивши лише повідомлення s, не змогла виявити існування повідомлення m. Під час роботи ідеальної стегосистеми ні людина, ні комп'ютер з використанням статистичних критеріїв не повинний виявити факт присутності прихованої інформації в стеганограмі.

Передаючи відкритим каналом стеганограму s, Аліса сподівається, що Віллі не помітить прихованого повідомлення. Боб здатний відновити повідомлення m, тому що знає стеганографічне перетворення, яке

використовується, і має необхідний стегоключ k. При цьому Бобу немає необхідності знати початковий вигляд контейнера c.

Третя особа – Віллі, який спостерігає за листуванням між Алісою і Бобом, – не повинна бути здатною без додаткової інформації визначити містить повідомлення, що пересилається, приховані дані чи ні. Більш формально, якщо спостерігач має доступ до набору контейнерів $C=\{c_1,...,c_n\}$, які можуть передаватися з обох боків зв'язку, то він не повинен бути здатним визначити чи містить контейнер c секретну інформацію.

Надійність стеганографічного зв'язку полягає головним чином у складності процедури виявлення стеганограми.

Формально, процес приховування інформації – це відображення E: $C\times M\to C$, де C – множина можливих контейнерів, а M – множина можливих повідомлень. Причому, якщо $m_1\neq m_2$, де $m_1\in M$ і $m_2\in M$, а $(c_1,m_1)\in C\times M$ і $(c_2,m_2)\in C\times M$, то $E(c_1,m_1)\cap E(c_2,m_2)=\varnothing$. У цьому випадку, процес витягування прихованої інформації – це відображення D: $C\to M$. Очевидно, що необхідно, щоб $|C|\geq|M|$. При цьому, обидва адресати (відправник і одержувач) повинні знати пряме та обернене секретне стеганографічне перетворення.

Взагалі ж як контейнер можна вибрати на *безальтернативній* основі перший же файл, що трапиться. Як контейнери можуть бути використані будь-які комп'ютерні дані типу файлу зображення, цифрового звуку або тексту. Однак на практиці не всі дані можуть використовуватися як контейнер. Це обумовлено тим, що зміни в контейнері, проведені стеганографічними перетвореннями, не повинні бути видимими для стороннього. Тому від контейнера потрібна наявність достатньої кількості надлишкових даних, які можуть бути замінені приховуваною інформацією. Наприклад, при оцифровуванні значень параметра деякого фізичного процесу завжди існують похибки вимірювання, які носять випадковий характер і називаються шумом вимірювання. Такі дані успішно застосовуються в більшості стеганографічних додатків. Бажано, щоб контейнер не використовувався двічі, тому що той, хто атакує, маючи дві стеганограми, отримані з одного й того ж контейнера, може легко знайти і, можливо, відновити повідомлення. Для запобігання повторного застосування контейнера, останні повинні знищуватися відразу ж після їхнього використання.

Для більшості стегосистем множина контейнерів C вибирається таким чином, щоб у результаті стеганографічного перетворення порожній контейнер і заповнений контейнер були подібними, що формально може бути оцінене за допомогою функції подібності.

Означення 2.1. Нехай C – непорожня множина, тоді функція $sim: C \to (\infty, 1]$ називається *функцією подібності* на множині C, якщо для $\forall x,y \in C$ справедливо, що $sim(x,y)=1 \Leftrightarrow x=y$ і $sim(x,y)<1$ для $x \neq y$.

Стегосистема може вважатися надійною при виконанні умови: $sim(c,E(c,m)) \approx 1$ для всіх $m \in M$ і $c \in C$. Причому як контейнер c повинен вибиратися об'єкт, який раніше не використовувався, а несанкціонований користувач не повинен мати доступу до набору контейнерів, використовуваних для секретного зв'язку.

Вибір конкретного контейнера c з набору можливих контейнерів C може здійснюватися довільно (*сурогатний метод* вибору контейнера) або ж шляхом вибору найбільш підходящого, який менше ніж інші зміниться під час стеганографічного перетворення (*селективний метод* вибору контейнера). В останньому випадку підходящий контейнер відбирається відповідно до вирішального правила:

$$c = \max_{x \in C} sim(x, E(x, m)) \qquad (2.1)$$

Наприклад, набір контейнерів C можна отримати в результаті послідовного сканування оригіналу одного й того ж зображення. Через шум сканера щоразу буде виходити різний контейнер, і відправник може найкращим чином обирати для зв'язку будь-який підходящий з них. У цьому випадку єдиною проблемою залишається те, що навіть оптимально організований контейнер дозволяє приховати обмежену кількість даних при дуже великому об'ємі самого контейнера.

У деяких стегосистемах пропонується мати відкриту базу контейнерів. При цьому для того, щоб той, хто атакує, не отримав зразок контейнера, передавачу пропонується, відразу ж після вибору контейнера з бази C, попередньо провести з ним деякі зміни для отримання контейнера c', і лише після цього використовувати його для секретного зв'язку. Однак цей метод має свої недоліки. Якщо той, хто атакує, знає про використовувані методи модифікації контейнерів, то він може сам створити «порожній» контейнер і провести атаку. Навіть якщо він не знає використовуваного

стеганографічного перетворення, то він може створити схожий контейнер і порівняти його зі стеганограмою.

У деяких стегосистемах пропонується не вибирати контейнер, а будувати його, моделюючи необхідні статистичні властивості (*конструювальний* метод стеганографії).

До стеганографічної системи зазвичай висувають такі основні вимоги:

1. У якості стеганографічного перетворення повинен застосовуватися загальновідомий алгоритм і секретний стегоключ.
2. Метод приховування повинен забезпечити автентичність і цілісність файлу.
3. Тільки при наявності правильного стегоключа можна виявити, витягти і довести існування прихованого повідомлення.
4. Навіть, якщо той, хто атакує, знає про факт існування прихованого повідомлення (або саме повідомлення), це не повинно дозволити йому довести даний факт третій особі і, тим більше, знайти подібні повідомлення в інших повідомленнях, поки стегоключ зберігається в таємниці.
5. Ніхто не повинен знайти який-небудь статистичний доказ існування прихованого повідомлення, його виявлення без знання ключа повинно бути обчислювально складною задачею.

Таким чином, властивості контейнера повинні бути модифіковані так, щоб зміну неможливо було виявити при контролі. Ця вимога визначає якість приховування вбудовуваного повідомлення: для безперешкодного проходження повідомлення стеганоканалом зв’язку воно ніяким чином не повинно привернути увагу того, хто атакує. Окрім цього стеганоповідомлення повинно бути стійким до перекручувань, у тому числі і зловмисних. У процесі передавання стеганограма може зазнати трансформації: зменшуватися або збільшуватися, перетворюватися в інший формат, ущільнюватись, у тому числі алгоритмами ущільнення з втратою даних. І, нарешті, для зберігання цілісності повідомлення, що вбудовується, необхідно використовувати код з виправленням помилки, а для підвищення надійності повідомлення, що вбудовується, бажано продублювати.

2.3 Класифікація стегосистем

За аналогією з криптографічними системами, у стеганографії розрізняють системи із секретним ключем і системи з відкритим ключем.

У стеганографічній системі з секретним ключем використовується один ключ, який повинен бути заздалегідь відомий абонентам до початку прихованого обміну секретними повідомленнями або пересланий захищеним каналом.

У стегосистемі з відкритим ключем для вбудовування і витягнення таємного повідомлення використовуються різні ключі, причому вивести один ключ з іншого за допомогою обчислень неможливо. Один з ключів (відкритий) може передаватися вільно незахищеним каналом зв'язку, а другий, секретний ключ, - захищеним каналом. Дана схема добре працює при взаємній недовірі відправника й одержувача.

З огляду на все різноманіття стеганографічних систем зведемо їх до таких типів: безключові стегосистеми, системи із секретним ключем, системи з відкритим ключем і змішані стегосистеми.

2.3.1 Безключові стегосистеми

Для функціонування безключових стегосистем не потрібно ніяких додаткових даних у вигляді стегоключа крім алгоритму стеганографічного перетворення.

Означення 2.2. Сукупність $\Xi=<C,M,D,E>$, де C – множина можливих контейнерів; M – множина секретних повідомлень, $|C|\geq|M|$; E: $C\times M\to C$ і D: $C\to M$ – функції приховування і витягування повідомлення з контейнера, причому $D(E(c,m))=m$ для будь-яких $m\in M$ та $c\in C$, називається *безключовою стегосистемою*.

З означення випливає, що безпека безключових стегосистем базується на таємності використовуваних стеганографічних перетворень E і D. Це суперечить основному принципові Кірхгофа для систем захисту інформації. Дійсно, якщо припустити, що противник знає алгоритми E і D, які використовуються для прихованого передавання інформації, то він здатний витягти будь-яку приховану інформацію з перехоплених стеганограм.

Найчастіше для підвищення безпеки безключових систем, перед початком процесу стеганографічного приховування попередньо виконується шифрування приховуваної інформації. Зрозуміло, що такий підхід збільшує захищеність усього процесу зв'язку, оскільки це ускладнює виявлення прихованого повідомлення. Однак «сильні» стеганографічні системи, як правило, не мають потреби в попередньому шифруванні приховуваних повідомлень.

2.3.2 Стегосистеми із секретним ключем

Дотримуючись закону Кірхгофса, безпека системи повинна ґрунтуватися на деякій секретній інформації, без знання якої не можна витягти з контейнера секретну інформацію. У стегосистемах така інформація називається *стегоключем.* Відправник, вбудовуючи секретне повідомлення в обраний контейнер c, використовує секретний стегоключ k. Якщо використовуваний у стеганографічному перетворенні ключ k відомий одержувачеві, то він зможе витягти приховане повідомлення з контейнера. Без знання такого ключа будь-який інший користувач цього зробити не зможе.

Означення 2.3. Стегосистемою із секретним ключем називається сукупність $\Xi=<C,M,K,D,E>$, де C – множина можливих контейнерів; M – множина секретних повідомлень, причому $|C|\geq|M|$; K – множина секретних ключів; $E_K{:}C\times M\times K\to C$ и $D_K{:}C\times K\to M$ – стеганографічне перетворення з властивістю $D_K(E_K(c,m,k),k)=m$ для будь-яких $m\in M$, $c\in C$ і $k\in K$.

Даний тип стегосистем припускає наявність безпечного каналу для обміну стегоключами.

Іноді стегоключ k обчислюють за допомогою секретної хеш-функції *Hash*, використовуючи деякі характерні риси контейнера: $k=Hash$ (особливості контейнера). Якщо стеганографічне перетворення E не змінює в остаточній стеганограмі обрані особливості контейнера, то одержувач також зможе обчислити стегоключ (хоча й у цьому випадку захист залежить від таємності функції *Hash*, і, таким чином, знову порушується принцип Кірхгофса). Очевидно, що, для досягнення адекватного рівня захисту, таку особливість у контейнері необхідно вибирати дуже акуратно.

У деяких алгоритмах під час витягування прихованої інформації додатково потрібні відомості про вихідний контейнер або деякі інші дані, які відсутні у стеганограмі. Такі системи становлять обмежений інтерес, оскільки вони вимагають передавання початкового вигляду контейнера, що еквівалентно традиційній задачі ключового обміну. Подібні алгоритми можуть бути відзначені як окремий випадок стегосистем з секретним ключем, у яких $K=C$ або $K=C\times K'$, де K' – означає додатковий набір секретних ключів.

2.3.3 Стегосистеми з відкритим ключем

Стеганографічні системи з відкритим ключем не мають потреби в додатковому каналі ключового обміну. Для їхнього функціонування необхідно мати два стегоключі: один секретний, який користувач повинен зберігати в таємниці, а другий – відкритий, який зберігається в доступному для всіх місці. При цьому відкритий ключ використовується в процесі приховування інформації, а секретний – для її витягування.

Означення 2.4. Стегосистемою з відкритим ключем називається сукупність $\Xi=<C,M,K,D,E>$, де C – множина можливих контейнерів; M – множина секретних повідомлень, причому $|C|\geq|M|$; $K=(k_1,k_2)$ – множина пар стегоключів (відкритий ключ k_1 використовується для приховування інформації, а секретний k_2 – для витягування); $E_K: C\times M\times k_1\rightarrow C$ і $D_K: C\times k_2\rightarrow M$ – стеганографічне перетворення з властивістю $D_K(E_K(c,m,k_1),k_2)=m$ для будь-яких $m\in M$, $c\in C$.

Простим способом реалізації подібних стегосистем є використання криптосистем з відкритим ключем. Стегосистеми з відкритими ключами використовують той факт, що функція витягування прихованої інформації D може бути застосована до будь-якого контейнера поза залежністю від того, знаходиться в ньому приховане повідомлення чи ні. Якщо в контейнері відсутнє приховане повідомлення, то завжди буде відновлюватися деяка випадкова послідовність. Якщо ця послідовність статистично не відрізняється від шифртексту криптосистеми з відкритим ключем, тоді в безпечній стегосистемі можна приховувати отриманий у такий спосіб шифртекст, а не відкритий.

2.3.4 Змішані стегосистеми

У більшості застосувань перевага віддається безключовим стегосистемам, хоча такі системи можуть бути відразу скомпрометовані у випадку, якщо противник дізнається про застосовуване стеганографічне перетворення. У зв’язку з цим у безключових стегосистемах часто використовують особливості криптографічних систем з відкритим і/або секретним ключем. Розглянемо один такий приклад [10].

Для обміну секретними ключами стегосистеми введемо поняття протоколу, реалізованого на основі криптосистеми з відкритими ключами (рис. 2.2). Спочатку Аліса генерує випадкову пару відкритого і секретного ключів, а потім передає відкритий ключ Бобу прихованим каналом,

створеним безключовою системою. Ні Боб, ні Віллі не можуть визначити, яка інформація передавалася прихованим каналом: ключ або ж випадкові біти. Однак Боб може запідозрити, що стеганограма від Аліси може містити її відкритий ключ і постарається його виділити. Після цього він шифрує за допомогою виділеного ключа секретний стегоключ *k*, проводить приховування результату шифрування в контейнер і його передавання Алісі. Віллі може спробувати витягти секретну інформацію зі стеганограми, але отримає лише випадковий шифртекст. Аліса витягає зі стеганограми приховану криптограму і розшифровує її своїм секретним ключем. Таким чином, сторони обмінялися секретним стегоключем *k* для спільного використання.

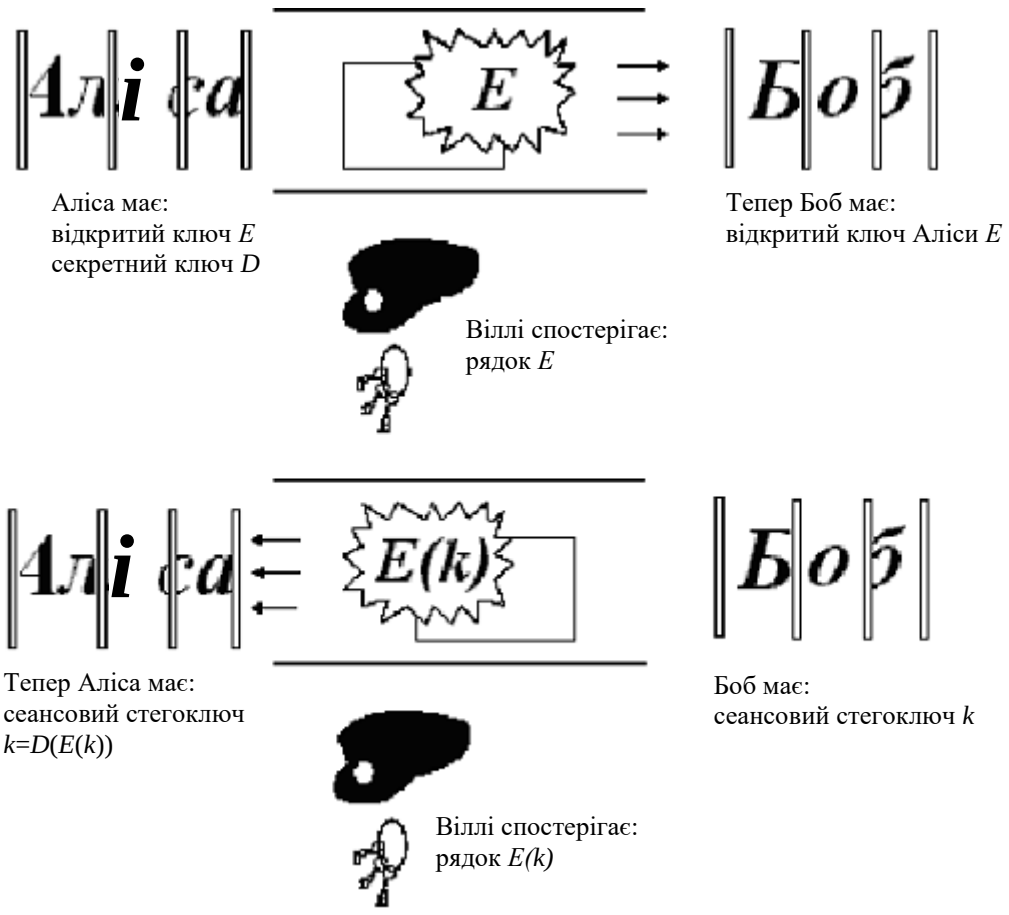


Рисунок2.2. Приклад протоколу обміну стегоключами

Відзначимо, що розглянута стегосистема не позбавлена недоліків і наведена лише як приклад змішаної системи.

2.4 Стеганографічний аналіз

Основною метою стеганоаналізу є моделювання стеганографічних систем та їхнє дослідження для отримання якісних і кількісних оцінок надійності використовуваного стеганографічного перетворення, а також побудова методів виявлення приховуваної в контейнері інформації, її зміни або руйнування.

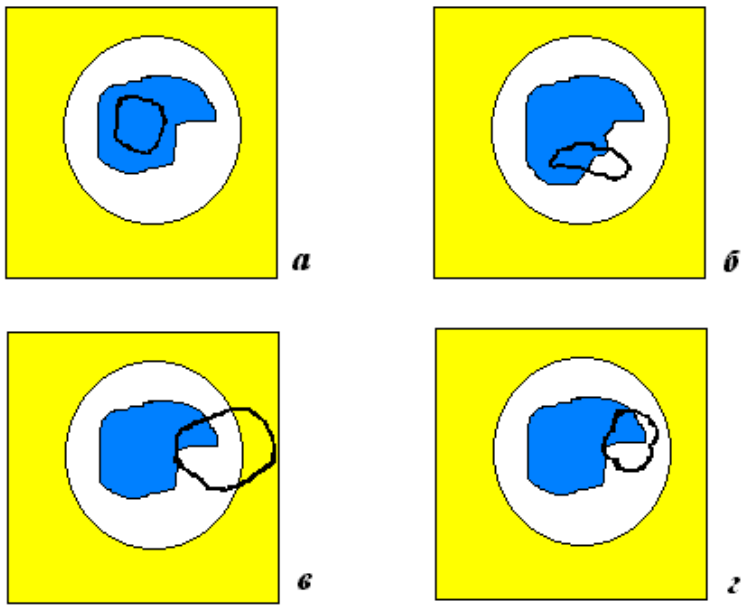
Термінологія стеганоаналізу аналогічна термінології криптоаналізу, однак є деякі істотні розходження. Криптоаналіз застосовується з метою дешифрування криптограм, а стеганоаналіз – для виявлення прихованої інформації. У криптоаналізі аналізуються частина відкритого тексту (можливо, не одна) і частина шифртексту, у стеганоаналізі – частини контейнера, стеганограми і можливі частини приховуваного повідомлення. У результаті шифрування виходить криптограма, а в результаті стеганографічного перетворення – стеганограма. Повідомлення, яке вбудовується в контейнер, може бути або відкритим, або зашифрованим. Якщо воно зашифроване, то після його успішного витягування зі стеганограми необхідно застосувати криптоаналітичні методи для дешифрування криптограми.

За рівнем забезпечення таємності стегосистеми поділяються на теоретично стійкі системи, практично стійкі і нестійкі.

Теоретично стійка (абсолютно надійна) стегосистема здійснює приховування інформації тільки в тих фрагментах контейнера, значення елементів яких не перевищують рівень шумів або помилок квантування, і при цьому теоретично доведено, що неможливо створити стеганалітичний метод виявлення прихованої інформації (рис. 2.3,*а*).

Практично стійка стегосистема проводить таку модифікацію фрагментів контейнера, зміни яких можуть бути виявлені, але відомо, що на даний момент необхідні стеганалітичні методи в противника відсутні або поки що не розроблені (рис. 2.3,*б)*.

Нестійка стегосистема приховує інформацію таким чином, що існуючі стеганалітичні засоби дозволяють її виявити (рис. 2.3,*в)*. У цьому випадку стеганографічний аналіз допомагає знайти уразливі місця стеганографічного перетворення і провести його покращення таким чином, щоб усі зміни, внесені в контейнер, знову виявилися б в області теоретичної або практичної нерозрізненості (рис. 2.3,*г)*.



– область захисту стегосистеми;

– область теоретичної нерозрізненості, де приховані елементи практично не можуть виявитися, тому що знаходяться нижче рівня шуму і помилок квантування;

– область практичної нерозрізненості, у якій зміни контейнера не виявляються існуючими в противника аналітичними методами;

– область, у якій зміни контейнера виявляються стеганоаналітичним методом.

Рисунок 2.3 – Ілюстрація співвідношення методів стеганозахисту і стеганоаналізу

2.4.1 Можливі атаки на стеганографічну систему

Стегосистема вважається зламаною, якщо противникові, принаймні, вдалося довести існування прихованого повідомлення в перехопленому контейнері. Передбачається, що він здатний проводити будь-які види атак і має необмежені обчислювальні можливості. Якщо йому не вдається підтвердити гіпотезу про те, що в контейнері приховано секретне повідомлення, то стегосистема вважається стійкою. Зазвичай виділяють декілька етапів зламу стеганографічної системи:

– виявлення факту присутності прихованої інформації;

– витягування приховуваного повідомлення;

– перекручування (підміна) приховуваної інформації;

– видалення (руйнування) приховуваного повідомлення;

– заборона на здійснення будь-якого пересилання інформації, у тому числі і приховуваної.

Перші два етапи відносяться до пасивних атак на стегосистему, а останні – до активних (або зловмисних) атак. Виділяють такі види атак на стегосистеми:

– *атака з відомою стеганограмою*, коли для аналізу доступна тільки стеганограма;

– *атака з відомим контейнером*, коли є можливість проводити аналіз зі стеганограмою і відповідним йому вихідним контейнером;

– *атака з відомим прихованим повідомленням*, якщо для аналізу надані зразки приховуваного повідомлення і відповідної стеганограми. Результати їхнього спільного аналізу можуть бути використані для проведення наступних атак на стегосистему (хоча це може виявитися дуже важкою задачею, яка еквівалентна першій);

– *атака з вибором контейнера*, якщо під час аналізу відомий використовуваний стеганографічний алгоритм і вихідний зразок контейнера;

– *атака з вибором стеганограми*, коли за допомогою досліджуваної стегосистеми (або алгоритму) є можливість створювати відповідні стеганограми для обраного повідомлення. Мета такої атаки полягає в тому, щоб визначити, які зразки стеганограм можуть ідентифікувати використання певних стегозасобів або алгоритмів;

– *атака з повною інформацією*, якщо надана вся необхідна інформація для аналізу: стеганографічний алгоритм, контейнери і відповідні їм стеганограми.

Основна мета атаки на стеганографічну систему аналогічна атакам на криптосистему з тією лише різницею, що різко зростає значимість активних атак. Будь-який контейнер може бути змінений з метою видалення або руйнування приховуваного повідомлення, незалежно від того існує воно в контейнері чи ні. Виявлення існування прихованих даних зберігає час на етапі їхнього видалення, тому що буде потрібно обробляти тільки ті контейнери, які містять приховану інформацію. Навіть за найкращих умов для атаки, задача витягування прихованого повідомлення з контейнера може виявитися дуже складною. Однозначно стверджувати про факт наявності прихованої інформації можна лише після її виділення в явному вигляді. Іноді метою стеганографічного аналізу є не алгоритм

взагалі, а пошук, наприклад, конкретного стегоключа, що використовується для вибору бітів контейнера в стеганоперетвореннi.

2.4.2 Основні етапи практичного стеганоаналізу

Будь-яке стеганографічне перетворення, як правило, базується на двох принципах:

– як носій прихованої інформації (контейнер) вибирається об’єкт, що допускає перекручування власної інформації, зберігаючи при цьому функціональність;

– рівень внесених перекручувань повинний бути нижче рівня чутливості засобів розпізнавання.

Як вказувалося, як контейнери можуть використовуватися практично всі носії інформації, застосовувані в мережах передавання даних. При цьому методи приховування інформації орієнтуються в основному на внутрішню структуру контейнера, яка може являти собою символьні або бітові дані, коефіцієнти перетворення Фур’є, широкосмугове кодування, коефіцієнти ущільнення та ін. Приховування інформації в медіа середовищі вимагає дотримання певних умов при внесенні змін, щоб не проявлялися сліди використання стеганографічного перетворення. Наприклад, стосовно до зображень, такі зміни можуть час від часу ставати видимими для людського ока і вказувати на використання стеганографічних засобів. Аналіз навмання вибраних зображень в Інтернеті показує, що деякі з них не мають тієї інформаційної надлишковості, що її повинні мати типові файли, тобто в них міститься інформація, в якій немає необхідності під час звичайного візуального перегляду зображення. Подібну картину можна отримати, наприклад, у результаті наявності бруду на склі сканера або обробки файлу зображення спеціальними ефектами, передбаченими графічними редакторами, або ж використовуючи стеганографічне перетворення. Сліди, залишені стегозасобами, можуть фактично допомогти виявити існування вбудованого повідомлення, таким чином, компрометуючи стегосистему в цілому.

Однією з головних задач стеганоаналізу є дослідження можливих слідів застосування стеганографічних засобів і розробка методів, які б дозволяли виявляти факти їхнього використання. Застосування конкретного стеганографічного перетворення вимагає від стеганалітика персонального підходу до його дослідження.

Дослідження повідомлень, прихованих стеганографічними засобами, або, точніше, підозрілих у цьому відношенні, є досить болісним процесом. Часто стеганалітик не може навіть сказати, наприклад, чи приховується якесь змістовне повідомлення за незграбно складеним або просто безграмотним текстом. І, навіть, якщо він цілком впевнений, що таке повідомлення там приховано, знайти його найчастіше просто неможливо.

Для успішного проведення стеганоаналізу необхідно, але не достатньо:

– мати для аналізу стегозасіб, за допомогою якого здійснюється приховування повідомлення;

– мати можливість відновлювати застосовувані в стегосистемі криптографічний і стеганографічний алгоритми, проводити їхній експертний аналіз і розробляти алгоритм визначення ключів;

– мати в наявності необхідний обчислювальний ресурс для проведення стеганоаналізу;

– підтримувати на відповідному рівні теоретичні і практичні знання в галузі цифрової стеганографії.

На практиці стеганографічний аналіз розвивається декількома напрямками.

По-перше, це розробка ймовірнісно-статистичних методів розпізнавання, застосування елементів штучного інтелекту для отримання оцінок надійності стеганографічних перетворень і при створенні фільтрів (детекторів) для аналізу інформаційних потоків з метою виявлення стеганограм. У цьому випадку перевірка наявності прихованої інформації зводиться до певної оцінки з використанням статистичних критеріїв (послідовної кореляції, ентропії зображення, дисперсії молодшого біта й ін). Розроблювані з цією метою засоби повинні бути універсальними і забезпечувати необхідний рівень похибки під час розпізнавання прихованих повідомлень, особливо в тих випадках, коли використовується попереднє шифрування.

По-друге, це аналіз конкретних програмних стегозасобів із метою відновлення алгоритмів і оптимальної розробки методу їхнього аналізу. Основна складність тут полягає у великій трудомісткості, яка обумовлена необхідністю індивідуального підходу до кожного конкретного алгоритму, що реалізує метод приховування інформації, а також об’ємом обчислень, необхідних для відновлення стегоключів.

По-третє, це розробка технології активних і зловмисних атак для внесення невідновлюваних перекручувань у передбачувану стеганограму з метою спровокувати її повторне передавання в іншому контейнері, що підтвердило б факт використання стегозасобів.

2.4.3 Аналіз стійкості стегосистеми

Створення й експлуатація надійного стеганографічного засобу передбачає наявність деякого інструментарію для його контролю й оцінювання. Кількісне оцінювання стійкості стеганографічної системи захисту до зовнішніх впливів являє собою складну задачу, яка зазвичай на практиці реалізується методами системного аналізу, математичного моделювання або експериментального дослідження.

Як правило, професійно розроблена стегосистема забезпечує трирівневу модель захисту інформації, що вирішує дві основні задачі. По-перше, це *приховування* самого факту наявності інформації, що захищається, (перший рівень захисту) і, по-друге, блокування несанкціонованого доступу до інформації, яке здійснюється шляхом вибору відповідного методу приховування інформації (другий рівень захисту). Нарешті, передбачається третій рівень захисту – криптографічний захист (шифрування) приховуваної інформації.

На рис. 2.4 представлена можлива структура процесу моделювання й оцінювання стійкості стегосистеми [55]. Як видно з представленої структури, надійність і час стійкості стегосистеми під час проведення аналізу й випробувань визначаються обчислювальними можливостями комплексу.

Оцінювання якості основної характеристики стегосистеми – рівня скритності – забезпечується шляхом проведення аналітичних досліджень (стеганоаналізу) і натурних випробувань. Для оцінювання якості стеганографічного приховування часто застосовують відомі методи з інших галузей, у першу чергу – криптоаналізу.

Рисунок 2.4 – Модель аналізу загроз і оцінювання стійкості стегосистеми

Оскільки абонент-одержувач може відновлювати приховану інформацію з прийнятого повідомлення, то існує деякий механізм її витягування. Якщо противник, висуваючи гіпотези про можливе стеганографічне перетворення, має деякий інструмент для їхньої перевірки, то він має шанси на підтвердження факту існування прихованої інформації, здійснення пошуку механізму витягання секретного повідомлення і розкриття змісту листування. Тому, у першу чергу, як детектування стеганограм можна застосовувати різновиди описаних вище атак на стегосистему і велику частину методів криптоаналізу.

У деяких випадках досить ефективним є метод оцінювання рівня скритності стегозасобів на основі аналізу їхніх статистичних характеристик. Статистична теорія дає кількісні критерії випадковості, що дозволяє створювати “детектори”, які виявляють статистичні розбіжності

між послідовностями. Якщо є необхідний об'єм аналізованої послідовності, то з досить високою ймовірністю можна судити про випадковості виділеної для аналізу послідовності з контейнера. На початковому етапі аналізу можна скористатися традиційними статистичними (хі-квадрат, тести на заборонені символи, на довжину циклу, «дні народжень»), емпіричними (перевірки частот, серій, інтервалів, перестановок, перевірки на монотонність, покер-тестом, тестом збирача купонів) або спектральними тестами. Далі використовуються більш «тонкі» методи, іноді розроблювані під конкретну задачу.

Для порівняльного оцінювання якості стеганографічних засобів розробляють різні метрики, що дають кількісні оцінки. Найбільша їхня кількість розроблена для стеганометодів (методів цифрових водяних знаків), які працюють із зображеннями. Звичайно такі метрики оперують із зображенням на рівні пікселів, хоча після деякої адаптації вони застосовні і до інших способів опису зображення, а також до аудіо даних. Найбільш популярною метрикою під час аналізу рівня перекручувань, що вносяться у контейнер під час приховування в ньому інформації, є взяте з радіотехніки співвідношення сигнал-шум, яке обчислюється в децибелах.

Нижче наведений ряд метрик, використовуваних під час оцінювання перекручувань, які вносяться стеганографічними перетвореннями в зображення [50]. У приведених співвідношеннях через $p_{x,y}$ позначається піксел порожнього контейнера з координатою (x,y), а через $\tilde{p}_{x,y}$ – відповідний піксель заповненого контейнера. У метриці *GSSNR* аналізоване зображення попередньо розбивається на блоки з пікселів розміром $X \times Y$, де X і Y – число рядків і колонок, відповідно:

– середня абсолютна різниця:

$$AD = \frac{1}{XY} \sum_{x,y} \left| p_{x,y} - \tilde{p}_{x,y} \right|; \tag{2.2}$$

– середня квадратична помилка:

$$MSE = \frac{1}{XY} \sum_{x,y} \left(p_{x,y} - \tilde{p}_{x,y} \right)^2; \tag{2.3}$$

– L^p-норма:

$$L^p = \left(\frac{1}{XY} \sum_{x,y} \left| p_{x,y} - \tilde{p}_{x,y} \right|^p \right)^{1/p}; \tag{2.4}$$

– середня квадратична помилка оператора Лапласа:

$$LMSE = \sum_{x,y}\left(\nabla^2 p_{x,y} - \nabla^2 \tilde{p}_{x,y}\right)^2 / \sum_{x,y}\left(\nabla^2 p_{x,y}\right)^2; \quad (2.5)$$

– відношення сигнал-шум:

$$SNR = \sum_{x,y} p^2{}_{x,y} / \sum_{x,y}\left(p_{x,y} - \tilde{p}_{x,y}\right)^2; \quad (2.6)$$

– максимальне відношення сигнал-шум:

$$PSNR = XY \max_{x,y} p^2{}_{x,y} / \sum_{x,y}\left(p_{x,y} - \tilde{p}_{x,y}\right)^2; \quad (2.7)$$

– нормалізована взаємна кореляція:

$$NC = \sum_{x,y} p_{x,y}\tilde{p}_{x,y} / \sum_{x,y} p^2{}_{x,y}\ ; \quad (2.8)$$

– якість кореляції:

$$CQ = \sum_{x,y} p_{x,y}\tilde{p}_{x,y} / \sum_{x,y} p_{x,y}\ ; \quad (2.9)$$

– загальне сигма відношення сигнал-шум:

$$GSSNR = \sum_{b}\sigma_b^2 / \sum_{b}\left(\sigma_b - \tilde{\sigma}_b\right)^2\ , \quad (2.10)$$

де $\sigma_b = \sqrt{\frac{1}{n}\sum_{block\,b} p_{x,y}^2 - (\frac{1}{n}\sum_{block\,b} p_{x,y})^2}$;

– подібність гістограм:

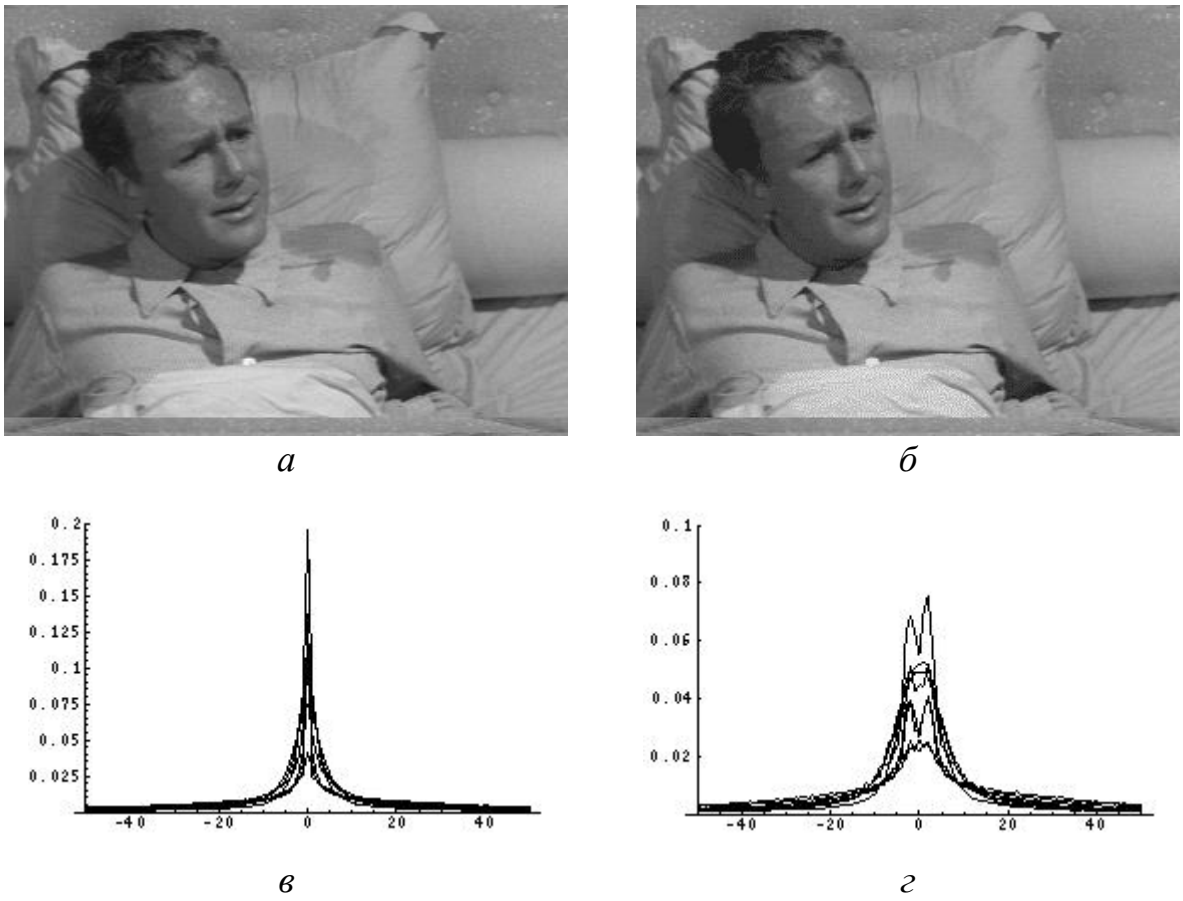
$$HS = \sum_{c=0}^{255}\left| f_I(c) - f_{\tilde{I}}(c)\right|, \quad (2.11)$$

де $f_I(c)$ – відносна частота градації кольору c у зображенні з 256 рівнями кольоровості.

Для ілюстрації розглянемо один приклад, який описує принцип, використовуваний при оцінюванні надійності приховування стеганоперетворення, а також при побудові детекторів стеганограм [49].

Припустимо, що в результаті роботи стеганографічної утиліти PGMSTEALTH шляхом приховування інформації, що захищається, у молодших бітах пікселів зображення-контейнера отримується стеганограма. У вихідному контейнері (рис. 2.5,*а*), який має розміри 640*480 пікселів і 256 відтінків сірого кольору, що відповідає приблизно

300 Кбітам інформації, приховується текстова інформація. Зовні результувальна стеганограма (рис. 2.5,*б)* залишається практично незмінною, за винятком деяких відтінків. Однак внесений при цьому в зображення корисний «шум» (тобто приховувана інформація) буде природно статистично відрізнятися від звичайних випадкових перешкод.



а *б*

в *г*

Рисунок 2.5 – Приклад аналізу стеганограм за допомогою фільтра Лапласа

Як інструмент аналізу отриманого зображення оберемо дискретний фільтр Лапласа верхніх частот:

$$L(P(x, y))=P(x+1,y)+P(x-1, y)+P(x,y+1)+P(x,y-1)-4P(x,y),$$

де *(x, y)* – координати пікселів зображення.

За допомогою даного фільтра можна провести оцінювання подібності відтінків прилеглих пікселів. На рис. 2.5,*в* і 2.5,*г* наведені гістограми фільтрів Лапласа для декількох зображень-контейнерів і отриманих стеганограм, відповідно. Як і очікувалося, у вихідних контейнерах сусідні пікселі мають схожі кольори, що на рис. 2.5,*г* відображено групуванням гістограм в околі значення нуля. Навпаки, гістограми, які відносяться до

стеганограм поблизу цього значення, є більш розмитими. Ці результати ще не надають твердого доказу існування в аналізованому зображенні прихованої інформації, але сигналізують про те, що з великою імовірністю зображення могло піддатися деяким модифікаціям.

2.4.4 Абсолютно надійна стегосистема

У [11] наведено формальне теоретико-інформаційне означення стійкості стегосистеми стосовно пасивних атак. Головна ідея базується на випадковому виборі контейнерів з множини C з імовірністю P_C.

Вбудовування в контейнер секретного повідомлення можна описати як функцію, визначену на C. Нехай P_S – ймовірність $E_к(c,m,k)$ на множині всіх можливих стеганограм, отриманих за допомогою стегосистеми. Якщо контейнер c ніколи не використовується для отримання стеганограми, то $P_S(c)=0$. Для обчислення імовірності P_S необхідно врахувати розподіл імовірностей на множині ключів K та множині повідомлень M.

Визначимо на множині Q таке співвідношення для відносної ентропії:

$$D(P_1 \,\|\, P_2) = \sum_{q \in Q} P_1(q) \log_2 \frac{P_1(q)}{P_2(q)}, \qquad (2.12)$$

за допомогою якого можна виміряти неефективність прийняття невірної гіпотези про розподіл P_2 у випадку істинного розподілу P_1.

Таким чином, для стеганографічного перетворення можна отримати деяку оцінку. Дамо означення надійності стегосистеми в термінах $D(P_C||P_S)$.

Означення 2.5. (абсолютна надійність) Нехай Ξ – стеганографічна система, P_S – розподіл імовірностей, переданих через канал зв'язку стеганограм, P_C – розподіл імовірностей використання контейнерів. Система Ξ називається ε-надійною до пасивних атак, якщо $D(P_C||P_S)\le\varepsilon$, і абсолютно надійною, якщо $\varepsilon=0$.

Співвідношення $D(P_C||P_S)$ дорівнює нулеві тоді і тільки тоді, коли обидва розподіли імовірності рівні. Таким чином, стеганографічна система є теоретично абсолютно надійною, якщо процес вбудовування секретного повідомлення в контейнер не змінює P_C. Зовсім безпечна система може бути створена, наприклад, на основі одноразової гамми.

Теорема 2.1. Існує абсолютно надійна стегосистема.

Проведемо конструктивне доведення даного твердження. Нехай C – набір усіх бітових рядків довжини n, P_C – рівномірний розподіл імовірності

контейнера на C і e – секретне повідомлення, $e \in C$. Відправник вибирає навмання $c \in C$ і обчислює $s=c \oplus e$, де $\oplus$ – порозрядна операція XOR. Результуюча стеганограма s рівномірно розподілена на C, тому що $P_C=P_S$ і $D(P_C||P_S)=0$. Секретне повідомлення e може бути відновлено шляхом обчислення $s \oplus c$.

2.4.5 Пасивна атака: виявлення прихованих повідомлень

Пасивний противник (Віллі) прагне відповісти на запитання, чи містить пересланий контейнер приховану інформацію чи ні. Для цього йому необхідно провести оцінювання неоднорідності деяких параметрів контейнера, виявити в ньому «підозрілі» ділянки, завищене зашумлення та інші сліди присутності прихованих повідомлень. Ця задача може бути формалізована у вигляді проблеми перевірки статистичних гіпотез. З цією метою введемо тестову функцію f: $C \to \{0,1\}$:

$$f(c) = \begin{cases} 1, & \textit{якщо с містить прихов.повідом.} \\ 0, & \textit{в іншому випадку} \end{cases}, \qquad (2.13)$$

за допомогою якої Віллі оцінює повідомлення, що перехоплюються в несекретному каналі. У деяких випадках Віллі правильно виділяє стеганограми, а в деяких – ні, роблячи при цьому помилки другого роду, β. Крім того, Віллі може помилково виявити приховане повідомлення в контейнері, який не містить інформацію. Тоді він зробить помилку першого роду. Практичні стегосистеми намагаються максимізувати для пасивного атакуючого помилку другого роду. Ідеальна стегосистема повинна забезпечувати помилку другого роду $\beta=1$. Далі буде показано, що всі абсолютно надійні стегосистеми мають цю властивість (за умови, що той, хто атакує, робить помилку першого роду з нульовою ймовірністю).

Для ε-надійних стеганографічних систем імовірності α і β, з якими той хто атакує робить помилки першого і другого роду, пов'язані між собою відповідно до поданої нижче теореми.

Теорема 2.2 [11]. Нехай Ξ – стеганографічна система, яка є ε-надійною проти пасивних атак. Тоді імовірність β того, що противник не знайде приховане повідомлення, і імовірність α того, що він невірно виявить приховане повідомлення, задовольняють співвідношення: $d(\alpha,\beta) \le \varepsilon$, де $d(\alpha,\beta)$ – відносна двійкова ентропія, що визначається як

$$d(\alpha,\beta)=\alpha\log_2\frac{\alpha}{1-\beta}+(1-\alpha)\log_2\frac{1-\alpha}{\beta}. \qquad (2.14)$$

зокрема, якщо $\alpha=0$, то $\beta\geq 2^{-\varepsilon}$.

Доведення. У випадку, коли контейнери не містять прихованого повідомлення, то імовірність їхнього розподілу відповідає P_C. Розглянемо випадкову величину $f(C)$ і обчислимо її розподіл π_C. У випадку, коли $f(C)=1$, той, хто атакує, робить помилку другого роду. Таким чином, $\pi_3(1)=\alpha$ і $\pi_3(0)=1-\alpha$. Якщо контейнер містить приховане повідомлення, то розподіл імовірності відповідає P_S. Обчислимо імовірність π_S для $f(S)$. У випадку, коли $f(S)=0$, той, хто атакує, не може знайти приховане повідомлення і робить помилку першого роду. Таким чином, $\pi_S(0)=\beta$ і $\pi_S(1)=1-\beta$. Відносна ентропія, відповідно до (2.12), $D(\pi_C||\pi_S)$ може бути виражена в такий спосіб:

$$D(\pi_C\,\|\,\pi_S)=\sum_{q\in\{0,1\}}\pi_C(q)\log_2\frac{\pi_C(q)}{\pi_S(q)}=(1-\alpha)\log_2\frac{1-\alpha}{\beta}+\alpha\log_2\frac{\alpha}{1-\beta}=d(\alpha,\beta)$$

.

Відзначимо таку властивість функції відносної ентропії: детермінована обробка не може збільшити відносну ентропію між двома розподілами. Нехай Q_0 і Q_1 – дві випадкових величини, визначені на множині Q з відповідними розподілами імовірностей P_{Q0} і P_{Q1}, а f – функція, що відображає Q на T: $Q\to T$. Тоді, $D(P_{T0}||P_{T1})\leq D(P_{Q0}||P_{Q1})$, де через P_{T0} і P_{T1} відповідно позначені імовірності $f(Q_o)$ і $f(Q_1)$. Отже, $d(\alpha,\beta)=D(\pi_C||\pi_S)\leq D(P_C||P_S)\leq\varepsilon$. Враховуючи $d(0,\beta)=\log_2 1/\beta$, отримаємо: $\lim_{\alpha\to 0}\log_2\alpha/(1-\beta)=0$. Таким чином, якщо $\alpha=0$, то $\beta\geq 2^{-\varepsilon}$. Отже, для ε-надійної стегосистеми з $\alpha=0$, необхідно забезпечити, щоб $\varepsilon\to 0$. Тоді імовірність $\beta\to 1$. Тому, якщо ε буде мале, то той, хто атакує, буде помилково виявляти стеганограми з дуже високою імовірністю.

2.4.6 Активні і зловмисні атаки

Дія завжди породжує протидію: навіть якщо приховане повідомлення неможливо виділити і прочитати, його можна виявити і порівняно легко знищити. Наприклад, якщо повідомлення приховане у файлі формату GIF шляхом перестановки кольорів, то вплив на цей файл шляхом випадкової зміни проходження кольорів у палітрі зробить повідомлення таким, що не витягується, тобто – знищить його.

Під час проектування та дослідження стегосистем спеціальна увага повинна бути приділена вивченню впливу на них активних і зловмисних атак. *Активні атаки* здатні змінити контейнер під час зв'язку: Віллі може перехопити стеганограму, послану від Аліси до Боба, змінити її і відправити результат Бобу. Тут передбачається, що при активній атаці неможливо повністю замінити контейнер і його семантику, а можна тільки провести незначні зміни так, щоб оригінал і змінений контейнер залишалися візуально і семантично подібними. *Зловмисними атаками* будемо вважати такі, при яких повідомлення повністю руйнується або організується стеганографічний обмін від імені одного з партнерів зв'язку.

Стеганографічні системи надзвичайно чутливі до модифікацій контейнера (наприклад, для зображення - це згладжування і фільтрація, для звуку – фільтрація). Іноді просте ущільнення з втратами може призвести до повної втрати інформації, тому що при цьому змінюється кількість інформації в об'єкті – вилучаються непомітні компоненти сигналу і, тим самим, знищується секретна інформація, яка була там прихована. Під час активних атак, коли немає можливості витягти приховану інформацію або довести її існування, її можна знищити простим додаванням у стеганограму випадкових перешкод. У випадку цифрових зображень той, хто атакує, може застосувати відомі методи обробки зображень, у тому числі перетворити його в інший формат. Усе це здатне зруйнувати приховану інформацію.

У сучасних комп'ютерних системах реалізуються стеганографічні перетворення з високою надлишковістю, які стійкі до трансформації контейнера (обертання, обрізання країв зображень, друкування/сканування і т.д.) або маніпуляціям з його параметрами (яскравістю, контрастністю, різкістю та ін.). Тому одна з важливих вимог до практичної стегосистеми – це забезпечення стійкості до випадкових або навмисних помилок.

2.4.7 Стійкість стеганографічної системи до активних атак

Стеганографічна система називається стійкою до активних атак, якщо приховувана з її допомогою інформація не може бути змінена без значних змін контейнера, внаслідок яких він втратить свою функціональність.

Означення 2.6. (*стійкість*) Нехай Ξ – стеганографічна система і ρ – клас відображень $C \to C$. Тоді система Ξ буде ρ-стійкою, якщо у випадку стегосистем із секретним ключем для всіх $p \in \rho$ справедливо

$$D_k(p(E_k(c,m,k)),k)=D_k(E_k(c,m,k)),k)=m \qquad (2.15)$$

а у випадку безключових стегосистем, незалежно від вибору $m \in M$, $c \in C$ і $k \in K$:

$$D(p(E(c,m)))=D(E(c,m))=m. \quad (2.16)$$

Очевидно, що є зворотний взаємозв'язок між надійністю і стійкістю стегосистеми: чим більш стійкою до модифікацій контейнера буде стегосистема, тим вона менш надійна, оскільки стійкість може бути досягнута завадостійким кодуванням, що може сильно спотворити контейнер і, можливо, змінити розподіл імовірності P_s.

Багато стегосистем є стійкими до певного класу відображень (ущільнення/розширення JPEG, фільтрації, додавання з білим шумом та ін.). Ідеальна стегосистема повинна бути стійкою до всіх відображень типу «збереження α-подібності», тобто відображенням p: $C \to C$ із властивістю $sim(c,p(c)) > \alpha$ і $\alpha \approx 1$. Однак такі системи важкі в проектуванні і, у силу застосування завадостійкого кодування, мають низьку пропускну здатність.

З іншого боку, система називається «α-слабкою», якщо для кожного контейнера існує таке відображення «збереження α-подібності», що прихована інформація буде невідновлюваною з точки зору співвідношень (2.15)-(2.16).

У загальному випадку, існує два підходи до створення стійких стегосистем. У першому підході, у передбаченні можливих модифікацій стеганограм, стеганографічне перетворення відразу проектується стійким до знищення прихованих даних певним класом модифікацій. У другому підході реалізуються перетворення, які мають властивість оберненості до можливих модифікацій для відновлення початкового вигляду стеганограми. Наприклад, у [12] запропонований метод «афінного кодування» для протидії афінним перетворенням зображення, у якому передбачена оцінка параметрів перетворень, вимір змін форми, розмірів і напрямків деяких кодованих образів.

Стійкі алгоритми повинні приховувати дані в найбільш істотних фрагментах контейнера, тому що інформація, яка кодується в шумовому компоненті, може бути вилучена без надзусиль. Наприклад, відомо [13], що стеганографічні перетворення, які працюють у частотній області контейнера, можуть бути більш стійкими до модифікацій, ніж алгоритми, які працюють у тимчасовій області. Використовуючи ці властивості, можна створити стійкі стегосистеми, які будуть зберігати приховувану

інформацію в DCT-коефіцієнтах зображення. Емпіричні дослідження показали, що такі методи стійкі до JPEG-ущільнення до рівня ≈60%. Інші методи, головним чином використовувані в цифрових водяних знаках, витримують JPEG-ущільнення до рівня ≈5%.

2.4.8 Відкритий стеганографічний канал

Припустимо, що при активній атаці противникові вдається внести тільки незначні зміни в контейнер, що пересилається. Отже, збережеться деяка інформація, яка специфічна для конкретного контейнера. Цю інформацію не можна видалити без істотної зміни семантики контейнера. Тому, якщо секретне повідомлення вбудовувати в істотні фрагменти контейнера, то його можна передавати між абонентами з високим ступенем цілісності навіть при наявності активних перешкод. Подібний спосіб передавання повідомлення названий *відкритим стеганоканалом* (*supraliminal channel*) [10]. Згідно з цим способом «інформація вбудовується в контейнер так, що її видно, але неможливо змінити без істотних змін характерних властивостей контейнера». Концепція відкритого стеганоканалу використовується переважно для цифрових водяних знаків і протистоїть активним атакам. Розглянемо принцип його використання.

Припустимо, що кожному контейнерові відповідає деякий шаблон, у якому формально описані всі характерні особливості контейнера. Нехай S – множина всіх шаблонів і f: $S \to \{0,1\}^N$ – функція, яка називається функцією шаблонів. Для того, щоб передати бітовий рядок $x \in \{0,1\}^N$, Аліса вибирає елемент $s \in f^{-1}(x)$ і надсилає несекретним каналом контейнер, якому відповідає шаблон s. Віллі може підозрювати про існування прихованого обміну в шумовому компоненті контейнера і трохи змінити стеганограму з метою видалення з неї секретного повідомлення. Однак при цьому він не в змозі змінити шаблон контейнера. В свою чергу Боб може відновити шаблон s із прийнятої стеганограми і витягти x за допомогою функції f (рис. 2.6).

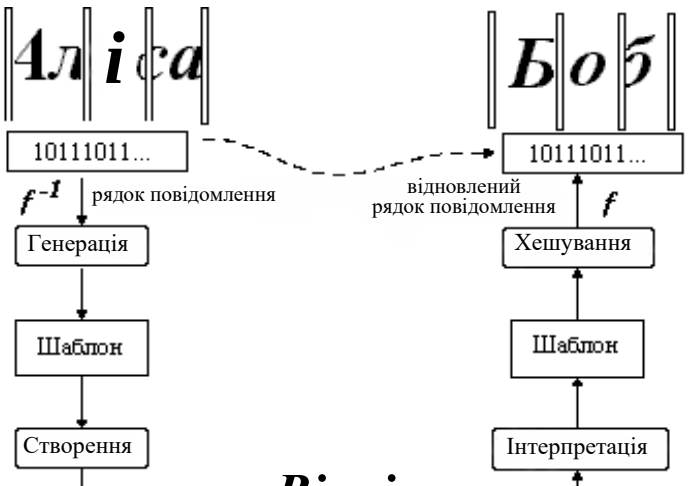


Рисунок 2.6 – Схема відкритого стеганографічного каналу

Використовувати відкритий стеганоканал для пересилання бітового рядка з явним змістом (наприклад: «Тут описаний план втечі з в'язниці. Аліса») недоцільно, оскільки Віллі за допомогою відкритої функції f зможе легко відновити вбудовану інформацію і застосувати репресії до Аліси і Боба. Однак, якщо кодоване повідомлення є випадковим секретним ключем або виглядає як випадковий шифртекст, то у Віллі не буде підстав для підозри і доказів (якщо він не здатний зламати криптосистему), що передана інформація є чимось більш істотним, ніж випадковий бітовий рядок.

Для практичної реалізації подібної схеми потрібно створити ряд умов. У першу чергу, необхідно вміти створювати для будь-якого шаблона контейнер, причому такий, що невеликі зміни, які можуть вноситися в цей контейнер при активних атаках, не повинні змінювати приховувані дані. В тому числі Віллі не повинен уміти шляхом маніпуляцій зі стеганограмою змінювати шаблон s, приводячи його до вигляду s' такого, що $f(s) \neq f(s')$. Необхідно також уміти будувати шаблон для кожного обраного контейнера. Крім того, функція f повинна бути загальнодоступною, а f і f^{-1} - обчислюваними. Контейнер, у якому відсутнє приховане повідомлення, повинен відображатися у випадковий рядок. Таким чином, єдине розходження між стеганограмою і порожнім контейнером полягає в тому, що рядок $f(s)$ має певне значення.

Описана схема може бути також застосована для прихованого обміну ключами. Аліса генерує відкритий ключ E і секретний ключ D, вибирає шаблон $s \in f^{-1}(E)$ і надсилає Бобу контейнер, що відповідає s. Боб відновлює E, обчислюючи за допомогою f шаблон. Він вибирає випадковий ключ k, шифрує його за допомогою E, вибирає контейнер, що відповідає шаблонові $s' \in f^{1}(E)$, і надсилає його Алісі, яка здатна відновити $E(k)$. Аліса розшифровує $E(k)$, використовуючи секретний ключ D. Внаслідок цього, Віллі ніяким чином не зможе отримати доказів, що подібна стеганограма є значимою для протоколу ключового обміну.

Слід зазначити, що головна проблема схеми відкритого стеганографічного каналу полягає в ефективній реалізації функції f.

2.5 Питання для самоконтролю знань

1. Назвіть рік і місце зародження комп'ютерної стеганографії.
2. Дайте означення стеганографічної системи.
3. Що таке контейнер?
4. В чому суть проблеми про «тюремника»?
5. Наведіть узагальнену схему стеганографічного зв'язку.
6. В чому полягає надійність стеганографічного зв'язку?
7. Дайте формальне представлення процесу приховування та витягання інформації.
8. Що може бути обраним як контейнер?
9. Дайте визначення функції подібності.
10. Які існують методи вибору контейнера?
11. Які вимоги висуваються до стеганографічних систем?
12. Дайте характеристику безключових стегосистем.
13. Дайте характеристику стегосистем з секретним ключем.
14. Дайте характеристику стегосистем з відкритим ключем.
15. Дайте характеристику змішаних стегосистем.
16. Яка основна мета стеганоаналізу?
17. Чим відрізняється стеганоаналіз від криптоаналізу?
18. Дайте визначення понять теоретичної, практичної та нестійкої стегосистем.
19. Назвіть етапи зламу стеганографічних систем.
20. Назвіть види атак на стегосистеми.
21. На яких принципах базується стеганографічне перетворення?

22. В чому полягає головна задача стеганоаналізу?

23. Назвіть складові успішного проведення стеганоаналізу.

24. Охарактеризуйте напрямки розвитку стеганоаналізу.

25. Наведіть модель оцінювання стійкості стегосистеми.

26. Наведіть метрики оцінювання перекручувань, що вносяться стеганографічними перетвореннями в зображення.

27. Яка стегосистема є абсолютно надійною?

28. Чи існує абсолютно надійна стегосистема?

29. Як визначається імовірність виявлення прихованих повідомлень в стегосистемі пасивним противником?

30. В чому полягають активні атаки противника?

31. Як визначається стійкість стегосистеми до активних атак?

32. Які існують підходи до створення стійких стегосистем?

33. Що таке відкритий стеганоканал?

34. Наведіть і поясніть схему відритого стеганоканалу.

РОЗДІЛ 3 СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

В даному розділі аналізуються стеганографічні методи приховування даних для різних типів інформаційного середовища. Під час розгляду методів будемо позначати буквою c контейнер, який являє собою послідовність елементів c_i довжини $l(c)$. Стосовно до цифрового звуку це буде кількість відліків в одиницю часу, до цифрового зображення – послідовність, отримана шляхом векторизації зображення (тобто шляхом вишикування всіх пікселів зліва направо від більшого до меншого). Для двійкового зображення значення c_i можуть бути «0» або «1», для квантованого зображення або звуку – змінюватись в діапазоні від «0» до «255», для текстів c_i – це символи алфавіту. Аналогічно, позначимо буквою s заповнений контейнер (стегооб'єкт) – послідовність елементів s_i довжини $l(s)$, а буквою m – секретне повідомлення довжини $l(m)$. Якщо не буде спеціально обумовлено, то будемо вважати, що $m_i \in \{0,1\}$. Кольорове зображення C будемо представляти через дискретну функцію, яка визначає вектор кольору $c(x,y)$ для кожного піксела зображення (x,y), де значення кольору задає трикомпонентний вектор у колірному просторі. Найбільш розповсюдженим способом передавання кольору є модель *RGB*, у якій основні кольори – червоний, зелений і синій, а будь-який інший колір може бути представлений у вигляді зваженої суми цих кольорів. Вектор кольору $c(x,y)$ у *RGB*-просторі представляє інтенсивність основних кольорів.

3.1 Класифікація методів приховування інформації

Більшість методів комп'ютерної стеганографії базується на двох принципах.

Перший полягає в тому, що файли, які не вимагають абсолютної точності (наприклад, файли з зображенням, звуковою інформацією та ін.), можуть бути до певного ступеня видозмінені без втрати функціональності.

Другий принцип ґрунтується на відсутності спеціального інструментарію або нездатності органів почуттів людини надійно розрізняти незначні зміни в таких вихідних файлах.

В основі базових підходів до реалізації методів комп'ютерної стеганографії в рамках того або іншого інформаційного середовища лежить виділення малозначимих фрагментів середовища і заміна існуючої

в них інформації на інформацію, яку передбачається захистити. Оскільки в комп'ютерній стеганографії розглядаються середовища, підтримувані засобами обчислювальної техніки і відповідних мереж, то все інформаційне середовище, в остаточному підсумку, може представлятися в цифровому вигляді. Таким чином, незначущі для кадру інформаційного середовища фрагменти відповідно до того або іншого алгоритму або методики заміняються (заміщуються) на фрагменти приховуваної інформації. Під кадром інформаційного середовища в даному випадку мається на увазі деяка його частина, виділена за певними ознаками. Такими ознаками часто бувають семантичні характеристики виділюваної частини інформаційного середовища. Наприклад, як кадр може бути обраний деякий окремий малюнок, звуковий файл, Web-сторінка та ін.

Для методів комп'ютерної стеганографії можна ввести певну класифікацію (рис. 3.1).

Рисунок 3.1 – Класифікація методів приховування інформації

Як уже вказувалося, *за способом добору контейнера* розрізняють сурогатні, селективні та конструювальні методи стеганографії.

В сурогатних (безальтернативних) методах стеганографії відсутня можливість вибору контейнера і для приховування повідомлення вибирається перший контейнер, що трапився, найчастіше не зовсім підходящий для повідомлення, що вбудовується. В цьому випадку біти контейнера замінюються бітами приховуваного повідомлення таким чином, щоб ця зміна не була помітною. Основним недоліком методу є те, що він дозволяє приховувати лише незначну кількість даних.

У селективних методах стеганографії передбачається, що приховане повідомлення повинно відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велике число альтернативних контейнерів, щоб потім вибрати найбільш підходящий з них для конкретного повідомлення. Окремим випадком такого підходу є обчислення деякої хеш-функції для кожного контейнера. При цьому для приховання повідомлення вибирається той контейнер, хеш-функція якого збігається зі значенням хеш-функції повідомлення (тобто стеганограмою є обраний контейнер).

У конструювальних методах стеганографії контейнер генерується самою стегосистемою. Тут може бути кілька варіантів реалізації. Так, наприклад, шум контейнера може моделюватися приховуваним повідомленням. Це реалізується за допомогою процедур, які не тільки кодують приховуване повідомлення під шум, але й зберігають модель початкового шуму. У граничному випадку за моделлю шуму може будуватися ціле повідомлення. Прикладом може служити метод, який реалізований у програмі MandelSteg, де як контейнер для вбудовування повідомлення генерується фрактал Мандельброта, або ж апарат функцій імітації (*mumic function*).

За способом доступу до приховуваної інформації розрізняють методи для потокових (безперервних) контейнерів і методи для контейнерів випадкового доступу (обмеженої довжини).

Методи, що використовують потокові контейнери, працюють з потоками неперервних даних (наприклад, інтернет-телефонія). У цьому випадку приховувані біти необхідно в режимі реального часу включати до інформаційного потоку. Про потоковий контейнер не можна попередньо сказати, коли він почнеться, коли закінчиться і наскільки тривалим він буде. Більш того, об’єктивно немає можливості довідатися заздалегідь, якими будуть наступні шумові біти. Існує цілий ряд труднощів, які необхідно подолати кореспондентам при використанні потокових

контейнерів. Найбільшу проблему при цьому складає синхронізація початку приховуваного повідомлення.

Методи, які використовуються для контейнерів випадкового доступу, призначені для роботи з файлами фіксованої довжини (текстова інформація, програми, графічні або звукові файли). У цьому випадку заздалегідь відомі розміри файлу і його вміст. Приховувані біти можуть бути рівномірно вибрані за допомогою підходящої псевдовипадкової функції. Недолік таких контейнерів полягає в тому, вони мають набагато менші розміри, ніж потокові, а також те, що відстані між приховуваними бітами рівномірно розподілені між найбільш короткою і найбільш довгою заданими відстанями, у той час як справжній шум буде мати експонентний розподіл довжин інтервалу. Перевага подібних контейнерів полягає в тому, що вони можуть бути заздалегідь оцінені з точки зору ефективності вибраного стеганографічного перетворення.

За типом організації контейнери, подібно завадозахищеним кодам, можуть бути систематичними і несистематичними. У систематично організованих контейнерах можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти самого контейнера, а де шумові біти, призначені для приховуваної інформації (як, наприклад, у широко розповсюдженому методі найменшого значущого біта). При несистематичній організації контейнера такого поділу зробити не можна. В цьому випадку для виділення прихованої інформації необхідно обробляти вміст усієї стеганограми.

За використовуваними принципами стеганометоди можна розбити на два класи: цифрові методи і структурні методи. Якщо цифрові методи стеганографії, використовуючи надлишковість інформаційного середовища, в основному, маніпулюють з цифровим представленням елементів середовища, куди впроваджуються приховувані дані (наприклад, у пікселі, в різні коефіцієнти косинус-косинусних перетворень, перетворень Фур'є, Уолша-Радемахера або Лапласа), то структурні методи стеганографії для приховування даних використовують семантично значимі структурні елементи інформаційного середовища.

Основним напрямком комп'ютерної стеганографії є використання властивостей надлишковості інформаційного середовища. Варто врахувати, що при приховуванні інформації відбувається перекручування деяких статистичних властивостей середовища або порушення його

структури, які необхідно враховувати для зменшення демаскувальних ознак.

В особливу групу можна також виділити методи, що використовують спеціальні властивості форматів представлення файлів:

– зарезервовані для розширення поля комп'ютерних форматів файлів, які зазвичай заповнюються нулями і не враховуються програмою;

– спеціальне форматування даних (зсування слів, речень, абзаців або вибирання визначених позицій букв);

– використання незадіяних місць на магнітних носіях;

– видалення ідентифікувальних заголовків для файлу.

В основному, для таких методів характерні низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

За призначенням розрізняють стеганографічні методи власне для прихованого передавання або прихованого збереження даних і методи для приховування даних у цифрових об'єктах з метою захисту самих цифрових об'єктів. Останні методи відносяться до галузі цифрових водяних знаків і будуть розглянуті в розділі 5.

За типами інформаційного середовища виділяються стеганографічні методи для текстового середовища, для аудіо середовища, а також для зображень (стоп-кадрів) і відео середовища.

Нижче більш докладно будуть розглянуті відомі стеганографічні методи для різних типів інформаційного середовища.

3.2 Текстові стеганографи

Сучасні стеганографічні засоби зазвичай працюють в інформаційних середовищах, що мають велику надлишковість. На відміну від інформації, яка містить багато шумових даних (наприклад, звук і зображення), письмовий текст містить малу кількість надлишкової інформації, яку можна використовувати для приховування даних.

Методи *лінгвістичної стеганографії* – приховування секретних повідомлень у тексті – відомі ще із середньовіччя. В основному такі методи використовують або природну надлишковість мови, або формати представлення тексту. З розвитком комп'ютерних технологій середньовічні методи лінгвістичної стеганографії відродилися на якісно новому рівні і дозволяють у деяких випадках приховати факт таємного

листування не тільки від «автоматичного цензора», який здійснює моніторинг мереж телекомунікацій, але й від людини.

Можна виділити такі методи, які зустрічаються в сучасних лінгвістичних стеганографах:

– методи перекручування формату текстового документа;

– синтаксичні методи;

– семантичні методи;

– методи генерації стеганограм за допомогою приховуваного повідомлення.

3.2.1 Методи перекручування формату текстового документа

Приховування даних шляхом зміни формату текстових файлів зазвичай проводиться так, щоб стандартні текстові редактори не змогли виявити ознак присутності додаткової інформації. Методи, що розглядаються нижче, маніпулюють інтервалами між словами і реченнями або ж пропусками наприкінці текстових рядків. Використання пропусків для приховування даних обумовлено такими причинами. По-перше, введення додаткових пропусків не вносить великих змін у значення фрази або речення. По-друге, у випадкового читача навряд чи відразу виникне підозра щодо вставлених додаткових пропусків.

Приховування таємного повідомлення (у бітовому представленні) можна проводити шляхом додавання одного або двох символів пропуску наприкінці речень після символу кінця (наприклад, крапки - для натуральної мови або крапки з комою - для коду програми мовою С): один додатковий пропуск кодує значення біта «0», а два – «1». Цей простий метод має недоліки. По-перше, він неефективний, тому що необхідно мати контейнер великого об’єму (швидкість передавання прихованих даних у даному випадку приблизно дорівнює одному бітові на 160 байтів тексту). По-друге, можливість приховування залежить від структури тексту (деякі тексти, типу «білі вірші», не мають чітких знаків кінця). По-третє, текстові редактори часто автоматично додають символи пропуску після крапки.

Кодувати секретні дані можна додатковими пропусками наприкінці кожного рядка тексту (рис. 3.2): два біти кодуються одним пропуском, чотири – двома, вісім – трьома і т.д. Перевага такого методу кодування полягає в тому, що воно може бути виконано з будь-яким текстом; зміни в форматі різко не впадають в око читачеві, забезпечується передавання більшої кількості прихованих даних у порівнянні з попереднім методом (1

біт на 80 байтів). Недолік методу полягає в тому, що деякі програми (наприклад, SendMail) можуть необережно видаляти додаткові пропуски. Крім цього, приховані в такий спосіб дані не завжди можуть бути відновлені з друкованої копії документа.

Рисунок 3.2 – Приклад приховування даних пропусками наприкінці текстових рядків

Ще один метод приховування даних за допомогою пропусків маніпулює з текстами, які вирівняні з обох боків. У цьому методі дані кодуються шляхом керованого вибору місць для розміщення додаткових символів пропуску. Один символ між словами інтерпретується як «0», а два – як «1». Метод дозволяє вбудовувати декілька бітів прихованої інформації в кожен рядок тексту (рис. 3.3).

У_людини__набагато__більше_ворогів_таємних,_ніж_явних.__Приховану_ворожість__найчастіше_породжує_заздрість.__Заздрість_викликають__розум,__краса,_багатство_і_здоров’я.__Ви_будете__мати__мало_ворогів_і__знати__їх__в__обличчя,__якщо_позбавлені__всіх__цих_достоїнств.

Рисунок 3.3 – Приклад приховування бітового повідомлення «0110»≡«100011010110»

У зв’язку з процедурою вирівнювання тексту з обох боків не кожен проміжок між словами може використовуватися для кодування прихованих даних. Для того, щоб визначити в якому з проміжків між словами прихована інформація, а які проміжки є частиною оригінального тексту, використовується такий метод декодування. Бітовий рядок, який витягається зі стеганограми, розбивається на пари. Пари бітів «01»

інтерпретується як «1»; пари «10» – як «0»; а біти «00» і «11» є порожніми, тобто такими, котрі не несуть ніякої інформації. Наприклад, бітове повідомлення «1000101101» скорочується до «001», а рядок «110011» – буде порожнім.

Розглянуті методи працюють успішно доти, поки тексти представлені в коді ASCII. Існують також стеганографічні методи, які інтерпретують текст як двійкове зображення. В даних методах приховувана інформація кодується зміною відстані між послідовними рядками тексту або словами. Приховування даних відбувається шляхом вибору місця розташування рядків у документі, які зсуваються вгору або вниз відповідно до бітів приховуваних даних. При цьому деякі рядки залишають для синхронізації на місці (наприклад, кожен другий). В цьому випадку один секретний біт повідомлення кодується зсувом одного рядка. Якщо рядок зсунутий, то значення секретного біта дорівнює «1», інакше – «0».

Витягання прихованого повідомлення проводиться шляхом аналізу відстаней між центрами рядків, які розташовані поруч. Позначимо через Δ_{R+} – відстань між центрами зсунутого рядка та попереднього незміненого рядка (синхрорядок), Δ_{R-} – відстань між центрами зсунутої лінії і наступного синхрорядка, а через Δ_{X+} і Δ_{X-} – відповідні відстані у вихідному документі. Тоді, якщо відстань між рядками була збільшена, то:

$$\frac{\Delta_{R+} + \Delta_{R-}}{\Delta_{R+} - \Delta_{R-}} > \frac{\Delta_{X+} + \Delta_{X-}}{\Delta_{X+} - \Delta_{X-}}.$$

Аналогічно, якщо відстань була зменшена, то:

$$\frac{\Delta_{R+} + \Delta_{R-}}{\Delta_{R+} - \Delta_{R-}} < \frac{\Delta_{X+} + \Delta_{X-}}{\Delta_{X+} - \Delta_{X-}}.$$

Відзначимо, що даний метод нечутливий до зміни масштабу документа, що забезпечує йому гарну стійкість до більшості перекручувань, які можуть мати місце під час активних атак.

Інша можлива схема приховування шляхом зсуву слів відформатованого тексту показана на рис. 3.4. В ній, у відповідності з приховуваними даними, змінюється горизонтальна позиція початку слів. Теоретично, можна використовувати зміни кожного проміжку між словами. Для того, щоб забезпечити зберігання початкового вирівнювання тексту необхідно дотримуватись єдиного обмеження: сума всіх зрушень в одному рядку повинна дорівнювати нулю.

Приклад приховування| даних| у тексті

Приклад приховування| даних| у тексті

Приклад приховування| даних| у тексті

Рисунок 3.4 – Приклад приховування даних у проміжках між словами (для наочності вказані вертикальні лінії)

Існують більш тонкі методи приховування інформації в текстовому середовищі. У деяких текстових редакторах реалізовані опції, які проводять автоматичне форматування тексту відповідно до визначених критеріїв. Наприклад, редактор T_EX використовує складний алгоритм обчислення кінця рядка або сторінки. Фактично обчислюються деякі спеціальні параметри, за якими визначається місце переходу з одного рядка або сторінки на іншу. Один з таких параметрів оцінює кількість пропусків, які необхідно вставити, щоб зберегти заданий стиль документа; інший – оцінює естетичний вигляд документа під час вибору переносу і т.д. У результаті T_EX намагається вибрати послідовність місць переносів таким чином, щоб сума всіх параметрів, які відносяться до параграфа, що його редагують, була мінімальною. Змінюючи деякі значення параметрів, можна керувати вибором місць переносів і використовувати їх для приховування даних.

Дотепер питання про створення безпечної лінгвістичної стегосистеми залишається відкритим. Будь-яка обробка тексту редактором, його друк або переклад в інший формат (HTML, Postscript, PDF або RTF) може змінити розташування пропусків і знищити прихований текст. Низька стійкість подібних методів до можливих модифікацій документа є однією з причин пошуку інших методів пошуку даних у тексті.

Синтаксичні і семантичні методи докорінно відрізняються від розглянутих вище, але можуть використовуватися одночасно з ними.

3.2.2 Синтаксичні методи

До синтаксичних методів лінгвістичної стеганографії відносяться методи зміни пунктуації і методи зміни стилю і структури тексту.

В будь-якій мові існують випадки, коли правила пунктуації є неоднозначними і мають слабкий вплив на зміст тексту. Наприклад, обидві

форми перерахування «хліб, олія і молоко» і «хліб, олія, молоко» є припустимими. Можна використовувати той факт, що вибір таких форм є довільним і використовувати альтернативний вибір для кодування даних у двійковому вигляді. Наприклад, якщо з'являється форма перерахування із сполучником «і», то кодується «1», інакше – «0». Для приховування можна також застосовувати скорочення й абревіатури.

У будь-якій мові мається багато можливостей для синтаксичного приховування даних, але вони не часто зустрічаються в типових текстах. Середня швидкість передавання даних такими методами дорівнює декільком бітам на кілобайт тексту.

Хоча більшість правил пунктуації є неоднозначними і надлишковими, їхнє суперечливе використання може стати об'єктом уваги для цензора. Крім того, існують випадки, коли зміна пунктуації може сильно змінити зміст тексту. Тому такий підхід повинен використовуватися з обережністю.

До синтаксичних методів відносяться методи зміни стилю або структури тексту без істотної зміни його значення або тону. Наприклад, пропозиція «До закінчення ночі я буду готовим» можна представити у виді «Я буду готовий швидше, ніж ніч закінчиться». Такий підхід більш прозорий, але можливість його обмежена.

3.2.3 Семантичні методи

Семантичні методи стеганографії аналогічні синтаксичним. Для цих методів елементарними лінгвістичними компонентами вважаються окремі слова, тому приховування даних реалізується шляхом безпосередньої заміни слів. Для такої заміни необхідні таблиці синонімів. Кодування секретного повідомлення проводиться вибором синоніма з необхідного місця таблиці. Наприклад, першому слову–синонімові відповідає «1», а другому – «0» (рис. 3.5). Якщо слову відповідає велика кількість синонімів, то можна кодувати більшу кількість бітів одночасно.

«1»	«0»
слід	відбиток
діра	отвір
оборона	захист
овація	оплески

Рисунок 3.5 – Таблиця синонімів

На рис. 3.6 наведений приклад іншого підходу до приховування даних, у якому секретне повідомлення керує перефразовуванням тексту контейнера. У результаті виходить стеганограма, яка має той же самий зміст, що і текст контейнера.

Рисунок 3.6 – Приклад роботи семантичної стегосистеми SubiText

3.2.4 Методи генерації стеганограм

На відміну від розглянутих вище стеганометодів, де приховувана інформація впроваджується в текстовий контейнер, існують методи, які цілком породжують стеганограму на основі захищуваних даних. В таких методах секретна інформація не вбудовується в текст, а подається повністю всією стеганограмою. Теоретичну основу для методів генерації стеганограм розробив П. Вайнер у теорії функцій імітації [14]. В стеганографії функції імітації застосовуються для того, щоб приховати ідентичність повідомлення шляхом зміни його статистичних властивостей.

Нехай мається файл A, який складається із символьних рядків. Позначимо через $p(t,a,A)$ – імовірність того, що символ a знаходиться в рядку t файлу A, а через $p(\cdot,a,A)$ і $p(t,\cdot,A)$ – відповідно, незалежні імовірності того, що символ a або рядок t існують у A. Два файли A і B будемо вважати статистично еквівалентними в межах ε, якщо $|p(t,\cdot,A)-p(t,\cdot,B)|<\varepsilon$ для всіх рядків t, довжина яких менша, ніж n.

Означення 3.1. Функцією імітації *n-го* порядку будемо називати таку функцію f, яка у ε-околі виконує статистично еквівалентне перетворення файлу A в файл B.

Таким чином, якщо $p(t,A)$ – імовірність появи деякого рядка t у файлі A, то функція f перетворить файл A в файл B так, що для всіх рядків t довжини менше n виконується співвідношення $|p(t,f(A))-p(t,B)|<\varepsilon$.

У [15] запропоновано декілька типів функції імітації, які, в залежності від складності, моделюються регулярною, контекстно-вільною або рекурсивно-рахунковою граматиками. Стеганографічні перетворення першого типу описуються в термінах процедур ущільнення інформації; другого – контекстно-вільними граматиками, в яких приховувані біти керують несуперечливими продукціями; для опису функцій третього типу застосовується апарат машин Тьюрінга.

Регулярні функції імітації можна змоделювати за допомогою схеми кодування за Хафманом. Відомо, що будь-яка мова має деякі статистичні властивості. Цей факт використовується багатьма методами ущільнення даних. Якщо на алфавіті Σ заданий розподіл імовірностей A, то можна скористатися схемою кодування за Хафманом для створення функції ущільнення з мінімальною надлишковістю $f_A:\Sigma\rightarrow\{0,1\}^*$, де символ «*» використовується як $\Sigma^*=\cup_{i\geq 0}\{x_1...x_i|x_1,...,x_i\in\Sigma\}$. Таку функцію можна побудувати на основі функції ущільнення Хафмана: $G(x)=f_B^{-1}(f_A(x))$.

Таким чином, секретний файл можна ущільнити за схемою Хафмана з розподілом A, в результаті чого вийде файл двійкових рядків, які можуть інтерпретуватися як результат операції ущільнення деякого файлу з розподілом B. Цей файл може бути відновлений із застосуванням інверсної функції ущільнення f_B^{-1} до файлу двійкових рядків і використовуватися надалі як стеганограма. Якщо функції f_A і f_B^{-1} є взаємно однозначними, то і створена функція імітації буде також взаємно однозначна. Доведено, що побудована в такий спосіб функція подібності оптимальна в тому розумінні, що якщо функція ущільнення Хафмана f_A є теоретично оптимальною і файл x складається з випадкових бітів, то взаємно однозначна функція $f_A^{-1}(x)$ має найкращу статистичну еквівалентність до A.

Регулярні функції імітації створюють стеганограми, які мають заданий статистичний розподіл символів, однак при цьому ігнорується семантика отриманого тексту. Для людини такі тексти виглядають повною нісенітницею з граматичними помилками. Для генерування більш осмислених текстів використовуються контекстно-вільні граматики (КВГ).

Контекстно-вільна граматика визначається впорядкованою четвіркою $<V,\Sigma\subseteq V,\Pi,S\subset V\setminus\Sigma>$, де V і Σ – відповідно, множини змінних і термінальних

символів, Π – набір продукцій (правил виведення), а S – початковий символ. Продукції подібні правилам підстановки, вони перетворять змінну в рядок, що складається з термінальних або змінних символів. Якщо за допомогою правил виведення зі стартового символу можна отримати послідовність термінальних символів, то говорять, що послідовність отримана граматикою. Такі граматики називаються контекстно-вільними, тому що будь-який символ можна замінити послідовністю символів, не звертаючи уваги на контекст, у якому він зустрівся. Якщо для кожного рядка s існує тільки один шлях, яким s може бути породжена з початкового символу, то така граматика називається однозначною.

Однозначні граматики можуть використовуватися як апарат для стеганографічних перетворень. Розглянемо граматику $<\{S,A,B,C\},\{A,\ldots,Z,a,\ldots,z\},\Pi,S>$, де для кожної можливої продукції приписана деяка імовірність: $\Pi=\{S\rightarrow_{0.5}$ Alise B, $S\rightarrow_{0.3}$ Bob B, $S\rightarrow_{0.1}$ Eve B, $S\rightarrow_{0.1}$ I A; $A\rightarrow_{0.3}$ am working, $A\rightarrow_{0.4}$ am lazy, $A\rightarrow_{0.4}$ am tired; $B\rightarrow_{0.5}$ is З, $B\rightarrow_{0.5}$ can cook; $C\rightarrow_{0.5}$ reading, $C\rightarrow_{0.1}$ sleeping, $C\rightarrow_{0.4}$ working$\}$.

Нехай $\Pi_{Vi}=\{\pi_{i,1},\ldots,\pi_{i,n}\}$ – набір усіх продукцій, що зв'язані зі змінною V_i. Тоді для кожного набору Π_i можна створити функцію ущільнення Хафмана $f_{\Pi i}$. На рис. 3.7 показані можливі дерева для Π_S і Π_A, з яких може бути легко отримана функція ущільнення Хафмана. Наприклад, продукція «Eve B» буде кодуватися як 110, «I am tired» – як 11 і т.д.

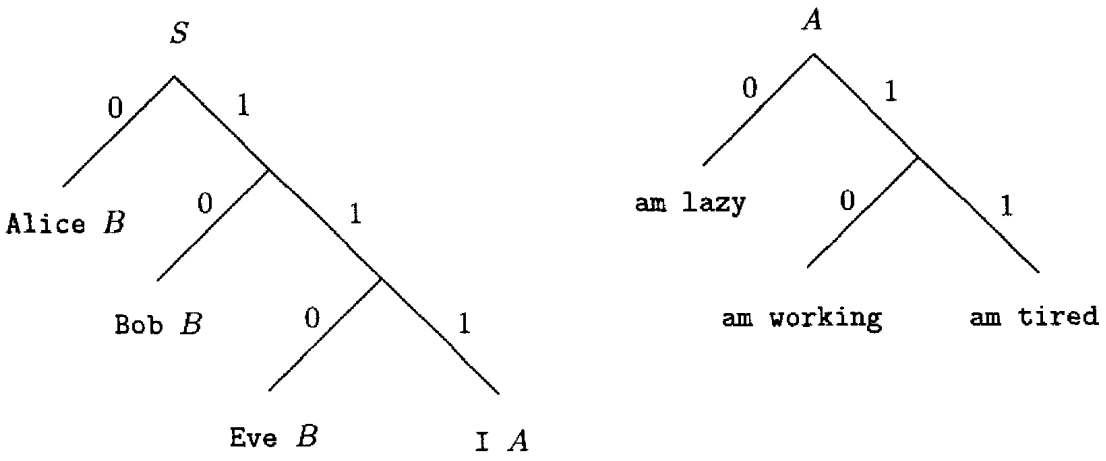


Рисунок 3.7 – Функція ущільнення Хафмана для Π_S і Π_A.

Для стеганографічних задач використовується інверсна функція Хафмана. На етапі приховування даних відправник отримує за допомогою

КВГ деякий рядок, який вважається стеганограмою. Стартуючи з початкового символу S, найлівіша змінна V_i замінюється за відповідною продукцією. Ця продукція визначається згідно з секретним повідомленням і функцією ущільнення Хафмана для Π_{Vi} таким чином. Відповідно до чергового біта секретного повідомлення відбувається перегляд дерева Хафмана доти, поки не буде досягнутий лист у дереві, після чого початковий символ замінюється на значення, яке приписано даному листові. Цей процес повторюється для всіх бітів повідомлення. Остаточний рядок складається тільки з термінальних символів.

Розглянемо приклад. Нехай секретне повідомлення буде «11110». Тоді для вказаної вище граматики Π на першому кроці перегляд дерева Π_S за допомогою трьох перших бітів повідомлення досягне листа «I». Таким чином, початковий символ S буде замінений на «I A». Потім, переглядаючи ще раз дерево, за допомогою наступних двох секретних бітів повідомлення відбудеться заміна чергових символів на «am working». У результаті кінцевий рядок буде складатися тільки з термінальних символів. У підсумку стеганограмі «11110» відповідає повідомлення «I am working».

Для витягання прихованої інформації необхідно провести аналіз стеганограми з використанням дерева розбору КВГ. Оскільки граматика і продукції однозначні, то витягання прихованого повідомлення може бути виконано.

Практичний досвід показав, що використання сучасних методів лінгвістичної стеганографії дозволяє створювати стеганограми, які важко знайти при автоматизованому моніторингу мереж телекомунікації, але обдурити з їх допомогою людину-цензора все-таки дуже складно. У зв’язку з цим найбільший розвиток одержали стеганографічні методи захисту для інших інформаційних середовищ.

3.3 Приховування даних у растрових зображеннях і відео

Розвиток мультимедійних засобів супроводжується великим потоком графічної інформації в обчислювальних мережах. Під час реалізації зображення, як правило, використовуються значні об’єми елементарних компонентів, що становить особливий інтерес для стеганографічних методів захисту. Візуальне середовище (цифрові зображення і відео) має велику надлишковість різної природи:

– кодова надлишковість, що виникає при неоптимальному описі зображення;

– міжпікселна надлишковість, яка обумовлена наявністю сильної кореляційної залежності між пікселами реального зображення;

– психовізуальна залежність, яка виникає через те, що орган зору людини не адаптований для точного сприйняття зображення піксел за пікселем і сприймає кожну ділянку з різною чутливістю.

Інформаційним відеопотокам, які складаються з послідовності окремих кадрів зображення, окрім вказаних вище, властива також надлишковість, обумовлена інформаційною, технічною, тимчасовою і функціональною (смисловою) залежністю між кадрами.

Останнім часом створена достатня кількість методів приховування інформації в цифрових зображеннях і відео, що дозволило провести їхню систематизацію і виділити такі групи:

– методи заміни в часовій (просторовій) області;

– методи приховування в частотній області зображення;

– широкосмугові методи;

– статистичні методи;

– методи перекручування;

– структурні методи.

Розглянемо деякі особливості, які характерні для кожної з виділених груп стеганометодів.

3.3.1 Методи заміни

Загальний принцип даних методів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення. Для витягання повідомлення необхідно знати місце, де була розміщена приховувана інформація.

Найбільш розповсюдженим методом цього класу є *метод заміни найменшого значущого біта* (НЗБ) [12].

Популярність НЗБ-методу обумовлена його простотою і тим, що він дозволяє приховувати у відносно невеликих файлах досить великі об’єми інформації. Даний метод зазвичай працює з растровими зображеннями, які представлені у форматі без ущільнення (наприклад, GIF і BMP). Основним його недоліком є сильна чутливість до найменших перекручувань

контейнера. Для послаблення цієї чутливості часто застосовують завадостійке кодування.

Суть методу НЗБ полягає в заміні найменш значущих бітів пікселів зображення бітами секретного повідомлення. У найпростішому випадку проводиться заміна НЗБ усіх послідовно розташованих пікселів зображення. Однак, оскільки довжина секретного повідомлення зазвичай менше кількості пікселів зображення, то після його вбудовування в контейнері будуть присутні дві області з різними статистичними властивостями (область, в якій незначні біти були змінені, і область, в якій вони не змінювалися). Це може бути легко виявлено за допомогою статистичних тестів. Для створення еквівалентної зміни ймовірності всього контейнера секретне повідомлення зазвичай доповнюють випадковими бітами так, щоб його довжина в бітах дорівнювала кількості пікселів у вихідному зображенні.

Інший підхід, *метод випадкового інтервалу* [16], полягає у випадковому розподілі бітів секретного повідомлення по контейнеру, у результаті чого відстань між двома вбудованими бітами визначається псевдовипадково. Ця методика найбільш ефективна при використанні потокових контейнерів (відео).

Для контейнерів довільного доступу (зображень) може використовуватися *метод псевдовипадкової перестановки* [17].

Його суть полягає в тому, що генератор псевдовипадкових чисел створює послідовність індексів j_1, ..., $j_{l(m)}$ і зберігає *k-й* біт повідомлення в пікселі з індексом j_k. Однак у цьому випадку один індекс може з'явитися в послідовності більше одного разу, тобто може відбутися «перетинання» – перекручування вже вбудованого біта. Якщо число бітів повідомлення набагато менше розміру зображення, то імовірність перетинання незначна, і ушкоджені біти можуть бути відновлені за допомогою коригувальних кодів. Імовірність, принаймні, одного перетинання оцінюється як

$$p \approx 1 - \exp(-\frac{l(m)[l(m)-1]}{2l(c)}), \text{ за умови, що } l(m) << l(c).$$

При збільшенні $l(m)$ і $l(c)=const$ дана імовірність прямує до одиниці. Для запобігання перетинань необхідно запам'ятовувати всі індекси використаних елементів j_i і перед приховуванням нового піксела проводити перевірку його на повторюваність.

Ще один підхід до реалізації методу заміни (*метод блокового приховування*) полягає в наступному. Вихідне зображення-контейнер розбивається на $l(m)$ неперетинних блоків, I_i $(1 \le i \le l(m))$ довільної конфігурації і для кожного з них обчислюється біт парності $p(I_i)$:

$$p(I) = \sum_{j \in I} НЗБ(c_j) \bmod 2 .$$

У кожному блоці проводиться приховування одного секретного біта m_i. Якщо біт парності $p(I_i)$ блоку I_i не збігається із секретним бітом m_i, то відбувається інвертування одного з НЗБ блоку I_i, у результаті чого $p(I_i)=m_i$. Вибір блоку може здійснюватись випадково з використанням стегоключа. Хоча цей метод має таку ж стійкість до перекручувань, як і всі попередні, він має ряд переваг. По-перше, мається можливість змінювати значення такого піксела в блоці, для якого статистика контейнера зміниться мінімально. Крім того, вплив наслідків вбудовування секретних даних у контейнер можна зменшити за рахунок збільшення розміру блоку.

Методи заміни палітри. Для приховування даних можна також скористатися палітрою кольорів, які присутні у форматі зображення.

Палітра з N кольорів визначається як список пар індексів (i,c_i), який визначає відповідність між індексом i і його вектором колірності c_i. У зображенні кожному пікселу привласнюється індекс у палітрі. Оскільки кольори в палітрі не завжди впорядковані, то приховувану інформацію можна кодувати послідовністю збереження кольорів у палітрі. Існує $N!$ різних способів перестановки *N-колірності* палітри, що цілком достатньо для приховування невеликого повідомлення. Однак методи приховування, в основі яких лежить порядок формування палітри, також нестійкі: будь-яка атака, пов’язана зі змінами палітри, знищує секретне повідомлення.

Найчастіше сусідні кольори в палітрі не обов’язково є схожими, тому деякі стеганометоди перед приховуванням даних проводять упорядкування палітри так, що суміжні кольори стають подібними. Наприклад, значення кольору може бути упорядковане за відстанню d у *RGB*-просторі, де $d = \sqrt{R^2 + G^2 + B^2}$. Оскільки орган зору людини більш чутливий до змін яскравості кольору, то набагато краще сортувати вміст палітри за значеннями яскравості сигналу. Після сортування палітри можна змінювати НЗБ індексів кольору без особливого перекручування зображення.

Деякі стеганометоди [18] передбачають зменшення загальної кількості значень кольорів (до $N/2$) шляхом «розмивання» зображення. При цьому елементи палітри дублюються так, щоб значення кольорів для них розрізнялися незначно. У підсумку кожне значення кольору розмитого зображення відповідає двом елементам палітри, які вибираються відповідно до біта секретного повідомлення.

До методів заміни можна також віднести *метод квантування зображень* [19]. Даний метод оснований на міжпікселній залежності, яку можна описати деякою функцією Q. У найпростішому випадку можна розрахувати різницю e_i між суміжними пікселами x_i та x_{i+1} і задати її як параметр функції Q: $\Delta_i=Q(x_i-x_{i-1})$, де Δ_i – дискретна апроксимація різниці сигналів x_i-x_{i-1}. Оскільки Δ_i є цілим числом, а реальна різниця x_i-x_{i-1} дійсним, то з'являється помилка квантування $\delta_i=\Delta_i-e_i$. Для сильно корельованих сигналів ця помилка близька до нуля: $\delta_i\approx0$. У даному методі приховування інформації проводиться шляхом коректування різницевого сигналу Δ_i. Стегоключ являє собою таблицю, яка кожному можливому значенню Δ_i ставить у відповідність визначений біт, наприклад:

Δ_i	-4	-3	-2	-1	0	1	2	3	4
	0	1	0	1	1	1	0	0	1

Для приховування *і-го* біта повідомлення обчислюється Δ_i. Якщо Δ_i не відповідає секретному бітові, який необхідно приховати, то його значення Δ_i замінюється найближчим Δ_j, для якого ця умова виконується. Витягання секретного повідомлення проводиться відповідно до різниці між Δ_i і стегоключем.

3.3.2 Методи приховування в частотній області зображення

Як уже відзначалося, стеганографічні методи заміни нестійкі до будь-яких перекручувань, а застосування операції ущільнення з втратами призводить до повного знищення всієї секретної інформації, прихованої НЗБ-методом у зображенні. Більш стійкими до різних перекручувань, у тому числі ущільнення, є методи, які використовують для приховування даних не тимчасову область, а частотну.

Існує декілька способів представлення зображення в частотній області. Наприклад, з використанням дискретного косинусного перетворення (ДКП), швидкого перетворення Фур'є або вейвлет-перетворення. Дані перетворення можуть застосовуватися як до всього зображення, так і до

деяких його частин. Під час цифрової обробки зображення часто використовується двовимірна версія дискретного косинусного перетворення:

$$S(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} s(x,y) \cos\left(\frac{\pi u(2x+1)}{2N} \right) \cos\left(\frac{\pi u(2y+1)}{2N} \right),$$

$$S(x,y) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(u)C(v)S(u,v) \cos\left(\frac{\pi u(2x+1)}{2N} \right) \cos\left(\frac{\pi u(2y+1)}{2N} \right),$$

де $C(u)=1/\sqrt{2}$, якщо $u=0$, і $C(u)=1$ в іншому випадку.

Один з найбільш популярних методів приховування секретної інформації в частотній області зображення оснований на відносній зміні величин коефіцієнтів ДКП [20]. Для цього зображення розбивається на блоки розміром 8×8 пікселів. Кожен блок призначений для приховування одного біта секретного повідомлення. Процес приховування починається з випадкового вибору блоку b_i, призначеного для кодування *i-го* біта повідомлення. Для обраного блоку зображення b_i проводиться ДКП: $B_i=D\{b_i\}$. Під час організації секретного каналу абоненти повинні попередньо домовитися про конкретні два коефіцієнти ДКП, які будуть використовуватися для приховування секретних даних. Позначимо їх як (u_1,v_1) і (u_2,v_2). Ці два коефіцієнти повинні відповідати косинус-функціям із середніми частотами, що забезпечить схоронність інформації в істотних областях сигналу, яка не буде знищуватися при JPEG-ущільненні. Оскільки коефіцієнти ДКП середніх є подібними, то процес приховування не внесе помітних змін у зображення.

Якщо для блоку виконується умова $B_i(u_1,v_1)>B_i(u_2,v_2)$, то вважається, що блок кодує значення «1», в іншому випадку – «0». На етапі вбудовування інформації вибрані коефіцієнти змінюють між собою значення, якщо їхній відносний розмір не відповідає кодованому бітові. На кроці квантування JPEG-ущільнення може впливати на відносні розміри коефіцієнтів, тому, додаючи випадкові значення до обох величин, алгоритм гарантує, що $|B_i(u_1,v_1)-B_i(u_2,v_2)|>x$, де $x>0$. Чим більше x, тим алгоритм буде більш стійким до ущільнення, але при цьому якість зображення погіршується. Після відповідного корегування коефіцієнтів виконується обернене ДКП.

Витягання прихованої інформації проводиться шляхом порівняння вибраних двох коефіцієнтів для кожного блоку.

3.3.3 Широкосмугові методи

Широкосмугові методи передавання застосовуються в техніці зв'язку для забезпечення високої завадостійкості й ускладнення процесу перехоплення. Суть широкосмугових методів полягає в значному розширенні смуги частот сигналу, більш ніж це необхідно для передавання реальної інформації. Розширення діапазону виконується в основному за допомогою коду, який не залежить від даних, що передаються. Корисна інформація розподіляється по всьому діапазону, тому при втраті сигналу в деяких смугах частот в інших смугах присутньо досить інформації для її відновлення.

Таким чином, застосування широкосмугових методів у стеганографії ускладнює виявлення прихованих даних та їхнє видалення. Мета широкосмугових методів подібна задачам, які вирішує стегосистема: спробувати «розчинити» секретне повідомлення в контейнері й унеможливити його виявлення. Оскільки сигнали, розподілені по всій смузі спектра, важко видалити, стеганографічні методи на основі широкосмугових є стійкими до випадкових і навмисних перекручувань.

Для приховування інформації застосовують два основних способи розширення спектра:

– за допомогою псевдовипадкової послідовності, коли секретний сигнал, що відрізняється на константу, модулюється псевдовипадковим сигналом;

– за допомогою стрибкоподібних частот, коли частота несучого сигналу змінюється за деяким псевдовипадковим законом.

Розглянемо один з варіантів реалізації широкосмугового методу [21]. Як контейнер використовується напівтонове зображення розміром $N \times M$. Усі користувачі прихованого зв'язку мають множину $l(m)$ зображень φ_i розміром $N \times M$, яка використовується як стегоключ. Зображення φ_i взаємно ортогональні, тобто

$$\phi_i \phi_j = \sum_{x=1}^{N} \sum_{y=1}^{M} \phi_i(x, y) \phi_j(x, y) = G_i \delta_{ij},$$

де $G_i = \sum_{x=1}^{N} \sum_{y=1}^{M} \phi_i^2(x, y)$, δ_{ij} – дельта-функція.

Для приховування повідомлення m необхідно згенерувати стегоповідомлення $E(x,y)$ у вигляді зображення, формуючи зважену суму

$$E(x,y)=\sum_i m_i\phi_i(x,y).$$

Потім, шляхом формування поелементної суми обох зображень, вмонтувати секретну інформацію E у контейнер C: $S(x,y)=C(x,y)+E(x,y)$.

В ідеалі, контейнерне зображення C повинно бути ортогональним до усіх φ_i (тобто $\langle C,\phi_i\rangle$ =0), і одержувач може витягнути *i-ий* біт повідомлення m_i, проектуючи стегозображення S на базисне зображення φ_i:

$$\langle S,\phi_i\rangle=\langle C,\phi_i\rangle+\left\langle\sum_j m_j\phi_j,\phi_i\right\rangle=\sum_j m_j\langle\phi_j\phi_i\rangle=G_i m_i. \qquad (3.1)$$

Секретна інформація може бути витягнена шляхом обчислення $m_i=\langle C,\phi_i\rangle/G_i$. Зазначимо, що на цьому етапі немає потреби знати вихідний контейнер C. Однак на практиці контейнер C не буде повністю ортогональний до всіх зображень φ_i, тому в співвідношення (3.1) повинна бути введена величина похибки $(C,\varphi_i)=\Delta C_i$, тобто $(C,\varphi_i)=\Delta C_i+G_i m_i$.

Покажемо, що при деяких припущеннях математичне сподівання ΔC_i дорівнює нулеві. Нехай C і φ_i дві незалежні випадкові величини розміром $N\times M$. Якщо припустити, що всі базиси зображень не залежать від повідомлень, що передаються, то:

$$\vec{E}[\Delta C_i]=\sum_{i=1}^{N}\sum_{j=1}^{M}\vec{E}[C(x,y)]\vec{E}[\phi_i(x,y)]=0.$$

Таким чином, математичне сподівання величини похибки $\langle C,\phi_i\rangle$=0. Тому операція декодування полягає у відновленні секретного повідомлення шляхом проектування стегозображення S на усі функції φ_i: $s_i=\langle S,\phi_i\rangle=\Delta C_i+G_i m_i$. Якщо математичне сподівання ΔC_i дорівнює нулеві, то $s_i\approx G_i m_i$. Якщо секретні повідомлення були закодовані як рядки -1 і 1 (замість простого використання двійкових рядків), значення m_i можуть бути відновлені за допомогою функції:

$$m_i=sign(s_i)=\begin{cases}-1, \textit{ при } s_i<0\\ 0, \textit{ при } s_i=0\\ 1, \textit{ при } s_i>0\end{cases}$$

за умови, що $G_i>>0$. Якщо m_i=0, то приховувана інформація буде втрачена. За деяких умов значення $|\Delta C_i|$ може зрости настільки (хоча його математичне сподівання дорівнює нулеві), що витягання відповідного біта

стане неможливим. Однак це відбувається рідко, а можливі помилки можна виправляти, застосовуючи коригувальні коди.

Основна перевага широкосмугових стеганометодів – це порівняно висока стійкість до перекручувань зображення і різного виду атак, оскільки приховувана інформація розподілена в широкій смузі частот і її важко видалити без повного руйнування контейнера. Перекручування стегозображення збільшують значення ΔC_i і, якщо $|\Delta C_i|>|\Delta G_i m_i|$, то приховане повідомлення не постраждає.

3.3.4 Статистичні методи

Статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення. Вони базуються на перевірці статистичних гіпотез. Суть методу полягає в такій зміні деяких статистичних характеристик контейнера, при якій одержувач зможе відрізнити модифіковане зображення від немодифікованого.

Дані методи відносяться до «однобітових» схем, тобто орієнтовані на приховування одного біта секретної інформації. $l(m)$-розрядна статистична стегосистема утвориться з множини однорозрядних шляхом розбивання зображення на $l(m)$ блоків, що не перетинаються, $B_1,...,B_{l(m)}$. При цьому секретний біт повідомлення m_i вбудовується в *i-й* блок контейнера. Виявлення прихованого біта в блоці здійснюється за допомогою перевірочної функції, яка відрізняє модифікований блок від немодифікованого:

$$f(B_i)=\begin{cases}1, & \textit{якщо блок } B_i \textit{ був модифікований}\\ 0, & \textit{в протилежному випадку}\end{cases}$$

Основна задача при розробці статистичного методу – це створення відповідної функції *f*. Побудова функції *f* здійснюється на основі теорії перевірки статистичних гіпотез (наприклад: основної гіпотези «блок B_i не змінений» і альтернативної – «блок B_i змінений»). Під час витягання прихованої інформації необхідно послідовно застосовувати функцію *f* до всіх блоків контейнера B_i. Припустимо, що відомо про статистику розподілу елементів немодифікованого блоку зображення $h(B_i)$. Тоді, використовуючи стандартні процедури, можна перевірити, чи перевищує статистика $h(B_i)$ аналізованого блоку деяке граничне значення. Якщо не перевищує, то передбачається, що в блоці зберігається біт «0», в іншому випадку – «1».

Найчастіше статистичні методи стеганографії складно застосовувати на практиці. По-перше, необхідно мати гарну статистику $h(B_i)$, на основі якої приймається рішення про те, чи є аналізований блок зображення зміненим чи ні. По-друге, розподіл $h(B_i)$ для «нормального» контейнера повинен бути заздалегідь відомим, що в більшості випадків є досить складною задачею.

Розглянемо приклад статистичного методу [22]. Припустимо, що кожен блок контейнера B_i являє собою прямокутник пікселів $p^{(i)}_{n,m}$. Нехай маємо псевдовипадкову двійкову модель того ж розміру $S = \{s^{(i)}_{n,m}\}$, в якій число одиниць і нулів збігається. Модель S у даному випадку являє собою стегоключ. Для приховування інформації кожен блок зображення B_i поділяється на дві рівних підмножини C_i і D_i, де $C_i = \{p^{(i)}_{n,m} \in B_i \mid s_{n,m} = 1\}$ і $D_i = \{p^{(i)}_{n,m} \in B_i \mid s_{n,m} = 0\}$. Потім до всіх пікселів множини C_i додається значення $k>0$. Для витягання повідомлення необхідно реконструювати підмножини C_i і D_i і знайти розходження між ними. Якщо блок містить повідомлення, то всі значення підмножини C_i будуть більші, ніж відповідні значення на етапі вбудовування повідомлення. Якщо припустити, що всі пікселі C_i і Di незалежні, випадково розподілені величини, то можна застосувати статистичний тест:

$$q_i = \frac{\overline{C}_i - \overline{D}_i}{\hat{\sigma}_i}, \quad \text{де } \hat{\sigma}_i = \sqrt{\frac{Var[C_i] + Var[D_i]}{|S|/2}},$$

де $\overline{C}_i$ – середнє значення всіх пікселів множини C_i, а $Var[C_i]$ – оцінка дисперсії випадкових змінних у C_i. Відповідно до центральної граничної теореми статистика q буде асимптотично прагнути до нормального розподілу $N(0,1)$. Якщо повідомлення вбудоване в блок зображення B_i, то математичне сподівання q буде більше нуля. Таким чином, i-ий біт секретного повідомлення відновлюється шляхом перевірки статистики q_i блоку B_i на рівність нулеві.

3.3.5 Методи перекручування

Методи перекручування, на відміну від попередніх методів, потребують знання про початковий вигляд контейнера. Схема приховування полягає в послідовному проведенні ряду модифікацій

контейнера, які вибираються відповідно до секретного повідомлення. Для витягання прихованих даних необхідно визначити усі відмінності між стеганограмою і вихідним контейнером. За цими відмінностями відновлюється послідовність модифікацій, які виконувалися під час приховування секретної інформації. Для більшості додатків такі системи не підходять, оскільки для витягання даних необхідно мати доступ до набору початкових контейнерів: якщо «противник» також буде мати доступ до цього набору, то він зможе легко виявити модифікації контейнера і отримати доказ прихованого листування. Таким чином, основною вимогою під час використання таких методів є необхідність розповсюдження набору вихідних контейнерів між абонентами мережі через секретний канал доставки.

Методи перекручування легко застосовні до цифрових зображень. Як і в методах заміни, для приховування даних вибирається $l(m)$ різних пікселів контейнера, які використовуються для приховування інформації. Такий вибір можна здійснити, використовуючи датчик випадкових чисел (або перестановок). Під час приховування біта «0» значення піксела не змінюється, а при приховуванні «1» до кольору піксела додається випадкове значення Δx. Хоча цей підхід подібний до методу заміни, існує одне істотне розходження: у LSB-методі значення вибраного кольору не обов'язково дорівнює секретному бітові повідомлення, а в методах перекручування під час приховування нульового біта не відбувається ніяких змін. Окрім цього, значення Δx може бути вибране так, що будуть зберігатися статистичні властивості контейнера. Для витягання прихованих даних необхідно провести порівняння всіх $l(m)$ вибраних пікселів стеганограми з відповідними пікселами вихідного контейнера. Якщо i-ий піксел буде відрізнятися, то це свідчить про те, що в прихованому повідомленні був одиничний біт, інакше – нульовий.

Інший приклад методу перекручування зображення під час приховування даних був запропонований у [23]. У даному методі під час вставлення приховуваних даних робиться спроба скоріше змінити порядок появи надлишкової інформації в контейнері, ніж змінити його вміст. Під час приховування даних складається певний «список пар» пікселів, для яких відмінність буде менше граничної. Цей список відіграє роль стегоключа - без нього не можна відновити секретне повідомлення. Якщо абонент має доступ до «списку пар», то він завжди зможе провести зворотну процедуру.

3.3.6 Структурні методи

Розглянуті вище методи в основному використовували інформаційну надлишковість на рівні пікселів або ж проводили перетворення в частотній області зображення. Нижче розглядається метод, в якому приховування інформації проводиться на змістовному рівні з використанням структурних та інформаційних параметрів зображення [24]. Власне кажучи, він є розвитком відомої стеганографічної технології – семаграм. Суть методу полягає в проведенні послідовних перетворень фрагментів графічного зображення, які в остаточному підсумку приводять до формування приховуваного тексту.

В даний час з'явилося безліч графічних пакетів програм і баз даних, за допомогою яких можна створювати різні графічні зображення, презентації, мультиплікацію та ін. У кожному графічному зображенні можна виділити окремі компоненти, які відповідно до його області інтерпретації мають своє інформаційне навантаження. Візуальний образ *S* можна представити у вигляді цифрової послідовності, яку потім можна легко перетворити в текст повідомлення. Це можливо, наприклад, у процесі покриття образу деяким графом, використовуючи інформаційну інтерпретацію його окремих компонентів. У першому наближенні вершинами такого графа можуть служити окремі компоненти рисунка, а ребрами – їх з'єднання. Під час кодування приховуваної інформації отриманий граф можна перетворювати досить широким спектром відомих у теорії графів перетворень. В остаточному підсумку такий граф може бути розмічений відповідно до визначеного алгоритму. Розмічений граф можна представити у вигляді його числового інваріанта. Найпростішим інваріантом може служити матриця суміжності графу, послідовність нумерації вершин. Можна використовувати кілька інваріантів, які описуються у вигляді многочлена. Секретним ключем у такому підході може бути спосіб нумерації графу. Відомо, що можлива кількість перенумерованих графів для довільного графу досить велика. Ця обставина робить запропонований спосіб приховування повідомлень досить стійким проти атак розкриття.

У структурних методах можна виділити окремі етапи стеганографічного перетворення.

Першим етапом є перетворення захищуваного секретного повідомлення *m* у цифрову *форму CH*. Це перетворення може бути, наприклад, будь-яким криптографічним перетворенням. Воно являє собою

шифрування тексту з усіма відповідними атрибутами, включаючи ключі шифрування.

Другий етап являє собою перетворення послідовності чисел *CH* у графічну структуру *GS*. Як графічні структури найчастіше використовуються графи. Крім графів можна використовувати різні піктограми або інші структури, які піддаються формальному опису тим або іншим способом.

На третьому етапі здійснюється перетворення графічної структури *GS* у візуальне інформаційне середовище *WS*. У загальному випадку як таке середовище може використовуватися, наприклад, будь-яке мультимедійне або програмне середовище.

Четвертий етап являє собою сукупність методів і відповідних процедур, за допомогою яких формується сюжет із візуальних образів з вбудованими в них таємними повідомленнями.

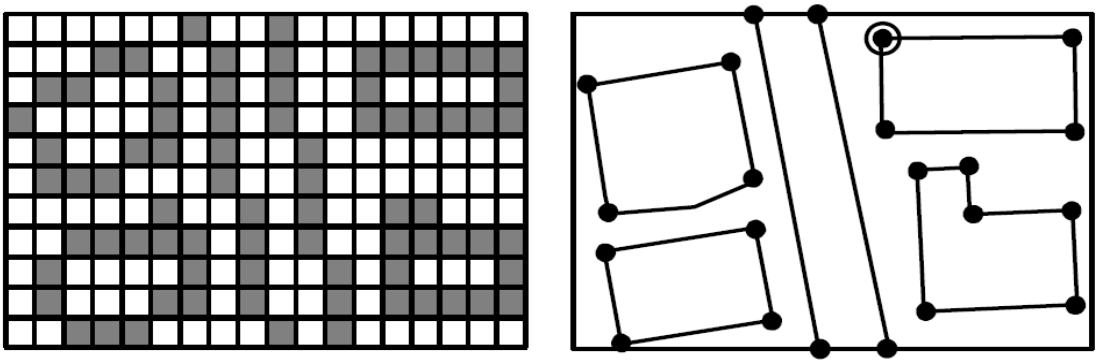
У рамках даного підходу візуальний образ складається з графічних елементів, які ідентифікуються з елементами *GS*. Дані елементи являють собою позначені вершини, позначені або непозначені ребра й інші елементи, що ідентифікують компоненти з *CH*. Необхідним етапом функціонування таких стегосистем є формування деякого сюжету для фрагмента інформаційного середовища з окремих графічних образів.

Таким чином, весь ланцюжок перетворень, який реалізується стегосистемою на рівні окремих етапів перетворення, може бути записаний у вигляді: $S \Rightarrow CH \Rightarrow GS \Rightarrow WS \Rightarrow SJ$, де *SJ* – опис сюжету, який складається з окремих графічних образів. Слід зазначити, що розглянутий підхід може застосовуватись як для перетворення зображення з метою розміщення в ньому приховуваного повідомлення, так і для генерування візуального зображення за секретним повідомленням.

3.4 Стеганографічні методи вбудовування інформації у векторні зображення

Поширені на сьогодні стеганографічні методи приховування даних та захисту растрових зображень для вбудовування стійких ЦВЗ, в основному, базуються на використанні статистичної та фізіологічної надлишковості інформації. При цьому вбудовування бітів ЦВЗ, в основному, відбувається зміною відтінків кольору точок.

Проте на сьогодні векторні зображення (рис. 3.8) теж мають достатньо широке використання, зокрема, для проектування архітектурних об’єктів, інтер’єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо.



Растрове Векторне

Рисунок 3.8 – Приклади растрового та векторного зображень

Двовимірні векторні географічні карти у наш час дуже широко використовуються і мають важливе значення. Існує велика кількість типів карт з різним призначенням та точністю відображення, на створення яких витрачається багато часу та коштів. Використання векторних карт сьогодні дуже поширене – існує достатньо Інтернет-сервісів, які надають доступ до деталізованих карт усього світу, крім того, кожен може скористатися системою GPS-навігації за допомогою спеціального пристрою чи мобільного телефону, які також використовують карти у векторному форматі. В зв’язку з цим виникає проблема, пов’язана з можливістю нелегального копіювання та розповсюдження векторних зображень, які мають свого правовласника.

Оскільки у файлі векторних зображень зберігається інформація про координати точок та колір, з яких за допомогою формул формуються об’єкти, то вбудовувати цифровий водяний знак можна, наприклад, шляхом зміни координат точок. Вбудовування ЦВЗ за рахунок зміни

кольору є неефективним, оскільки кількість кольорів об’єктів у векторному зображенні, в основному, є значно меншою, ніж кількість точок, з яких формуються відповідні об’єкти.

На сьогодні запропоновано низку методів, що дозволяють вбудовувати інформацію в зображення векторного формату. Як і для растрових зображень, методи вбудовування цифрових водяних знаків у векторні зображення можна розділити на декілька груп залежно від того, яким чином вбудовується інформація. За аналогією з методами растрових зображень, де існують «прямі» та «непрямі» методи [22], так само можна здійснити поділ і методів для векторних зображень. До першої групи можна віднести «прямі» методи, які вбудовують біти ЦВЗ шляхом зміни абсолютних значень координат точок згідно з певним алгоритмом в так званій просторовій області. До другої групи можна віднести методи вбудовування інформації в зображення шляхом представлення його у певній формі з використанням певного математичного перетворення.

3.4.1 Прямі методи вбудовування інформації у векторні зображення

Загальний підхід методів першої групи щодо вбудовування ЦВЗ у векторні зображення схожий з тим, що використовується для растрових зображень. Якщо для растрових методів – це пряма зміна значень кольорів зображень, то для векторних – незначна зміна координат точок, з яких складається зображення. Тому для векторних зображень можна використовувати алгоритми вбудовування інформації, що використовуються для растрових методів. Це ж стосується і підходів щодо покращення стійкості «прямих» методів, наприклад, за допомогою алгоритму псевдовипадкового інтервалу або псевдовипадкової перестановки. Слід зазначити, що особливістю векторних зображень є можливість змінювати не тільки значення точок, а й їх кількість, на основі чого можна розробляти нові алгоритми вбудовування інформації.

Проаналізуємо існуючі на сьогодні методи, що вбудовують ЦВЗ у просторову область.

У роботі [22] автори для запропонованого методу використовують оновлений та модифікований алгоритм квадрадерева. При використанні цього алгоритму векторне зображення розділяється на трикутну сітку, що базується на щільності вершин, ЦВЗ вбудовується шляхом модифікації координат вершин трикутних сіток. В той самий час порядок вбудовування ЦВЗ визначається поділом трикутних сіток на рівні. Для того, щоб витягнути ЦВЗ, необхідно розділити зображення з ЦВЗ таким самим чином і після цього порівняти координати вершин з даними ЦВЗ.

Також відомий метод [23], згідно з яким пропонується додавати точки зображення, змінювати довжину, напрям та атрибути ліній для вбудовування ЦВЗ. Вставка точок та зміна ліній є дуже простим методом, що не забезпечує стійкості методу, а метод зміни напрямку ліній та атрибутів не є підходящим для точних векторних даних.

Автори методу [24] взяли за основу метод, що використовує PN-послідовність (PN – псевдо-шум) в якості ЦВЗ і складається зі значень від'ємного та додатного максимальних відхилень (похибки) та вбудовують його в координати 2-х вимірних векторних карт. Витягування ЦВЗ здійснюється за допомогою релевантності PN-послідовності та даних, що були вбудовані.

У роботі [25] автори пропонують метод, згідно з яким векторна карта ділиться на послідовність сіток висотою в 4/3 допустимого відхилення координат точок, після чого в кожній сітці рисуються дві лінії довжиною 1/3 допустимого відхилення і позначаються як лінія 0 і лінія 1. ЦВЗ вбудовується шляхом переміщення вершин в сітці до лінії 0 чи лінії 1. Якщо вершина в області 0 і нам необхідно вбудувати 1, ми переміщаємо вершину в область 1. Нова позиція є симетричною до оригінальної позиції відносно діагоналі.

Відомий метод [26], згідно з яким векторне зображення ділиться навпіл та проводиться адаптивне регулювання на стійкість ЦВЗ відповідно до щільності точок векторного зображення. Після цього, враховуючи дозволену максимально допустиму похибку відхилень координат точок векторного зображення, вбудовується ЦВЗ в векторне зображення шляхом зміни координат вершин. Для того, щоб витягнути дані ЦВЗ, необхідно перевірити карту з подвійним порогом.

У роботі [27] автори пропонують метод, згідно з яким векторне зображення розкладається відповідно до характеристик полігону. Після цього проводиться аналіз векторного полігону, обираються необхідні для вбудовування елементи зображення та проводиться вбудовування ЦВЗ у вершини полігонів. Для того, щоб витягнути ЦВЗ, необхідною є наявність оригінального зображення та самого ЦВЗ, після аналізу яких виконується витягування ЦВЗ з вершин полігонів.

Також відомий метод [28] перевірки цілісності векторної карти. Метод базується на зворотній технології вбудовування крихкого ЦВЗ та використовує ущільнення даних без втрат для досягнення зворотності. Оригінал векторного зображення використовується при витягуванні ЦВЗ для виявлення найменших змін векторного зображення. Основним недоліком цього методу є те, що додавання або видалення вершин полігонів чи поліліній знищує можливість виявлення модифікації векторного зображення.

У роботі [29] запропоновано метод, який комбінує метод найменш значущого біта (НЗБ), метод запису топології просторових даних ГІС, а також шифрування ЦВЗ. Цей метод реалізований для приховування псевдовипадково розповсюдженого ЦВЗ в файлах певного формату, що використовуються програмним забезпеченням GISArc/Info.

Також відомий метод [30], автори якого пропонують двошаровий алгоритм вбудовування стійких ЦВЗ. Цей алгоритм розділяє векторну

карту на два прошарки, в кожну з яких вбудовується ЦВЗ шляхом зміни точок векторного зображення, використовуючи при цьому різні алгоритми зміни. Для витягування ЦВЗ, необхідно не виходячи за межі допустимого рівня спотворень розрахувати позиції ЦВЗ в кожному прошарку, визначити точки, в яких вбудовано ЦВЗ та порахувати середнє значення координат.

Основними недоліками розглянутих методів є забезпечення недостатнього рівня стійкості до зловмисних атак на векторні зображення, особливо до пасивних, що дозволяють визначити місце розташування ЦВЗ для можливого його подальшого видалення. Це пов'язано з низьким рівнем кореляції між сусідніми точками, які були змінені внаслідок вбудовування ЦВЗ, що також спричиняє помітні спотворення векторного зображення.

Суть «непрямих» методів вбудовування ЦВЗ у використанні математичних перетворень для представлення зображень у такій формі, особливості якої дають додаткові можливості для вбудовування ЦВЗ. Для растрових зображень такі перетворення дозволяють представити зображення у вигляді значень частот певного кольору та дозволяють виділити в зображенні більш значущі елементи від незначущих, якими можна знехтувати без помітних людському оку візуальних змін. Така особливість дає можливість модифікувати такі значення перетворення, зміна яких суттєво не вплине на якість зображення та забезпечить достатню стійкість зображення до навмисних спотворень, наприклад, ущільнення згідно з алгоритмом JPEG.

На сьогодні запропоновано декілька «непрямих» методів вбудовування інформації у векторні зображення, які також використовують математичні перетворення. При цьому вбудовування ЦВЗ відбувається шляхом зміни не координат точок, а, наприклад, їхніх частотних характеристик. Наприклад, використання методу тріангуляції Делоне дозволяє перетворити векторне зображення, що є набором точок з певними координатами, у цілісне

двовимірне зображення. Це зображення формується шляхом з'єднання всіх точок між собою згідно з методом та представляється у вигляді сітки, де лінії між точками не перетинаються. Такий підхід використовується для подальшого застосування частотного перетворення. Після цього відбувається зміна значень використаного перетворення для вбудовування бітів цифрового водяного знаку.

Основною проблемою при вбудовуванні ЦВЗ є погіршення якості зображення. Якщо для растрових зображень це погіршення якості зображення внаслідок значної зміни відтінків пікселів, то для векторних зображень – це зміна контурів об'єктів, чи їх положення внаслідок зміни кількості та координат точок. Причому для векторних зображень, що відображають реальні об'єкти в масштабі (архітектурні споруди, механічні та електронні прилади, географічні карти тощо), ця проблема є дуже актуальною, бо суттєва зміна координат точок може спотворити інформацію про існуючі об'єкти чи вплинути на їх створення.

3.4.2 Методи вбудовування інформації у векторні зображення на основі математичних перетворень

Оскільки у «прямих» методів вбудовування ЦВЗ у просторову область векторних зображень існують проблеми, пов'язані з недостатнім рівнем стійкості до зловмисних атак, більший інтерес викликають методи, що при вбудовуванні ЦВЗ використовують математичні перетворення для представлення зображення у певному вигляді і забезпечують вищий рівень стійкості.

Виходячи з поставлених завдань дослідження, важливим є аналіз цих методів з точки зору рівня спотворення зображень внаслідок вбудовування ЦВЗ, а також можливості витягування ЦВЗ без наявності оригіналу зображення чи самого ЦВЗ.

У роботі [21] запропоновано метод вбудовування ЦВЗ, що базується на дискретному перетворенні Фур'є (ДПФ). Суть методу полягає у зміні координат точок, з яких сформовані закриті полігони векторних карт. Цей

метод використовує особливості перетворення Фур'є для геометричних перетворень. ЦВЗ вбудовується у послідовність коефіцієнтів ДПФ, що відповідають масивам вершин закритих полігонів. Витягування бітів ЦВЗ проводиться з використанням адаптованого методу виявлення лінійної кореляції. Для витягування необхідною є наявність оригіналу векторного зображення, що дещо ускладню процедуру підтвердження авторства.

На основі цього методу у роботі [22] запропоновано вдосконалений метод вбудовування ЦВЗ у векторні зображення, який не потребує для витягування ЦВЗ оригіналу зображення. Однак це досягається шляхом значної зміни коефіцієнтів ДПФ, що в деяких випадках суттєво впливає на якість векторного зображення внаслідок вбудовування ЦВЗ.

Також на основі методу [22] в роботі [23] запропоновано метод вбудовування ЦВЗ, в якому вдосконалено процедуру витягування ЦВЗ. Суть вдосконалення полягає у забезпеченні кращого рівня правильності розпізнавання бітів ЦВЗ. Для цього використовується надлишковість вбудованих даних, а також розроблено метод визначення наявності ЦВЗ у зображенні шляхом перевірки лише одного багатокутника. Недоліком цього методу є те, що для витягування ЦВЗ виникає необхідність наявності його оригіналу.

Автори роботи [24] пропонують метод, що також базується на ДПФ. Згідно з методом спершу виконується перетворення координат точок в ціле значення, а потім перетворення ДПФ для масивів з 8 точок. ЦВЗ вбудовується шляхом зміни високочастотних коефіцієнтів. В роботі також проведений детальний аналіз рівня спотворень векторних зображень внаслідок вбудовування ЦВЗ, а також можливого розміру ЦВЗ. Недоліком цього методу є невеликий розмір вбудованого ЦВЗ, а також необхідність наявності оригіналу зображення при витягуванні ЦВЗ.

У роботі [25] запропоновано метод, який є оптимізацією попереднього методу [24]. Згідно з методом також з'єднуються 8 сусідніх точок, однак

над ними виконується ДКП. Коефіцієнти, отримані в результаті цього перетворення, діляться на два діапазони – R1 і R2. Для кожного коефіцієнта з діапазону R2, якщо він не більший за максимальний елемент з R1, відбувається подвоєння його значення. Якщо цей коефіцієнт більший, ніж максимальне значення в R1, до нього додається максимальне значення з R1. Таким чином, ЦВЗ вбудовується шляхом зміни коефіцієнта R2. Цей метод забезпечує витягування без наявності оригіналу ЦВЗ, однак внаслідок вбудовування ЦВЗ можливі значні спотворення векторного зображення.

Також запропоновано метод [26], що вбудовує ЦВЗ в діапазон коефіцієнтів ДПФ та використовує практичний алгоритм витягування ЦВЗ. Для витягування ЦВЗ використовується коефіцієнт кореляції витягнутого і оригінального ЦВЗ. Недоліком цього методу є необхідність наявності оригіналу самого ЦВЗ.

Метод, поданий в роботі [27], також вбудовує ЦВЗ у векторні зображення на основі частотного перетворення. Для цього методу використовується дискретне вейвлет-перетворення (ДВП) над множиною координат точок ліній і площин. Вбудовування ЦВЗ проводиться шляхом зміни низькочастотних коефіцієнтів, що отримані в результаті вейвлет-перетворення, після чого виконується зворотне ДВП для отримання векторного зображення з вбудованим ЦВЗ. Недоліком запропонованого методу є значний вплив зміни низькочастотних коефіцієнтів на значення координат точок, а також те, що при видаленні однієї з точок векторного зображення буде неможливо розпізнати ЦВЗ.

У роботі [28] запропоновано метод захисту авторського права векторних зображень за допомогою цифрових водяних знаків Обуші-Уеда-Ендоха. Суть методу полягає у вбудовуванні ЦВЗ у частотну область представлення векторного зображення.

Для цього векторне зображення представляється як масив точок, які з’єднуються між собою за допомогою тріангуляції Делоне. В результаті утворюється двовимірна поверхня з трикутників, вершинами яких є усі точки векторного зображення, приклад якої показано на рис. 3.9.

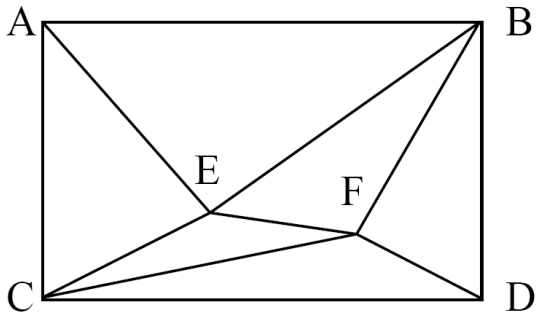


Рисунок 3.9 – Приклад частини сформованої поверхні після тріангуляції Делоне

Для представлення зображення у частотному вигляді проводиться послідовне перетворення частин утвореної поверхні за допомогою матриць Лапласа розміром $n \times n$. Коефіцієнти отриманих матриць перетворення показують частоту появи певних значень довжин сторін трикутників. Приклад сформованої матриці показано на рис. 3.10.

$$\begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & D & E & F \end{array} \\ \begin{bmatrix} 1 & -1/3 & -1/3 & 0 & -1/3 & 0 \\ -1/4 & 1 & 0 & -1/4 & -1/4 & -1/4 \\ -1/4 & 0 & 1 & -1/4 & -1/4 & -1/4 \\ 0 & -1/3 & -1/3 & 1 & 0 & -1/3 \\ -1/4 & -1/4 & -1/4 & 0 & 1 & -1/4 \\ 0 & -1/4 & -1/4 & -1/4 & -1/4 & 1 \end{bmatrix} \end{array}$$

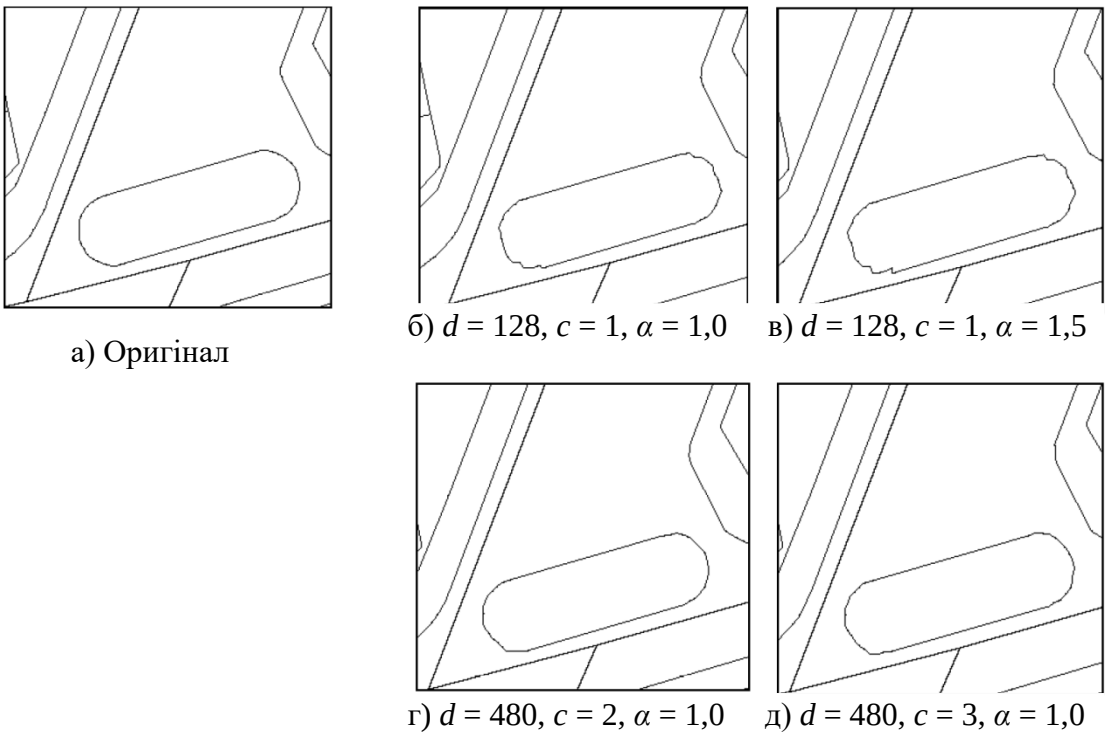
Рисунок 3.10 – Приклад сформованої матриці Лапласа частотних коефіцієнтів

Вбудовування бітів ЦВЗ проводиться шляхом зміни значень частотних коефіцієнтів залежно від біта ЦВЗ згідно з такою умовою:

$$b_i' = \begin{cases} -1, \textit{якщо } b_i = 0; \\ 1, \textit{якщо } b_i = 1. \end{cases}$$

Витягування ЦВЗ проводиться шляхом порівняння матриць частотних коефіцієнтів зображення з вбудованим ЦВЗ та матриць оригіналу векторного зображення.

Автори запропонованого методу проаналізували його щодо впливу вбудовування ЦВЗ на якість зображення, результати якого показані на рис. 3.11.



а) Оригінал

б) d = 128, c = 1, α = 1,0

в) d = 128, c = 1, α = 1,5

г) d = 480, c = 2, α = 1,0

д) d = 480, c = 3, α = 1,0

З вбудованими ЦВЗ

Рисунок 3.11 – Приклади фрагментів зображень до та після вбудовування ЦВЗ

З рис. 3.11 видно, що цей метод забезпечує в деяких випадках незначний вплив вбудовування ЦВЗ на якість векторного зображення.

Такий результат досягається тим, що для витягування ЦВЗ використовується оригінал самого зображення, що дає змогу вбудовувати біти ЦВЗ без значних змін координат точок зображення. Однак потреба в оригіналі зображення може дещо ускладнювати процедуру витягування ЦВЗ для користувача, особливо при великій кількості захищених зображень, оскільки вони всі повинні бути в наявності для підтвердження авторства.

У роботі [29] запропоновано метод вбудовування ЦВЗ у двовимірні векторні карти на базі одновимірного ДКП, який дозволяє витягувати ЦВЗ без додаткової інформації.

Згідно з методом Войта-Янга-Буша векторне зображення перетворюється в частотний вигляд за допомогою одновимірного ДКП. Суть методу полягає у вбудовуванні бітів ЦВЗ шляхом зміни значень високочастотних коефіцієнтів. Для цього, залежно від біта ЦВЗ, змінюється значення останнього коефіцієнта. Якщо біт ЦВЗ – «1», то останній коефіцієнт A_7 збільшується на максимальне значення коефіцієнта з діапазону A_1-A_6. Змінене значення буде позначатися як A'_7. Якщо біт ЦВЗ дорівнює «0», коефіцієнт не змінюється. Приклад вибору точок, результат ДКП та вбудовування ЦВЗ показано на рис. 3.12.

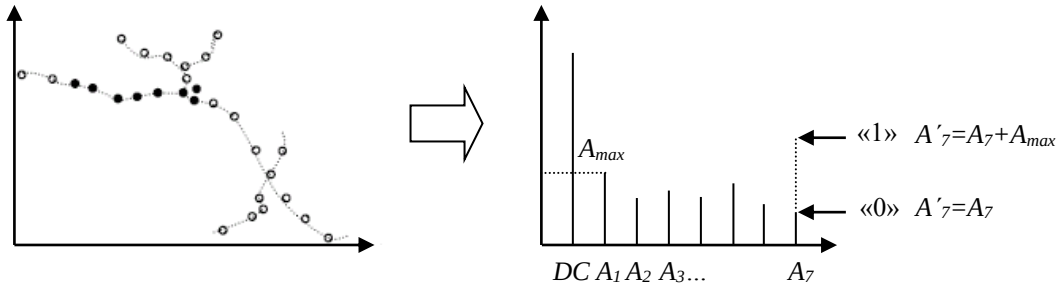


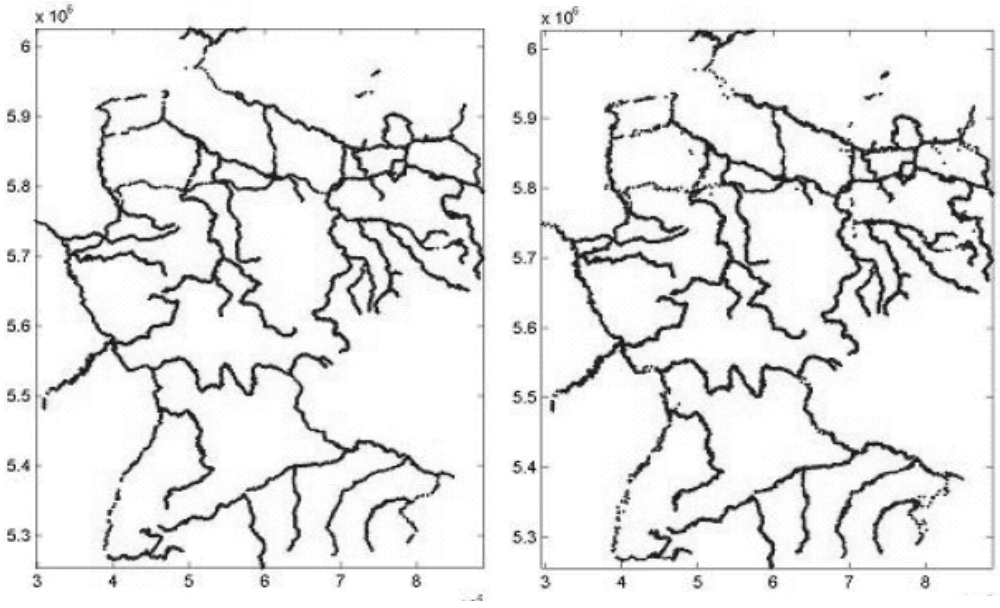
Рисунок 3.12 – Приклад процесу вбудовування ЦВЗ

Такий підхід забезпечує витягування ЦВЗ без наявності оригіналу карти чи ЦВЗ, бо для витягування бітів достатньо порівняти значення

останнього коефіцієнта з іншими: якщо він більший – значить це «1», якщо менший – «0».

Вбудовування ЦВЗ у зображення згідно із запропонованим авторами методом дещо більше впливає на якість векторних зображень у порівнянні з методом Обуші-Уеда-Ендоха, однак його перевага полягає у тому, що для витягування не потрібна наявність оригіналу зображення чи ЦВЗ.

В [29] було показано, що сумарна похибка відхилення координат точок відносно оригіналу в деяких випадках є досить суттєвою. Для зменшення впливу ЦВЗ на координати точок в роботі було запропоновано обмежити значення A_{max} шляхом вибору його з діапазону A_4–A_6. Але це не дає прийнятного результату щодо збереження якості зображення, бо можливі випадки, коли серед значень діапазону A_4 – A_6 знаходиться велике порівняно з A_7 число. Результати візуального спотворення показано на рис. 3.13.



Оригінал **З вбудованим ЦВЗ**

Рисунок 3.13 – Приклад векторного зображення до та після вбудовування ЦВЗ

Також до стеганографічних методів, що для витягування ЦВЗ не потребують оригіналу зображення чи самого ЦВЗ та базуються на певних перетвореннях векторних зображень, відносять відомі методи Базіна-

Барса-Маделана [30], Хе-Жу-Ванга [31], Солачідіса-Ніколаїдіса-Пітаса [32]. Проте загальною проблемою цих методів є помітне погіршення якості векторного зображення внаслідок вбудовування ЦВЗ.

Виходячи з проведеного аналізу існуючих методів, актуальним є дослідження щодо зменшення рівня спотворення векторних зображень при забезпеченні витягування ЦВЗ без наявності оригіналу зображення чи самого ЦВЗ.

3.5 Приховування інформації в звуковому середовищі

Особливий розвиток знайшли цифрові методи стеганографії в аудіо середовищі. З їхньою допомогою забезпечується пересилання великих об'ємів прихованих даних у звукових повідомленнях, які транслюються телевізійними, радіо або телефонними мережами. Сучасні засоби телекомунікації дозволяють передавати звукові сигнали не тільки в реальному часі, але й у цифровому форматі через будь-яку мережу передавання даних. Відомо, що слуховий апарат людини функціонує в широкому динамічному діапазоні; він дуже чутливий до випадкових адитивних перешкод, здатний розрізняти відносну фазу, зовсім нечутливий до абсолютної фази. Ці особливості слухового апарату дозволяють вдало використовувати стеганографічні методи в аудіо середовищі [26,27].

3.5.1 Стеганографічні методи захисту даних у звуковому середовищі

Метод найменших значущих бітів застосовується при цифровому представленні аудіо сигналу і придатний для використання при будь-яких швидкостях зв'язку. Під час перетворення звукового сигналу в цифрову форму завжди присутній шум дискретизації, який не вносить істотних перекручувань. «Шумовим» бітам відповідають молодші біти цифрового представлення сигналу, які можна замінити приховуваними даними. Наприклад, якщо звуковий сигнал представлений у 16-бітовому вигляді, то зміна чотирьох молодших з них не призведе до істотного для слуху перекручування. Як стегоключ зазвичай використовується покажчик місця розташування бітів, у яких містяться приховувані дані.

Методи широкосмугового кодування використовують ті ж принципи, що методи приховування даних у зображеннях. Їхня суть полягає в незначній одночасній модифікації цілого ряду певних бітів контейнера під час приховування одного біта інформації. Існує кілька різновидів методу. У найбільш розповсюдженому варіанті вихідний сигнал модулюється високошвидкісною псевдовипадковою послідовністю $w(t)$, яка визначена на області значень {-1, 1}. Внаслідок цього для передавання результату необхідна велика (іноді, більш ніж у 100 разів) смуга пропускання. Зазвичай послідовності $w(t)$ вибирають ортогональними до сигналу контейнера. Результувальний стегосигнал $s(t)$ являє собою сумарний сигнал контейнера $c(t)$ і приховуваних даних $d(t)$: $s(t)=v(t)+\alpha\times d(t)\times w(t)$, де коефіцієнт загасання α призначений для вибору оптимального рівня шуму, який вноситься даними, що вставляються.

Для витягання прихованих даних $d(t)$ на приймаючій стороні необхідно мати ту ж саму псевдовипадкову імпульсну послідовність $w(t)$, забезпечивши при цьому її синхронізацію зі стегосигналом: $s(t)\times w(t)=v(t)\times w(t)+\alpha\times d(t)$. У зв'язку з цим дану псевдовипадкову бітову послідовність зазвичай використовують як стегоключ.

Метод приховування в луна-сигналі. Приховувати дані можна також шляхом внесення луни в звуковий сигнал. Відомо, що при невеликих часових зсувах луна-сигнал практично не сприймається на слух. Тому, якщо ввести певні часові затримки (наприклад, Δ_1 – для одиничного біта даних і Δ_0 – для нульового), величина яких не перевищує поріг виявлення, то, розбиваючи вихідний звуковий сигнал $v(t)$ на сегменти, у кожний з них можна ввести відповідний луна-сигнал, у залежності від приховуваного біта: $c(t)=v(t)+\alpha v(t-\Delta)$.

У базовій схемі передбачено приховування в аудіо сигналі одного біта, але сигнал можна розбити випадковим чином на l відрізків і в кожен з них вставити по біту. Для виділення луна-сигналу і відновлення прихованих даних застосовується автокореляційний аналіз. Як стегоключ тут зазвичай використовуються значення величин Δ_0 і Δ_1 з урахуванням вибраних границь для відрізків.

Фазові методи приховування застосовуються як для аналогового, так і для цифрового сигналу. Вони використовують той факт, що плавну зміну фази на слух визначити не можна. У таких методах захищувані дані

кодуються або певним значенням фази, або зміною фаз у спектрі. Якщо розбити звуковий сигнал на сегменти, то дані зазвичай приховують тільки в першому сегменті при дотриманні двох умов:

– збереження відносних фаз між послідовними сегментами;

– підсумковий фазовий спектр стегосигналу повинен бути гладким, оскільки різкі стрибки фази є демаскувальним чинником.

Розглянемо приховування даних шляхом зсуву фази. Сигнал контейнера c розбивається на N коротких сегментів $c_i(n)$ довжиною $l(m)$, і за допомогою ШПФ будується матриця фаз $\varphi_i(k)$ і амплітудний спектр $A_i(k)$:

$$\phi_i(k) = \arctan \frac{\mathrm{Im}\left[F\{c_i\}(k)\right]^2}{\mathrm{Re}\left[F\{c_i\}(k)\right]^2} \quad \text{і} \quad A_i(k) = \sqrt{\mathrm{Re}\left[F\{c_i\}(k)\right]^2 + \mathrm{Im}\left[F\{c_i\}(k)\right]^2}$$

У зв’язку з тим, що фазові зсуви між двома сусідніми сегментами можуть бути легко виявлені, то в стегосигналі повинні бути збережені різниці фаз. Тому секретне повідомлення вбудовується тільки у фазу першого сегмента:

$$\bar{\phi}_0(k) = \begin{cases} \pi/2 & якщо \quad m_k = 0 \\ -\pi/2 & якщо \quad m_k = 1 \end{cases}$$

і, крім того, створюється нова матриця фаз:

$$\bar{\phi}_1(k) = \bar{\phi}_0(k) + [\bar{\phi}_1(k) - \bar{\phi}_0(k)]$$

…

$$\bar{\phi}_N(k) = \bar{\phi}_{N-1}(k) + [\bar{\phi}_N(k) - \bar{\phi}_{N-1}(k)].$$

Після цього за допомогою ОШПФ створюється стегосигнал з використанням нової матриці фаз і амплітудного спектра $A_i(k)$. Таким чином, зі зміною початкової фази $\varphi_0(k)$ фази всіх наступних сегментів будуть змінені на відповідну величину. Під час витягання прихованого значення одержувач секретної інформації, знаючи довжину послідовності $c(m)$, зможе обчислити ШПФ і знайти фази $\varphi_0(k)$.

3.5.2 Музичні стегосистеми

Музична форма звукового середовища займає велику частину інформаційного простору Інтернет. Крім цього вона широко використовується в радіомережах загального призначення і

розповсюджується на електронних носіях інформації, які, в зв'язку з розвитком комп'ютерної техніки, отримали широке поширення. Тому використання музичного середовища для приховування інформаційних повідомлень представляється досить перспективним. Для приховування даних крім методів, описаних вище, можна застосовувати методи, що базуються на модифікації тих параметрів музичного середовища, які у теорії музики можна описати якісно [27]. Музичне середовище має своє текстове відображення у вигляді нот та інших знаків, які дозволяють досить адекватно відображати музичний твір і його внутрішню структуру такими елементами, як ноти, гами, періоди, такти, каденції, акорди, мотиви, модуляції, тональності, різні види розвитку, секвенції та ін. Побудови музичних компонентів підкорюються синтаксичним правилам, які можна описати, що дозволяє будувати логічні взаємини і, відповідно, опис структур музичних творів.

Музичні стегосистеми забезпечують приховування інформації в музичному середовищі за аналогією з імпровізацією музичних творів. Власне кажучи імпровізація являє собою таку зміну музичного твору або його фрагментів, яка зберігає основні теми початкового твору у вигляді мелодій, але при цьому розширює образ музичної теми іншими, що доповнюють основний образ рисами, яких не було в основному музичному творі. Основна відмінність від імпровізації полягає в тому, що метою є не розширення образів базового музичного твору, а внесення змін, які зберігають мелодію основного твору, відповідають усім правилам побудови даного твору і при цьому кодують приховуване повідомлення, не перекручуючи головної теми твору.

Фрагмент музичного твору може бути описаний у вигляді деякої логічної структури [28]. Аналогом слова текстового речення в музичному творі буде один такт мелодії, а аналогом речення в музиці будемо вважати фрагменти, що розділяються цензурами. Як правило, музичний твір складається з ряду фраз, які складаються з тактів. Нехай мається фрагмент мелодії, який представляє слово тексту у вигляді співвідношення $\beta(i, j) + ... + \beta(i + k, j + r) = x_i(t)$, а також фрагмент мелодії, записаний у вигляді співвідношення $\alpha(\eta, \xi) + ... + \alpha(\eta + e, \xi + q) = x_\eta(m)$. Вбудовування тексту в музичний твір здійснюється окремими реченнями, кожне з яких може зіставлятися з окремою мелодією.

На першому етапі роботи стегосистеми аналізується кількість мелодій (кількість її модифікацій) у рамках музичного твору в зіставленні з кількістю речень повідомлення. На другому етапі здійснюється аналіз допустимості розширення деякого речення музичного твору реченнями тексту повідомлення. Цей аналіз проводиться на основі дослідження логічних формул тексту речення $L(t)$ і музичного речення $L(m)$. На наступному етапі, у випадку вибору відповідної пари $L(m)$ і $L(t)$, здійснюється аналіз послідовності фраз мелодій, окремих слів тексту і слів мелодії, що відповідає узгодженню пар на рівні опису $x_i(t)$ і $x_i(m)$. Після позитивного вирішення задач перерахованих рівнів формується нотне відображення розширеного музичного твору з внесеним у нього приховуваним повідомленням. На підставі нотного відображення розширення здійснюється його музична реалізація за допомогою засобів, які реалізовані в сучасних комп'ютерах, що представляють собою програмно-апаратні синтезатори звуку.

Зовсім не обов'язково припускати звукове відображення музичних записів, оброблених стегосистемою. Оскільки основна область застосування музичних стегосистем це середовище Інтернет, у якій музичні записи розміщаються в цифровому форматі на WEB-сторінках, то достатньо, щоб розширений музичний твір сприймався сторонніми особами не як шум, а як деяка музика, яка має мелодію або сукупність мелодій, що допускають ту або іншу тематичну інтерпретацію.

3.6 Питання для самоконтролю знань

1. На яких принципах базуються методи комп'ютерної стеганографії?
2. За якими ознаками класифікуються методи комп'ютерної стеганографії.
3. Дайте характеристику сурогатним, селективним та конструювальним методам.
4. Дайте характеристику потоковим методам та методам з довільним доступом.
5. Дайте характеристику систематичним та несистематичним методам.
6. Дайте характеристику цифровим та структурним методам.
7. Назвіть методи, які зустрічаються в сучасних лінгвістичних стеганографах.

8. Які існують методи приховування даних шляхом зміни формату текстових файлів?

9. Які існують синтаксичні та семантичні методи лінгвістичної стеганографії?

10. Наведіть методи генерації стеганограм.

11. Дайте визначення функції імітації.

12. Дайте характеристику типів функції подібності.

13. Яку природу може мати надлишковість візуального середовища?

14. Які існують методи заміни?

15. Які ви знаєте методи приховування в частотній області зображення?

16. В чому полягає суть широкосмугових методів?

17. Які існують способи розширення спектру для приховування інформації?

18. Наведіть статистичні методи приховування даних.

19. Назвіть причини, з яких статистичні методи важко застосувати на практиці.

20. Охарактеризуйте методи перекручування інформації.

21. Назвіть етапи стеганографічного перетворення у структурних методах.

22. Які існують методи захисту даних у звуковому середовищі?

23. На чому базуються музичні стегосистеми?

РОЗДІЛ 4 ПРИХОВАНІ КАНАЛИ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Предметом досліджень стеганографії є також проблеми, які пов'язані зі створенням, виявленням і використанням прихованих каналів. Вперше на формальному рівні проблема передавання інформації прихованими каналами була розглянута *Сімонсом* у задачі про тюремника [9]. Подальші дослідження показали, що механізм прихованого каналу є універсальним засобом – з його допомогою можна як забезпечити традиційне приховане передавання захищуваної інформації, так і створити приховані канали витоку [51].

4.1 Деякі приклади організації прихованих каналів

4.1.1 Приховування даних у невикористаних і зарезервованих полях

Використання зарезервованого простору в форматах зберігання і передавання даних дозволяє приховувати додаткову інформацію без порушення функціонування обчислювального процесу.

Наприклад, в операційних системах під час зберігання файлів зазвичай утворюється простір, що не використовується. Так, наприклад, у вінчестерах, відформатованих в операційній системі Windows/95 як FAT16, розмір кластера зазвичай дорівнює 32 кілобайтам. Це означає, що мінімальний розмір пам'яті, відведеної для файлу, дорівнює 32 Кбайтам, навіть якщо сам файл має розмір у 1 Кбайт. Таким чином, усе невикористане місце може бути відведено для приховування додаткової інформації без відображення цього факту в системних каталогах.

Приховане збереження додаткової інформації можна також здійснювати в невикористаному просторі заголовків файлів зображення і звуку.

Інший метод приховування інформації у файлових системах полягає у створенні прихованих розділів, яких не буде видно при звичайному запуску системи. При цьому відсутні будь-які ознаки існування файлу в системі. Доступ до таких файлів надається тільки у випадку, якщо користувач знає пароль та ім'я файлу [56].

Нарешті, приховані канали передавання повідомлень можна організувати в мережних протоколах TCP/IP. Це обумовлено тим, що

заголовки пакетів TCP/IP мають зарезервовані поля (шість невикористаних бітів у заголовку пакету TCP і два - у заголовку пакету IP).

4.1.2 Приховані канали в операційних системах

Якщо два партнери мають доступ до одного комп'ютера або ініціювали одночасно виконання двох процесів в одній обчислювальній системі, то є безліч способів для створення прихованого каналу зв'язку.

При розробці операційних систем завжди ретельно досліджуються можливі канали витоків чутливої інформації через так звані «діри» для того, щоб перекрити непередбачені можливості передавання даних з більш захищених частин системної області до менш захищених. У нашому випадку канал зв'язку буде вважатися прихованим, якщо він спеціально для цього ніколи не розроблявся, а використовує для передавання інформації об'єкти в незвичній якості.

В операційній системі приховані канали можуть виникати у випадку, коли одна частина загальнодоступного ресурсу (тієї ж операційної системи), яка використовується на одному рівні безпеки, здатна передати інформацію іншій системній частині, що обслуговує інший рівень.

Розглянемо такий приклад. Нехай в операційній системі процес *A* функціонує на більш високому рівні безпеки і може записувати дані на диск. Інший процес *B*, який працює на більш низькому рівні безпеки, може звертатися до таблиці файлів (наприклад, до імен і розмірів усіх файлів, які створені іншим процесом). Таку ситуацію можна використовувати для організації прихованого каналу в такий спосіб: процес *A*, шляхом вибору відповідних імен файлів і їхніх розмірів, може пересилати інформацію процесові *B*.

Аналогічно, як прихований канал передавання даних можна застосувати файлову систему Linux, кодуючи інформацію за допомогою кількості файлів у каталогах.

Маються також більш тонкі можливості. Наприклад, тимчасові мітки IP-пакету можуть використовуватися для передавання одного біта даних у такий спосіб: пакети, відіслані в парний відлік часу, представляють логічний нуль, а в непарний – одиницю.

4.1.3 Приховування даних у виконуваних файлах

Завантажувальні файли програм мають велику надлишковість, яка закладена в послідовності виконання незалежних ланцюжків команд. Для

захисту алгоритму програми від його відновлення хакерами застосовують спеціальні методи зміни коду програми. Такі методи перетворять програму P у функціонально еквівалентну програму P', яка є більш складною для аналізу хакерами.

Однак такі ж методи можна використовувати для приховування додаткової інформації у виконуваних файлах програм. У цьому випадку секретна інформація може приховуватися в послідовності виконуваних перетворень завантажувального коду програми. При цьому повинна виконуватися єдина вимога – користувач не повинен помітити змін у поведінці програми. Тобто, якщо $P \rightarrow P'$ є перетворенням вихідної програми P у стеганопрограму P', то результат P' повинен цілком збігатися з результатом програми P.

Відомі численні методи приховування інформації в тілі програми. Для цього використовуються перетворення типу вставлення переходу (додаткового переходу до функціонально еквівалентного блоку команд), вставлення в цикл додаткової умови та ін.

Процес приховування секретних даних у програмному середовищі можна також автоматизувати за допомогою всіляких систем генерації програм і звітів [57].

4.2 Організація прихованих каналів криптографічними засобами

Можливості стеганографії дозволяють створювати приховані канали передавання інформації в діючих криптосистемах, що сприяє створенню каналів витоку ключових даних і може зруйнувати систему захисту в цілому. Внаслідок цього виявлення і дослідження можливих прихованих каналів у реально діючих системах криптографічного захисту інформації є актуальним.

Необхідно визнати, що сформовані в даний час умови дозволяють істотно знизити імовірність виявлення факту застосування стеганопрограм для організації прихованого каналу передавання інформації. Подібний висновок базується на таких роздумах. По-перше, очевидно, що приховати факт використання специфічної програми можна за допомогою маскування під іншу програму, алгоритм якої широко використовується іншими користувачами. По-друге, така можливість реальна, оскільки в ряді міжнародних стандартів плануються до використання різні

криптопротоколи для узгодження і передавання ключів, а також механізми цифрового підпису.

Використання криптопротоколів для прихованого передавання інформації є природним у тому розумінні, що прихована інформація маскується одночасним вирішенням задачі, властивої даному протоколу. Недоліком такого підходу є коротка довжина прихованого повідомлення, яке можна передати за один сеанс, що обумовлено параметрами цифрового підпису а також з умовами використання секретних ключів для організації прихованого каналу зв'язку.

Розглянемо кілька прикладів створення прихованих каналів у криптографічних системах.

I. Один з можливих способів організації прихованого каналу криптографічними засобами базується на залежності результату C_i функції шифрування E від приховуваної інформації t_i: $E(M,t_i)\to C_i$. Причому функція розшифрування D, незалежно від t_i, повинна відображати будь-яку отриману криптограму C_i у вихідне повідомлення, тобто $D(C_i)\to M$ для будь-якого i. У цьому випадку, витягання прихованої інформації t_i відбувається шляхом порівняння прийнятої криптограми C_i з множиною можливих криптограм $\{C_i\}$.

Наприклад, нехай число $n=pqr$ – добуток простих чисел p, q і r, причому $p\equiv 3 mod 4$, $q\equiv 3 mod 4$, $r\equiv 5 mod 8$, а n – досить велике для того, щоб його легко можна було розкласти на прості множники. Відомо, що під час відомого розкладання числа n на множники визначення кореня порівняння проводиться за поліноміальний час. У той же час задача визначення квадратичного кореня в кільці лишків R_n еквівалентна за складністю задачі розкладання великого числа n на прості множники. Будь-який квадратичний лишок x^2 у кільці R_n за модулем n, де $(x^2, n)=1$, має вісім коренів у вигляді $x = \pm\alpha qr \pm \beta pr \pm \gamma pq$.

Процес передавання інформації виглядає таким чином (рис. 4.1). Вибирається повідомлення $M= x^2 \bmod n$, і для нього обчислюються всі корені. У залежності від прихованої інформації каналом передається один з коренів. На приймальній стороні основне повідомлення M легко визначається простим піднесенням до квадрату отриманої криптограми.

Інформація прихованого каналу може бути відновлена після порівняння криптограми з усіма можливими числами $\sqrt{M}$.

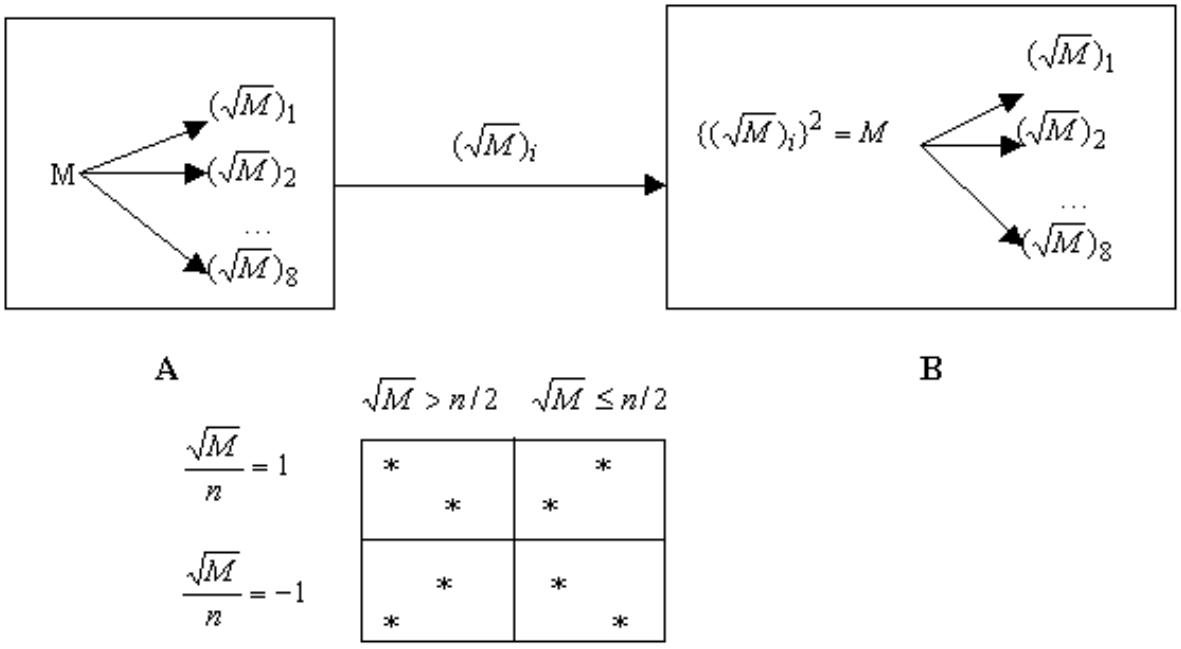


Рисунок 4.1 – Приклад прихованого каналу в кільці лишків R_n

Сторонній спостерігач, без знання розкладання числа *n* на множники, не зможе змінити криптограму, не зруйнувавши при цьому прихований канал.

II. Інший приклад створення прихованого каналу грунтується на можливості довільно вибирати деякі значення параметрів криптографічних перетворень. Такий вибір можна поставити у певну залежність від приховуваних даних. Відзначимо, що випадковий вибір параметрів криптосистеми зазвичай є тим «слабким місцем», через яке реалізуються різного виду «лазівки».

Розглянемо приклад організації прихованого каналу за допомогою схеми цифрового підпису Ель Гамаля.

Нагадаємо, що для генерації ключів за схемою Ель Гамаля, необхідно вибрати просте число *p*, $g \in Z_p^*$ і випадкове число $x<p$. Після цього обчислюється $y=g^x \ mod \ p$. Відкритим ключем користувача буде трійка чисел $\{y,g,p\}$, а секретним – *x*. Щоб підписати повідомлення *m* користувач спочатку вибирає таке випадкове число *k*, яке є взаємно простим до числа (p-1). Потім обчислює значення $a \equiv g^k \bmod p$ і розв'язує тотожність $M \equiv xa+kb \bmod(p-1)$ для *b*. У цьому випадку цифровим підписом є пара чисел *a* і *b*.

Для перевірки підпису необхідно переконатися у справедливості співвідношення $y^a a^b \equiv q^M \bmod p$.

Для приховання секретної інформації в цифровому підписі одержувач повинен мати доступ до секретного ключа відправника x. Щоб надіслати додатково секретні дані M' разом з деяким відкритим повідомленням M, необхідно як випадкове число k у схемі Ель Гамаля використовувати значення M'. Тобто, обчислюється значення $a=g^{M'} \bmod p$ і розв'язується співвідношення $M \equiv xa+M'b \bmod(p\text{-}1)$ для b. Підписом, як і вище, буде пара чисел a і b. Якщо одержувач знає значення x, то він зможе відновити M', використовуючи алгоритм Евкліда.

III. У [28] показано, що розглянуті вище можливості, які властиві класичним підписам типу Ель Гамаля, зберігаються і для їхніх аналогів на еліптичних кривих. Це дозволяє легко організувати прихований канал.

Нагадаємо, що відповідні криптографічні перетворення використовують властивості групи точок на еліптичній кривій над полем $F=GF(p^m)$. У групу точок $E=E(F)$ на еліптичній кривій над полем F входять пари $P=(x,y)\in F\times F$, які є розв'язком деяких рівнянь [52]. Такі пари називаються кінцевими точками кривої. Множина кінцевих точок еліптичної кривої розширюється до абелевої групи E, якщо приєднати особливий елемент, який називається нескінченно віддаленою точкою O. Кількість елементів групи E позначається через $\#E$. Нескінченно віддалена точка є нейтральним елементом групи і не має представлення у вигляді пари координат, які задовольняють дане рівняння.

Для побудови схеми цифрового підпису (ЦП) необхідно так вибрати еліптичну криву, щоб число $\#E$ містило простий дільник $n>4\sqrt{p^m}$. Крім того, необхідно визначити на кривій точку $G=G(x,y)$, порядок якої в групі E дорівнює n. Розмір двійкового представлення n зазвичай складає 180-400 бітів.

Механізм ЦП використовує властивості циклічної підгрупи $E(G)\subset E$ з елементами виду $G_0=G$, $G_1=G+G$, $G_2=G+G+G$ і т.д. Якщо записувати подібне *k-кратне* додавання на кривій у вигляді $[k]G$, поклавши $[0]G=0$, то коефіцієнт k можна подавати за модулем n і розглядати вираз у вигляді $[u]P+[v]Q$ і $[u]([v]P)$. Операція $[k]G$ називається скалярним множенням на k. В еліптичних аналогах цифрового підпису секретний і відкритий ключі підпису являють собою, відповідно, псевдовипадкове число $d\in[1,n\text{-}1]$ і точку кривої вигляду $P=[d]G$. Підпис являє собою пару чисел (R,S), які

зв’язані з координатами точки $[k]G$ (де k – псевдовипадковий параметр), секретним ключем підпису та один з одним. Друга частина підпису S залежить від підписуваного повідомлення M, наприклад, через функцію хешування: $H=H(M)$. Специфікою еліптичних кривих обумовлене застосування перетворення $G\to\pi(G)$ точки на кривій у ціле число. Це перетворення є функцією від координат точки G, наприклад, хеш-функцією від її першої координати. Крім того, використовуються додаткові параметри, пов’язані з реалізацією заходів проти використання як точки G елемента (іншої) підгрупи кривої малого порядку. Відповідна процедура основана на використанні так званого кофактора $c=\#E/n$ як додаткового множника для точок вигляду $[k]G$.

Для початку розглянемо можливість прихованого передавання даних за допомогою механізму накладення цифрового підпису.

Нехай $(d,P=d)$ – ключова пара власника підпису для криптосистеми на еліптичних кривих, n – порядок базової точки G. Вибираємо псевдовипадкове число $k\in[1,n-1]$ і обчислюємо точку $[k]G=(x,y)$ на еліптичній кривій. Зашифровуємо значення $H=H(M)$ за допомогою першої координати точки $[k]G$ додаванням за модулем n, отримуємо значення першої частини підпису $R=(H+x) \bmod n$. Друга частина підпису дорівнює $S=(k-d)\bmod n$.

Розглянемо випадок, коли обом абонентам відомий секретний ключ цифрового підпису d. Скористаємося тим, що при знанні ключа d у підписах типу Ель Гамаля параметр k може бути визначений з S. Нагадаємо, що, крім того, при перевірці підпису одержувач завжди має можливість явно отримати точку $[k]G$. Припустимо, що між абонентами A і B існує лінія зв’язку, якою передаються повідомлення з цифровим підписом. Припустимо, що між абонентами погоджений деякий довгостроковий ключ $K\in GF(n)$. Нехай необхідно передати повідомлення $M^*\neq 0$ прихованим каналом від A до B, забезпечивши автентичність джерела.

Спочатку абонент A формує повідомлення $M=M^*\|r$, де r – псевдовипадкове число (розміром, скажімо, 80 бітів) і визначає число k з рівності $M=Kk$ (операції розглядаються в полі $GF(n)$). Далі A вибирає довільне повідомлення $M_1\neq 0$, $M_1\neq M$, обчислює його цифровий підпис (R,S) і відправляє абонентові B підписане повідомлення. Абонент B перевіряє ЦП, переконується в автентичності джерела повідомлення і, знаючи ключ

d, визначає з S параметр k. Потім, використовуючи ключ K, обчислює повідомлення M. Використання параметра r необхідно для уникнення можливості підписання різних повідомлень M_1 тим самим значенням k під час повторного передавання M^*. У цьому випадку k і d можуть бути визначені двома підписами.

Розглянемо ситуацію, коли значення d одержувачу невідомо. У цьому випадку для передавання одного біта можна використовувати передавання одного повідомлення. Дійсно, вибираючи k псевдовипадковим чином, можна домогтися того, щоб черговий біт повідомлення M^* збігся, скажімо, з останнім бітом числа $\pi([Kk]G)$. Оскільки під час перевірки підпису легко обчислити точку $[K][k]G=[Kk]G$, то одержувач у змозі прийняти біт, переданий прихованим каналом.

Можна ускладнити вибір k, вимагаючи, щоб наступні декілька бітів повідомлення M^* збігалися з числом $\pi([Kk]G) \bmod t$ для невеликого простого числа t. Таким чином, перевага в обчислювальній потужності приводить до кращої якості прихованого каналу.

Тепер розглянемо можливу організацію прихованого каналу в механізмі пересилання ключів типу Ель Гамаля, в якому використовується кофактор c і додатковий параметр v та забезпечується однопрохідний протокол пересилання ключа K від абонента A до абонента B.

Для автентифікації ключа K абоненти використовують алгоритм обчислення коду автентифікації повідомлень (MAC). Для цього алгоритму формується свій псевдовипадковий ключ K_1. Крім того, для перешифрування ключа K формується блок Z гамми за модулем два. Ключі K_1 і Z формуються за допомогою функції генерації похідних ключів (*kdf*), яка використовує значення інших аргументів, пов'язані з параметрами користувачів і параметрами алгоритму (MAC).

Нехай для абонентів з ідентифікаторами A і B ключові пари для криптосистем на еліптичних кривих відповідно рівні (d_1,P_1) і (d_2,P_2). Абонент A вибирає псевдовипадкове число $u \in \{1,\ldots,n-1\}$, обчислює точку uG і гамму $Z=kdf(\pi(uvcP_2,par1))$. Потім зашифровує ключ, що підлягає пересиланню: $D=(A||K)\oplus Z$, і виробляє проміжний ключ $K_1=kdf(\pi(uvcP_2,par2))$.

Пояснимо роль додаткових параметрів. При виборі $v=c^{-1} \bmod n$ загальний секретний параметр не залежить від кофактора і протокол доступний у рамках вихідної групи користувачів. Якщо $v=1$, то протокол

доступний тільки для користувачів, що використовують множення на кофактор. Крім того, якщо порядок точки G не дорівнює n, то $[c]G=0$, що дозволяє користувачеві знайти порушення протоколу.

Абонент A використовує K_1 для отримання коду автентифікації повідомлення $\mathrm{MAC}(K_1,D)$ і пересилає абонентові B повідомлення $M=D||uG||\mathrm{MAC}(K_1,D)$. Абонент B у змозі обчислити перший аргумент функції *kdf*, виходячи із секретного ключа d_2 і переданої йому точки uG, оскільки $uP_2=d_2uG$ і $\pi(uvcP_2)=\pi(uvcd_2G)$. Далі він знімає гамму Z, отримує D, перевіряє збігання ідентифікатора A з реальним ідентифікатором абонента, виробляє ключ $K_1=K(c,d_2,u,v)$ і обчислює заново $\mathrm{MAC}(K_1,D)$. Якщо значення знову обчисленого коду MAC збігається з кодом, що зберігається в M, то абонент B визнає ключ K істинним.

Таким чином, створений прихований канал зв'язку для випадку, коли використовується механізм множення на кофактор ($v=1$). Зазначимо, що використання кофактора в даному протоколі приводить до того, що виявлення порушення коректності перетворень у ході його виконання не є однозначно свідченням спроби несанкціонованих дій. З цієї причини некоректність перетворень, викликана використанням кофактора, для системи не є критичною.

Очевидно, при якісних криптографічних перетвореннях, задіяних для реалізації протоколу, можна вважати, що його коректне завершення практично достовірно свідчить про використання істинного значення кофактора. Іншими словами, стосовно кофактора абонент B володіє деяким перевірочним співвідношенням T. Таким чином, коректність криптопротоколу взаємно однозначно залежить від глобального (несекретного) параметра c. Виходячи з цього, приховане передавання повідомлення M^* від A до B (t бітів інформації) можна здійснити в такий спосіб.

Абоненти заздалегідь погоджують довгостроковий ключ Y (випадкове число, що не перевершує n), а також стеганографічний параметр W, який складається з t чисел, що вказують на номери різних розрядів у двійковому записі c. Для передавання даних абонент A, порозрядно, додаванням за модулем два, модифікує відповідними бітами повідомлення M^* розряди кофактора c, перераховані в списку W. Потім результат збільшується на Y. У підсумку виходить модифікований кофактор $c_1=Y(c\oplus M^*(W)) \bmod n$. Далі, при використанні протоколу пересилання ключа K, абонент A діє стандартно, за винятком того, що використовує

модифікований кофактор замість вихідного. Абонент B, виявляючи порушення коректності перетворень у ході протоколу, будує модифікований кофактор перебором, із критерієм істинності T. Потім обчислює $Y^{-1}c_1 \oplus c = M^*(W) \bmod n$. Оскільки реальні значення $t \approx 30$ нехтовно малі в порівнянні з n, то ключ K може бути прийнятий абонентом B практично з вихідною надійністю.

4.3 Поняття про клептографію

У даному пункті розглянемо приклад застосування концепції прихованого каналу стосовно до задачі контролю за застосуванням засобів криптографічного захисту інформації (КЗІ). Якщо необхідність застосування надійних засобів КЗІ для захисту державних і воєнних секретів ні в кого не викликає сумніву, то нерегламентоване їхнє застосування в недержавній сфері, особливо після проходження в усьому світі хвилі терористичних актів, створює ряд проблем.

Одна з них – складність державного контролю за шифрованою інформацією. У багатьох країнах з цією метою вводяться обмеження у використанні засобів КЗІ. Для цього в основному застосовуються механізми ліцензування, сертифікації та експортно-імпортних обмежень. Іншим підходом забезпечення контролю за шифрованою інформацією є концепція криптосистем з відновленням ключа (*key recovery system*). Відповідно до цієї концепції в засобах КЗІ передбачена наявність механізму, який забезпечує передавання копії ключа користувача для зберігання в офіційний орган – довіреній особі (*trusted third-party*). Цим забезпечується гарантований доступ правоохоронних органів до відкритої інформації для виконання контрольних функцій за фінансовою, комерційною та іншою діяльністю за постановами суду.

Таким чином, існує певна потреба в таких засобах криптографічного захисту інформації, які забезпечували б належний рівень безпеки захищуваної інформації і одночасно володіли б можливістю надійного розшифрування інформації у випадках, коли криптографічний ключ був загублений або існує потреба в проведенні контрольних заходів.

Вирішення даної проблеми можливо шляхом створення прихованих каналів передавання елементів ключової інформації. У [53-54] був запропонований підхід до побудови системи захищеного контролю криптографічних засобів захисту.

Припустимо, що криптографічна система задана як «чорний ящик», функціонування якого можна вивчити лише за вхідними та вихідними даними. Таке припущення має, наприклад, місце у випадку, коли виробник засобів КЗІ повідомляє про специфікацію свого виробу, але тримає в таємниці криптографічний алгоритм, або ж коли у виробах КЗІ вбудовані стандартні чіпи з набором криптографічних функцій, розроблені іншими виробниками.

Нехай криптографічна система S визначається кортежем: $S=<I,K,O>$, де I і O – вхід і вихід системи відповідно до її специфікації, K – ключова система. Розглянемо основні вимоги до вбудованого механізму захищеного контролю (МЗК) засобів КЗІ. Основною задачею МЗК є організація прихованого каналу передавання ключової та іншої чутливої інформації у вихідних даних системи S.

Припустимо, що МКЗ може проводити алгоритмічну модифікацію криптографічної системи M: $S \rightarrow S'$ таким чином, що:

$$S'=<I,E'/D',O'=f(O,K)>,$$

де I' і O' – відповідно, вхід і вихід МЗК; E' – асиметрична функція шифрування, яка належить розширенню S'; D' – функція розшифрування, яка відома лише контролюючому органу.

У цьому випадку для забезпечення необхідних властивостей МЗК повинен відповідати таким вимогам:

B1. Вхідні дані модифікованої системи S' повинні повністю збігатися з вхідними даними системи S.

B2. Система S' повинна шифрувати ключову інформацію за допомогою асиметричної функції E'.

B3. Функція розшифрування D' не входить до складу системи S' і відома лише контролюючому органу.

B4. Вихідні дані $O'=f(O,K)$ відповідають специфікації системи S і містять, окрім зашифрованої інформації користувача, додатково дані про використовуваний секретний ключ K.

B5. У випадку компрометації МЗК неможливо провести дезінформацію контролюючого органу.

У залежності від задач, які повинен забезпечувати МЗК, можуть висуватися додаткові вимоги. Наприклад, якщо буде потрібно забезпечити в таємниці від користувача факт наявності МЗК, то, скоріш за все, необхідно додатково вимагати:

B6. Пошук невідповідностей між виходами *O* та *O'* повинен бути NP-складною задачею для всіх, за винятком контролюючого органу.

У попередньому розділі були розглянуті деякі приклади організації прихованих каналів за допомогою криптографічних засобів, які відповідають вказаним вимогам і можуть забезпечити захищений контроль засобів КЗІ.

Створення різних засобів КЗІ не є самометою. Їхні споживчі властивості повинні відповідати кожному конкретному додатку. Внаслідок цього, засоби КЗІ з вбудованим механізмом контролю знайдуть свого споживача. Більш того, можна спрогнозувати, що для них можуть бути надані більш сприятливі умови на ринку засобів захисту.

Насамкінець слід відзначити, що якщо стеганографія як наука вивчає питання захисту конфіденційної інформації від несанкціонованого доступу під час її передавання або зберігання, то розглянуте у даному розділі питання створення МЗК засобів КЗІ має зовсім інший аспект. Фактично вивчається питання щодо створення механізму відбору чутливої інформації у законного користувача з метою можливого відновлення зашифрованої інформації. Внаслідок цього питання розробки та пошуку прихованих механізмів контролю можна віднести до нового напрямку досліджень у рамках стеганографії – *клептографії*.

4.4 Питання для самоконтролю знань

1. Наведіть приклади приховування даних у невикористаних та зарезервованих полях.
2. Наведіть приклади прихованих каналів в операційних системах.
3. Наведіть приклади приховування даних у виконуваних файлах.
4. Які існують способи створення прихованих каналів у криптографічних системах?
5. Які існують приклади організації прихованого каналу за допомогою механізму накладання цифрового підпису?
6. Наведіть приклад організації прихованого каналу на основі схеми Ель Гамаля.
7. Які існують способи створення прихованого каналу на основі еліптичних кривих?

8. Як створюється прихований канал зв’язку, використовуючи механізм множення на кофактор?

9. Які існують підходи забезпечення контролю за шифрованою інформацією?

10. В чому полягає концепція криптосистем з відновленням ключа?

11. Які існують підходи до створення прихованих каналів передавання елементів ключової інформації?

12. Назвіть основні вимоги до вбудованого механізму захищеного контролю засобів КЗІ.

13. Що таке клептографія?

РОЗДІЛ 5 ЦИФРОВІ ВОДЯНІ ЗНАКИ

Інтернет уже насичений усілякою графічною, відео-, звуковою інформацією. Росте пропускна здатність каналів, удосконалюються потокові технології, все аналогове переводиться в «цифру» або створюється відразу в «цифрі». При постійному вдосконаленні ефективності аудіо- і відео-кодеків стає очевидною можливість широкого продажу оцифрованих та ущільнених даних через Інтернет. Природно, що в кожному витворі є свій автор-правовласник, для багатьох з яких актуальною стає проблема захисту від піратства, а точніше роялті – відрахування на користь автора або правовласника. У сформованих умовах проблема захисту авторського права стає особливо актуальною, тому що в сфері створення і використання мультимедійних даних повсюдно відзначається його порушення. І це незважаючи на те, що діє відповідне законодавство і технічні методи захисту прав автора.

Для вирішення вказаної проблеми останнім часом стали активно застосовувати цифрові водяні знаки.

Мистецтво створення водяних знаків на папері народилося в Італії більш ніж 700 років тому. У середні віки наявність водяних знаків була гарантом якості паперу; пізніше їх стали використовувати для автентифікації документів з метою захисту від підробки. За аналогією, стосовно до цифрових даних став застосовуватися термін «*цифрові водяні знаки»* (*digital watermark*), вивчення яких сформувалося в окремий науковий напрям у рамках стеганографії.

Предметом вивчення цифрових водяних знаків (ЦВЗ) є можливості маркування мультимедійної інформації з метою її ідентифікації, автентифікації, а також моніторингу її поширення і копіювання. Теоретичним фундаментом технологій цифрових водяних знаків є стеганографія.

Цифровий водяний знак являє собою деяку інформацію, яка додається до цифрового об’єкта і може бути пізніше виявлена або витягнена для висування прав на цей об’єкт. Найчастіше як об’єкт, що охороняється, виступають музичні твори, оцифрована відео- та комп’ютерна графіка.

У системах з цифровими водяними знаками (ЦВЗ), так само як і в стеганографії, застосовуються методи, за допомогою яких одні дані приховуються в інших. Але, на відміну від стеганографії, цифрові водяні знаки захищають сам носій (тобто контейнер). ЦВЗ містять спеціальну

інформацію (про час і місце його створення, про авторські права та ін.) і можуть бути розпізнані лише спеціальними засобами.

Терміни «*відбиток пальця*» і «*маркування*» позначають спеціальні застосування технології цифрових водяних знаків, згідно з якими дані про творця або одержувача цифрових даних вносяться у вигляді ЦВЗ в захищувану інформацію. Процедура реєстрації відбитка пальця означає проставлення водяних знаків з унікальним кодом, а маркування цифрового об'єкта передбачає внесення ЦВЗ із будь-якою необхідною інформацією.

Рисунок 5.1 – Зразок видимого водяного знака

Основна вимога до систем цифрових водяних знаків – це стійкість цифрової мітки до різноманітних трансформацій файлу-носія (зміни формату, ущільнення, аналогового перетворення, цифрових обробок) та до спроб її видалення третіми особами (тобто ворожими піратами-хакерами). Іноді не менш важливою вимогою є невидимість (або нечутність) мітки. Цифрові водяні знаки можуть бути настільки стійкими, що зберігаються після кількаразових перетворень форматів зображень і можуть бути виявлені навіть після сканування типографського офсетного відбитка.

Відзначимо деякі існуючі особливості термінології.

Видимі водяні знаки (як правило такі, що збігаються з офіційним легко пізнаваним товарним знаком фірми) – це візуальні зразки, які вставляються в цифрові дані (або записуються поверх них). Вони дуже схожі на водяні

знаки для паперу (рис. 5.1) і застосовуються головним чином у зображеннях і відео. Такі знаки використовуються для видимого «перекручування» цифрового об'єкта і можуть, наприклад, видалятися після придбання цифрового об'єкта.

Напіввидимі водяні знаки – це мітки, які проставляються в цифрових об'єктах, не заважаючи сприйняттю, але у певних умовах можуть проявитися. Це може бути текстовий файл з інформацією про автора або правовласника, який з'являється на екрані через якийсь час після того, як курсор зависне над зображенням або після спроби скопіювати зображення натисканням правої кнопки миші.

Невидимі цифрові водяні знаки не призначені для загального огляду і використовуються для полегшення роботи вузько спеціалізованих пошукових «павуків», запрограмованих конкретним хазяїном для пошуку саме свого знаку серед безлічі цифрових об'єктів, розміщених в Інтернеті. У ряді випадків такий пошук дозволяє з'ясувати адреси сторінок, на яких цифрові об'єкти виставлені без дозволу автора. Невидимі цифрові водяні знаки є найкращим рішенням для створення потенційної загрози можливого в майбутньому переслідування порушників виняткових авторських прав.

Крихкі водяні знаки – це знаки, які мають дуже обмежену стійкість до будь-яких змін. Вони найчастіше використовуються для виявлення модифікацій маркірованих цифрових об'єктів.

Уже зараз будь-якому користувачеві доступні програмні засоби для забезпечення захисту цифрових зображень за допомогою цифрового водяного знака. Як приклад розглянемо послідовність роботи з одним із них. У графічному редакторі Photoshop (а також у CorelDraw і PhotoPaint) присутнім є плагін Digimarc, який дозволяє вносити цифровий водяний знак практично у будь-який цифровий об'єкт, а також зчитувати його з файлів.

Процес використання технології цифрового водяного знака виглядає в такий спосіб. Після створення графічного зображення автор звертається на сайт компанії Digimarc і отримує свій унікальний ідентифікатор Digimarc ID. Потім у графічному редакторі за допомогою модуля PictureMarc автор вводить інформацію і вносить цифровий водяний знак у зображення. Це дає можливість навіть при перекручуванні зображення (не до невпізнанності, звичайно) розпізнати за допомогою того ж PictureMarc унікальний ідентифікатор автора. До того ж, якщо встановити додатковий

сервіс, кожна така картинка буде прямим посиланням на інтернет-сайт автора.

Сьогодні існує безліч невирішених проблем в галузі цифрових водяних знаків і практично відсутня теоретична основа створення систем ЦВЗ. Незважаючи на це, у даний час інтерес до технологій водяних знаків надзвичайно високий. Науковий інтерес відбивається в стрімкому зростанні кількості публікацій і кількості проведених міжнародних конференцій. Інтерес промисловості до водяних знаків стимулює розробку стандартних рішень. Наприклад, у проекті TALISMAN [45], який фінансується Європейським економічним співтовариством, розробляється стандартний механізм маркування водяними знаками цифрових виробів. Передбачається, що система TALISMAN буде сприяти боротьбі проти великомасштабного комерційного піратства і незаконного копіювання. Міжнародні організації зі стандартизації також зацікавлені в технологіях ЦВЗ. Розроблено стандарт ущільнення відеосигналу MPEG-4 (ISO/IEC 14496), в якому передбачено одночасне використання процесів шифрування і проставлення водяних знаків. Промисловий стандарт DVD передбачає вбудовування механізму захисту від несанкціонованого копіювання на основі цифрових водяних знаків. Інтенсивно також розробляється юридична база, яка буде регламентувати всі аспекти, пов’язані із застосуванням водяних знаків для захисту інтелектуальної власності.

5.1 Приклади використання цифрових водяних знаків

В даний час цифрові водяні знаки розглядаються як найбільш перспективна технологія під час вирішення проблеми захисту прав власності та ідентифікації цифрових об’єктів мультимедіа (аудіо, зображення і відео).

Розглянемо деякі приклади можливого використання систем цифрових водяних знаків.

1. *Проблема захисту авторських прав* на інформацію, яка представлена в цифровому вигляді. В даний час це найбільш важливе застосування систем ЦВЗ. У цьому випадку водяні знаки містять інформацію про законного власника, що дозволяє запобігти зазіханню інших осіб на права власності захищуваних даних. Перелічимо ті функціональні можливості,

які повинна забезпечувати «ідеальна» електронна система захисту авторських прав:

– виявлення, запобігання та облік різних операцій, які проводяться з цифровими об’єктами (відкриття, друкування, завантаження, копіювання, зміна і т.д.);

– реєстрація статусу доступу до цифрових об’єктів і суб’єкта, що визначив цей статус;

– фіксація користувачів, які читали, копіювали або друкували цифровий об’єкт;

– відправлення повідомлення власникові авторських прав з попередженням про завершення оплаченого терміну його прав на цифровий об’єкт.

2. *Системи захисту від несанкціонованого копіювання*. Для них застосовуються ЦВЗ, які вказують на статус цифрової копії (чи можна її копіювати). Наприклад, стандартний плеєр DVD не дозволяє магнітофонові програвати або копіювати дані, які позначені водяним знаком «копіювати заборонено»; дані, які позначені знаком «можна зняти лише одну копію», можуть бути скопійовані один раз, але надалі ні однієї копії не можна буде зробити. Захист від копіювання дуже важко реалізувати у відкритих системах, але в закритих або спеціалізованих системах це цілком здійсненно.

3. *Автентифікація цифрових даних*. ЦВЗ можна використовувати для автентифікації даних і виявлення їхньої можливої модифікації. Для цього застосовуються водяні знаки, які мають низьку завадостійкість тільки до деяких видів перетворень (наприклад, ущільнення), стійкі до інших перекручувань і модифікацій. У даних системах вимоги до завадостійкості водяних знаків найнижчі, оскільки за фактом руйнування вбудованого водяного знака і приймається рішення про автентичність цифрового об’єкта.

4. *Моніторинг інформаційних потоків*. Іноді виникає необхідність у здійсненні контролю за циркулюючою в мережах інформацією або у виявленні фактів незаконного виготовлення і поширення копій цифрових даних (наприклад, програмних продуктів). У таких випадках у кожну легальну копію цифрових даних вносяться різні водяні знаки.

5.2 Узагальнена модель системи цифрових водяних знаків

Як правило, усі системи цифрових водяних знаків мають два типових блоки (рис.5.2): схему внесення водяного знака і схему пошуку/витягання водяного знака.

Вхідною інформацією для схеми внесення водяного знака є цифровий об'єкт *I*, водяний знак *W* і стегоключ *K* (необов'язковий параметр). Водяний знак *W* може мати будь-який вигляд: число, текст, зображення та ін. Практично в усіх системах ЦВЗ передбачена наявність одного або навіть декількох стегоключів, які необхідні для захисту водяних знаків від несанкціонованих змін. Виходом системи є цифровий об'єкт з вбудованим водяним знаком.

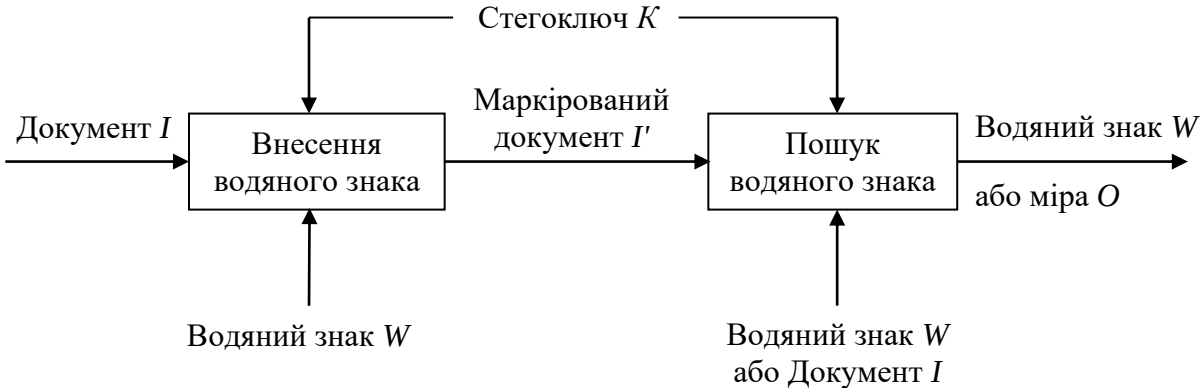


Рисунок 5.2 – Узагальнена схема системи ЦВЗ

Вихідними даними для процесу пошуку і/або видалення водяного знака є: цифровий об'єкт $\bar{I}'$ з водяним знаком (можливо, випадково або навмисно перекручений), стегоключ *K* і, в залежності від реалізованого методу, оригінальні копії даних *I* та/або водяного знака *W*. Результатом роботи схеми є витягнений водяний знак *W* або деяка оцінка *O*, за якою можна судити про ймовірне існування знака *W* в об'єкті $\bar{I}'$.

Подібна структура систем водяних знаків характерна для усіх видів цифрових даних: аудіо, зображень, відео, форматованих текстів, тривимірних моделей, параметрів мультиплікаційних моделей та ін.

5.3 Класифікація систем цифрових водяних знаків

Загальний процес маркування цифрового об'єкта водяними знаками може бути визначений як відображення такого вигляду: $I \times K \times W \to \hat{I}$, де I – вихідний цифровий об'єкт, W – водяний знак, K – стегоключ, $\hat{I}$ – маркований цифровий об'єкт. Результатом роботи схеми детектування ЦВЗ може бути або витягнений водяний знак W, або деяка оцінка O, яка вказує на ймовірність того, що об'єкт $\hat{I}$ є промаркірованим.

Можна виділити декілька типів систем цифрових водяних знаків [29].

– *Конфіденційні системи ЦВЗ* вимагають, принаймні, наявності вихідних даних I. Існують дві модифікації подібних систем. Перша з них використовує вихідне зображення як підказку для витягання водяного знака W у цифрових, можливо перекручених, даних $\hat{I}$. Функціонування таких систем можна описати як: $\hat{I} \times I \times K \to W$. Друга –тільки дає відповідь «так» або «ні» на питання: «чи міститься в зображенні водяний знак W?», а також вимагає ще копію внесеного водяного знака: $\hat{I} \times I \times K \times W \to \{0,1\}$. Вважається, що такі системи є найбільш завадостійкими до будь-яких атак, тому що вимагають наявності секретного стегоключа K і видають мінімум інформації.

– *Напівконфіденційні системи ЦВЗ* не вимагають вихідної копії об'єкта для виявлення водяного знака W. Схему їхньої роботи можна представити як: $\bar{I}' \times K \times W \to \{0,1\}$.

– *Напіввідкриті системи ЦВЗ* використовують стегоключ (або іншу додаткову інформацію для виявлення водяного знака), який залежить від вихідної копії даних: $\bar{I}' \times K(I) \to W$.

– *Відкриті системи ЦВЗ* для своєї роботи не вимагають знання ні оригінальної копії даних I, ні вбудованого водяного знака W. Такі системи витягають водяний знак з маркірованих даних: $\bar{I}' \times K \to W$.

Більшість реально діючих систем ЦВЗ відноситься до конфіденційного або напівконфіденційного типу. Але найбільший інтерес для сучасних досліджень представляють відкриті системи цифрових водяних знаків.

5.4 Вимоги до систем цифрових водяних знаків

У системах цифрових водяних знаків повинні враховуватися, принаймні, такі аспекти:

– завадостійкість водяного знака до випадкових перекручувань і навмисних атак – найважливіша характеристика, від якої залежать споживчі властивості системи;

– обов'язкове використання стегоключів для гарантованого захисту водяних знаків від навмисних перекручувань і видалень;

– оптимальний поріг «видимості» водяного знака – параметр, який характеризує припустимий рівень внесених водяним знаком перекручувань (на цьому параметрі базуються основні критерії й оцінки);

– відносний об'єм вносимої інформації – параметр, який залежить від характеру приховуваних даних (ідентифікатор, індекс або покажчик, відкритий текст, емблема та ін.) і від природи цифрового об'єкта (текст, зображення, відео, звук і т.д.). Під час внесення водяного знака великого об'єму знижується його завадостійкість до атак.

Непомітність водяних знаків є загальною вимогою для всіх систем ЦВЗ. Це означає, що перекручування, які вносяться водяними знаками, повинні залишатися нижче певного порогу «видимості». Водяні знаки повинні бути невидимими не тільки для простого користувача, але й для експертів, озброєних досконалими методами статистичного аналізу. Для забезпечення цієї вимоги повинні існувати деякі критерії оцінювання кількості допустимих перекручувань, що їх викликало внесення водяних знаків.

Забезпечення безпеки систем ЦВЗ за допомогою стегоключів. У системах водяних знаків виділяють два рівні безпеки. Вищий рівень безпеки не дозволяє несанкціонованому користувачеві знайти і виділити водяні знаки. Другий рівень дозволяє будь-якому користувачеві тільки виявляти факт присутності водяного знака, але інші дії з водяним знаком без знання ключа неможливі. Стегоключі відіграють важливу роль у захисті систем ЦВЗ від різного виду атак. Вимоги до системи керування ключами сильно залежать від застосувань, однак ключовий простір повинен бути достатньо великим для тотального перебору.

Можливість вирішення суперечок про право власності. У системі ЦВЗ повинні бути передбачені механізми визначення пріоритету проставлених водяних знаків у тому випадку, якщо в цифровому об'єкті їх знаходиться

декілька і від різних джерел. Це, наприклад, може бути досягнуто введенням конструктивних обмежень на водяні знаки (наприклад, умови незворотності ЦВЗ) або додаткових функціональних можливостей (наявності тимчасових міток).

Доступність вихідних даних. Під час пошуку та витягання водяних знаків, копії оригіналу об'єкта та/або водяного знака можуть бути або доступними, або недоступними. Якщо вони доступні, то зазвичай реалізується система, яка під час витягання водяного знака використовує оригінал цифрових даних *I*. Такі системи мають велику завадостійкість не тільки до шумоподібних перекручувань, але і до геометричних. Однак у деяких застосуваннях (наприклад, під час моніторингу інформації) доступ до вихідної копії неможливий, а в інших (відео з водяними знаками) це практично неможливо через великий об'єм оброблюваних даних. Якщо в ранніх системах ЦВЗ для витягання водяних знаків зазвичай була потрібна вихідна копія контейнера, то в даний час намітилася чітка тенденція розробки методів, у яких вона не потрібна.

Спосіб витягання і верифікації водяних знаків. Є два підходи до процесу внесення і відновлення ЦВЗ. Під час першого підходу вносимий водяний знак вибирається з деякого припустимого набору, а під час його витягання перевіряється належність відновленого знака до даного набору. Під час другого – водяний знак вноситься шляхом модуляції деякої випадкової послідовності символів, а під час витягання вбудовані символи відновлюються шляхом демодуляції.

Завадостійкість водяних знаків від можливих випадкових перекручувань та/або навмисних модифікацій є одною із ключових вимог до систем ЦВЗ. Під час проектування систем часто керуються таким принципом: будь-яка успішно проведена атака на цифровий об'єкт із водяними знаками повинна знецінити комерційне значення захищуваних даних. Дотепер ще не розроблено «ідеального» методу, який би забезпечив абсолютну захищеність водяних знаків. Тому практичні системи повинні прагнути до досягнення компромісу між такими суперечливими вимогами, як завадостійкість, невидимість та об'єм інформації у водяному знаку.

Стійкість водяного знака до видалення зазвичай визначається розрахунковим часом, який необхідно затратити тому, хто атакує, для вилучення вбудованого водяного знака або внесення в нього таких перекручувань, при яких його неможливо було б відновити. Саме такий

підхід використовувала міжнародна організація IFPI для формування вимог до стійкості водяних знаків у звукові:

– механізм введення водяних знаків не повинен впливати на якість звуку при відтворенні;

– необхідна наявність можливості відновлення водяного знака після різного виду перетворень (фільтрація, цифроаналогове перетворення з подальшим аналого-цифровим, 10% часове ущільнення-розширення, методи ущільнення даних типу MPEG, адитивний і мультиплікативний шум, викривлення частотної характеристики до 15dB, групові затримки часу та ін.);

– не повинно бути ніякого іншого способу видалення або зміни водяних знаків без істотного викривлення якості звуку;

– для рівня «сигнал/шум» не менш 20dB внесений сигнал повинен мати ширину смуги в 20 біт/сек незалежного від рівня і типу сигналу (мова, класична або поп-музика).

Аналогічні вимоги можна розробити для систем маркування фотознімків, відео і мультимедійних об’єктів.

Незалежно від того, яким перекручуванням (навмисним або випадковим) піддаються об’єкти з ЦВЗ, розрізняють дві групи перекручувань. До першої відносять перекручування, які можна розглядати як адитивний шум (атака руйнуванням). До другої – перекручування, які представляються як неузгодженість між водяним знаком і стегоключем (атака на синхронізацію). Можна виділити такі види перекручувань та атак:

– ущільнення з втратами (для зображень: JPEG; для відео: H.261, H.263, MPEG-2, MPEG-4; для аудіо: MPEG-2 аудіо, MP3, MPEG-4 аудіо, G.723);

– розширення смуги сигналу (збільшення різкості, додавання константи, корекція кольору);

– обробка даних (підрізання, відсікання, модифікація гістограми);

– адитивний і мультиплікативний шум (гаусів, однорідний та ін.);

– афінні перетворення (перенесення, обертання, масштабування);

– цифроаналогове та аналого-цифрове перетворення;

– застосування транскодерів (H.263→MPEG-2, GIF→JPEG);
– багаторазове застосування водяних знаків;
– лінійна і нелінійна фільтрація;
– статистичне усереднення;
– атака «змовою»;
– мозаїчні атаки.

5.5 Методи цифрових водяних знаків

Останнім часом розроблена достатня кількість методів ЦВЗ, що дозволяє провести їхню систематизацію і виділити найбільш характерні задачі:

– вибір місця розташування водяного знака;
– вибір простору для представлення зображення і водяних знаків;
– попереднє форматування водяного знака;
– спосіб внесення водяного знака в цифровий об’єкт.

Розглянемо більш докладно особливості їх реалізації в системах цифрових водяних знаків для зображень.

5.5.1 Вибір місця розташування водяного знака

Відповідно до принципу Кірхгофса, алгоритм внесення і витягання водяних знаків не повинний бути секретним, а доступ до водяного знака повинен бути обмежений. Цю умову можна виконати під час вибору місця розташування водяного знака, яке буде залежати від стегоключа. Від правильного вибору місця розташування водяного знака залежать також видимі перекручування в зображенні. Це обумовлено особливостями органів зору людини, чутливість яких змінюється відповідно до характеру текстури зображення. Розглянемо деякі прийоми вибору місця розташування водяних знаків.

Алгоритм Єралаш (*patchwork* [30]) дозволяє приховати в зображенні однобітовий водяний знак та отримати відповідь на питання: «чи знає користувач істинний стегоключ?». Ідея алгоритму базується на припущенні, що значення пікселів незалежні й однаково розподілені. При цьому секретний ключ використовується для ініціалізації генератора псевдовипадкових чисел, які вказують на ті місця в зображенні, куди

вноситься біт водяного знака. Під час випадкового вибору достатньо великої кількості пар бітів (a_i,b_i), справедливе співвідношення:

$$\mathrm{E}[S] = \sum_{i=1}^{n} \mathrm{E}[a_i] - \mathrm{E}[b_i] = 0.$$

Для внесення біта водяного знака необхідно, у відповідності зі стегоключем K_s, вибрати n пар пікселів $(a_i,b_i)_{i=1\ldots n}$, у яких значення яскравості змінюються в такий спосіб: $\tilde{a} = a_i + 1$, $\tilde{b} = b_i - 1$. Під час витягання водяного знака у відповідності зі стегоключем K_s вибираються n пар пікселів і обчислюється сума

$$S = \sum_{i=1}^{n} \tilde{a}_i - \tilde{b}_i .$$

Якщо у вибраних парах містився водяний знак, то сума S буде дорівнювати $2n$, в іншому випадку S приблизно дорівнює нулеві. Таким чином, тільки маючи істинний ключ можна дізнатися про правильне місце розташування водяного знака та отримати $S \approx 2n$.

Алгоритми з відкритим ключем для доступу до водяного знака [31]. Алгоритми, в яких для доступу до водяного знака необхідний секретний ключ, не дають можливості будь-якому користувачеві перевірити факт наявності водяного знака в цифровому об’єкті. Для усунення такого недоліку використовують принцип асиметричної криптографії. У таких алгоритмах стегоключ являє собою пару *<секретний ключ, відкритий ключ>*: для приховування водяного знака застосовується секретний стегоключ, а для перевірки – відкритий стегоключ.

Розглянемо приклад. Відомо, що для широкосмугових методів потрібна несуча випадкова послідовність S, яка модулює вихідний сигнал. Завдяки завадостійкості, властивої широкосмуговому кодуванню, існує можливість відновити вихідний сигнал без знання всієї послідовності S. В алгоритмах водяних знаків з відкритими ключами це можна зробити в такий спосіб: секретним стегоключем, відомим лише власникові цифрового об’єкта, можна обчислити всю послідовність S, тоді як відкритим ключем - тільки її частину $S^{\text{відкр}}$, але цієї частини буде достатньо для витягання водяного знака. На практиці, загальнодоступна послідовність $S^{\text{відкр}}$ представляє один біт з N бітів вихідної послідовності $S^{\text{вих}}$, тоді як всі інші біти вибираються випадковим чином:

$$S_i^{відкр} = \begin{cases} S_i^{вих} \quad з \quad ймовірністю \quad 1/N \\ random\{-1,1\} \quad в \quad інших \quad випадках \end{cases}$$

Алгоритми з передбачуванням [19]. Моделі з передбачуванням широко застосовуються в теорії зв'язку під час кодування джерела сигналів. Суть кодування з передбачуванням полягає в мінімізації помилки між передбачуваним та істинним значеннями сигналу і кодуванні цієї помилки таким способом, щоб математичне сподівання розподілу помилок було близьким до нуля з малою дисперсією. Для зображень характерна наявність сильної кореляції між сусідніми пікселами, тому алгоритми з передбачуванням знайшли своє застосування в системах з водяними знаками. Крім того, у таких алгоритмах враховуються психовізуальні особливості людини. Відомо, що візуальна система людини менш чутлива до текстури і границь зображень, що робить ці зони найбільш підходящими місцями для приховування водяного знака. З іншого боку, очі людини дуже чутливі до змін на ділянках зображення, де є однорідні значення. Тому такі зони непридатні для приховування водяних знаків. Вбудовування водяного сигналу відбувається так, щоб розподіл помилки неузгодженості не змінювався.

Алгоритми з передбачуванням часто використовуються в системах ЦВЗ, для яких не потрібно знання оригіналу зображення.

5.5.2 Вибір простору для представлення водяного знака

Перед вбудовуванням водяного знака цифрове зображення може бути попередньо представлене в частотній області. Розглянемо можливі види перетворень, використовувані в системах водяних знаків.

Дискретне перетворення Фур'є (ДПФ), яке широко використовується в цифровій обробці сигналів, застосовується також під час внесення водяних знаків у зображення, представлене в частотній області. Це дозволяє оптимально вибрати ті частини зображення, куди можна помістити водяний знак для досягнення кращого співвідношення між видимістю та завадостійкістю. У системах ЦВЗ дискретне перетворення Фур'є використовується для фазової модуляції під час вбудовування водяного знака в цифровий об'єкт. Однак найчастіше це перетворення застосовується для отримання дискретного косинусного перетворення або в перетвореннях Меліна-Фур'є.

Дискретне косинусне перетворення (ДКП) широко застосовується в системах ЦВЗ із ряду причин: водяні знаки більш стійкі до ущільнення; існують відпрацьовані методики оцінювання впливу вбудованих знаків на видимі перекручування зображення; процес вбудовування водяних знаків за допомогою ДКП легко реалізується апаратно усередині сучасних кодерів JPEG або MPEG. Існує кілька варіантів використання дискретного косинусного перетворення під час внесення водяного знака:

– додавання відповідних коефіцієнтів ДКП зображення і водяного знака [32];

– облік значень бітів водяного знака в множниках коефіцієнтів ДКП [33];

– зміна квантування коефіцієнтів ДКП відповідно до бітів вбудовуваного водяного знака [19].

Перетворення Меліна-Фур'є (ПМФ) [34]**.** У багатьох алгоритмах ЦВЗ виникає проблема з виділенням водяних знаків із зображень, які піддалися афінним геометричним перетворенням. У зв'язку з цим, у системах ЦВЗ часто застосовують перетворення Меліна-Фур'є, яке використовує властивість перетворення Фур'є змінювати тільки фазу: $F(x_1+a,x_2+b)\leftrightarrow F(k_1,k_2)\exp[-i(ak_1+bk_2)]$. Таким чином, якщо водяний знак буде приховуватися в амплітуді перетворення Фур'є, то він буде нечутливий до просторових зсувів зображення. Для того, щоб водяні знаки були нечутливі також до обертання зображення і зміни його масштабу, використовується також полярно-логарифмічне відображення:

$$(x, y) \mapsto \begin{cases} x = \exp\rho\cos\theta \\ y = \exp\rho\sin\theta \end{cases}, \text{ де } \rho\in\boldsymbol{R} \text{ і } \theta\in[0,2\pi].$$

Відповідно до цього співвідношення, обертання будь-якого елемента *(x,y)* у декартовій системі координат можна представити перетворенням у логарифмічній системі координат. Аналогічно, масштабування зображення можна представити перетворенням у полярній системі координат (рис.5.3). Під час використання адекватної модифікації системи координат, операції обертання і масштабування можуть бути скорочені. Таким чином, властивість інваріантості перетворення можна використовувати для побудови простору, нечутливого до таких операцій над промаркірованими зображеннями, як обертання або зміна масштабу.

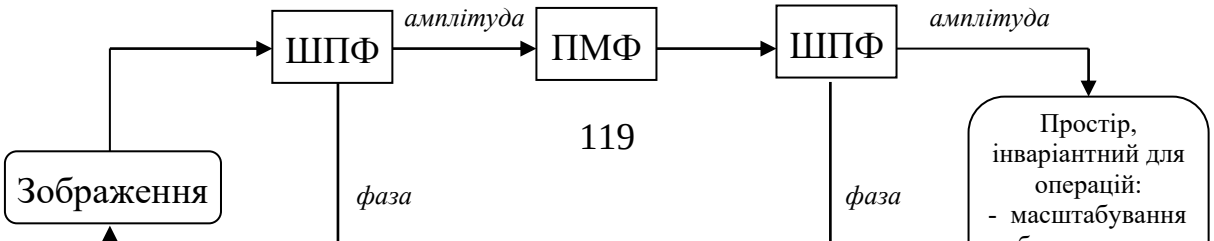


Рисунок 5.3 – Схема перетворення Меліна-Фур’є

Дискретне вейвлет-перетворення (ДВП) також застосовують у системах цифрових водяних знаків [35]. Загальна суть вейвлет-перетворення полягає в багатомасштабному просторово-частотному розкладанні зображення. На рис. 5.4 показаний приклад розкладання вихідного зображення з трьома масштабними множниками. Кожен масштабний множник забезпечує різний рівень роздільності зображення. Нижній діапазон частот з найменшим масштабним множником знаходиться в лівому верхньому кутку (блок LL_3). На тому ж самому рівні роздільності в блоці HL_3 утримується інформація щодо верхнього горизонтального і нижнього вертикального діапазону частот. Відповідно, блок LH_3 містить інформацію щодо нижнього горизонтального і верхнього вертикального діапазону частот з найменшим масштабним множником, а блок HH_3 – верхню смугу частот з тим же множником. Аналогічно будуються й інтерпретуються наступні рівні роздільності.

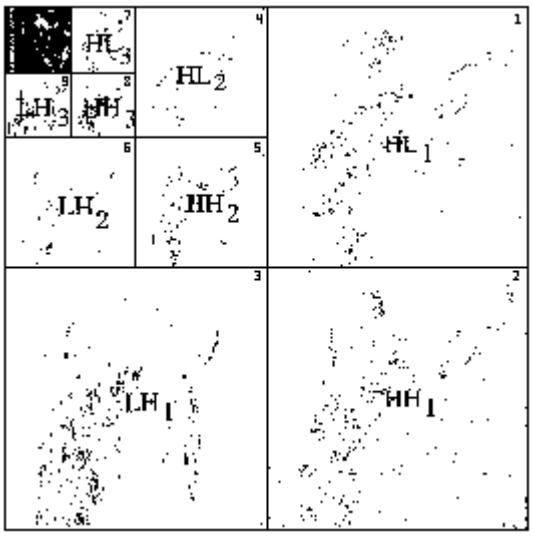


Рисунок 5.4 – Просторово-частотне розкладання зображення

На рис. 5.5 представлена каскадна схема двоканальних фільтрів для побудови просторово-частотного розкладання зображення.

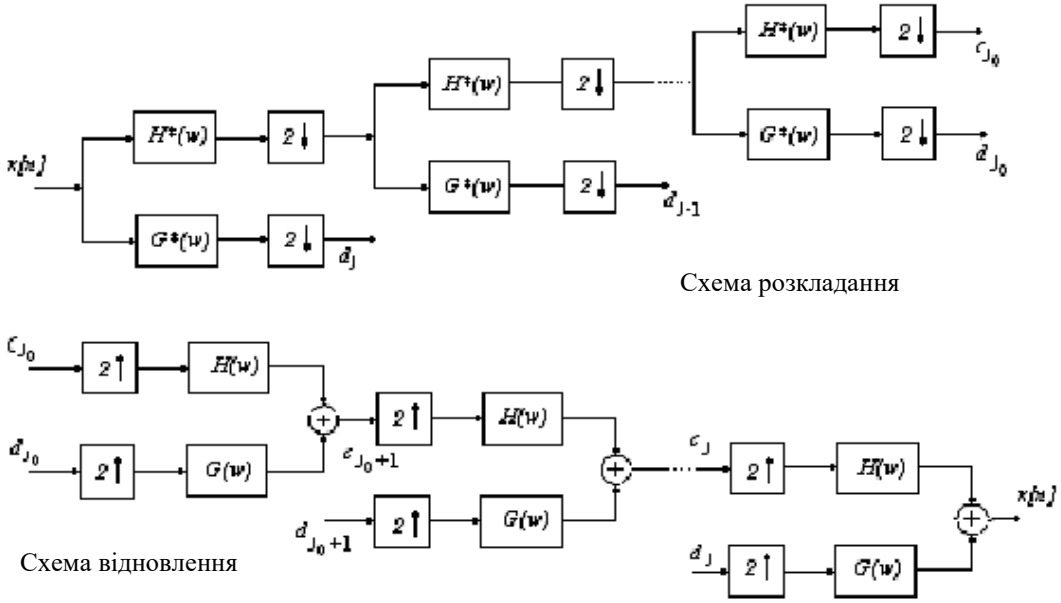


Рисунок 5.5. Схема реалізації вейвлет-перетворень

Набори двоканальних ортогональних фільтрів описуються рівняннями:

$$H(\omega) = \sum_k h_k \exp(-jk\omega) \quad \text{і} \quad G(\omega) = \sum_k g_k \exp(-jk\omega),$$

відповідно для верхньої і нижньої смуг.

Ітеративний процес розкладання зображення можна описати такими формулами:

$$c_{j-1,k} = \sum_n h_{n-2k} c_{j,n} \text{ і } d_{j-1,k} = \sum_n g_{n-2k} c_{j,n},$$

а ітеративний процес витягання зображення як:

$$c_{j,n} = \sum_k h_{n-2k} c_{j-1,k} + \sum_k g_{n-2k} d_{j-1,k}.$$

Вбудовування водяного знака в зображення відбувається шляхом додавання відповідних коефіцієнтів ДВП водяного знака і зображення різних рівнів роздільності. Попередньо коефіцієнти ДВП водяного знака можна підправити з урахуванням обмежень, які накладаються параметрами моделі зорових органів людини.

Розглянемо один з варіантів витягання ієрархічного водяного знака [36]. За допомогою ДВП проводиться просторово-частотне розкладання прийнятого зображення і його оригіналу (він повинен бути відомий) на чотири діапазони (1-ий рівень). Потім обчислюється взаємна кореляція між водяним знаком, доданим у діапазон HH_1, і різницею коефіцієнтів ДВП прийнятого зображення і його оригіналу в цьому ж діапазоні HH_1. Якщо взаємна кореляція набуває максимального значення, то вважається, що водяний знак виявлений. Інакше розглядаються інші діапазони на тому ж самому рівні (тобто HL_1, LH_1). У випадку, якщо водяний знак там не знайдений, то обчислюється новий рівень ДВП (2-ий рівень) і робиться ще одна спроба виявити водяний знак. Цей процес повторюється доти, поки водяний знак не буде виявлений або буде досягнутий верхній рівень роздільності ДВП.

Практика показує, що за допомогою вейвлет-перетворень можна забезпечити безпеку водяного знака від видалення під час здійснення операцій ущільнення з втратами, забезпечити внесення водяних знаків в ущільнені дані а також вибирати оптимальне місце розташування водяного знака.

5.5.3 Форматування водяного знака

У деяких системах перед внесенням водяного знака в цифровий об’єкт проводиться його попереднє форматування. Нижче описані найбільш розповсюджені методи форматування.

Широкосмугові методи використовуються в системах ЦВЗ з тих же причин, що й у стеганографії [13]. Відомо, що використання високих частот краще для забезпечення невидимості водяного знака, але це знижує рівень завадостійкості; і навпаки, низькі частоти забезпечують кращу

завадостійкості, але вносять видимі перекручування. Застосування широкосмугових методів дозволяє згладити ці протиріччя, оскільки вони забезпечують вбудовування сигналу малої потужності в кожен діапазон частот. У широкосмугових методах водяний знак розглядається як вузькосмуговий сигнал, а захищуване зображення – як широкосмуговий.

Існують два основних підходи до розширення спектра: за допомогою псевдовипадкової послідовності і за допомогою стрибкоподібних частот.

Суть першого підходу полягає в модуляції широкосмугового псевдовипадкового сигналу (шуму) вузькосмуговим сигналом, який відповідає водяному знаку (рис. 5.6). У результаті такої модуляції виходить сигнал, вигляд і спектр якого подібний шумовому сигналові. Одержувач може відновити вихідний сигнал водяного знака, якщо він демодулює прийнятий сигнал, використовуючи той же самий широкосмуговий псевдовипадковий сигнал (рис. 5.7). У зв’язку з тим, що інформація про водяний знак розташована в декількох діапазонах частот, вихідний сигнал буде відновлюватися без помилок, навіть якщо деякі частоти будуть вилучені під час передавання даних.

Рисунок 5.6 – Розширення спектра за допомогою псевдовипадкової послідовності

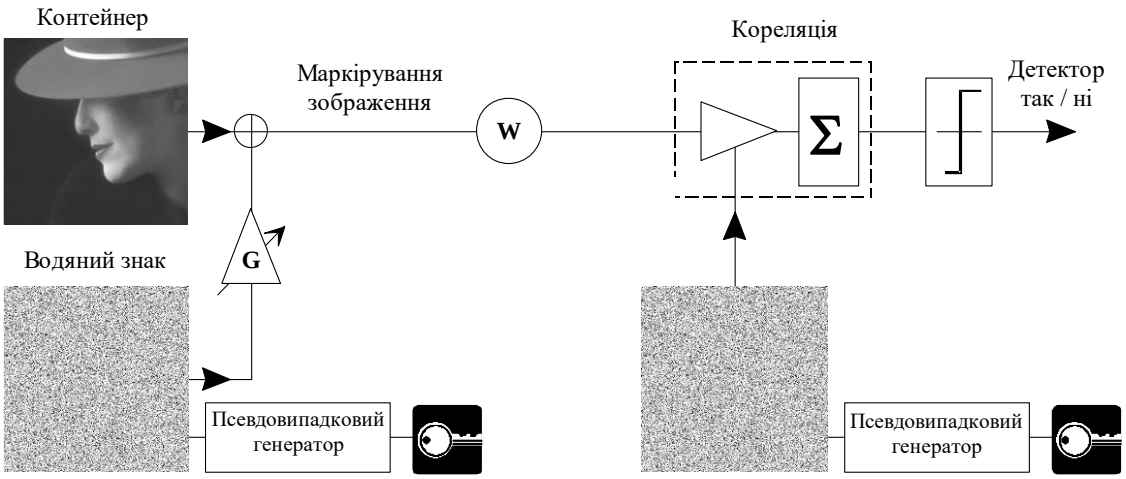


Рисунок 5.7 – Схема формування широкосмугового водяного знака

Під час використання стрибкоподібних частот основна частота сигналу водяного знака змінюється в широкому діапазоні у відповідності з випадковим законом, який визначається стегоключем. У результаті модульований сигнал має широкий спектр.

Головна проблема, яка виникає під час витягання водяного знака в умовах різних атак (особливо геометричних), полягає в підтримці правильної синхронізації між отриманим сигналом, який відповідає зображенню з водяним знаком, і псевдовипадковим сигналом. Захищеність водяного знака під час розширення спектра забезпечується за допомогою секретного ключа, за яким генерується псевдовипадкова послідовність.

В деяких мікросхемах, розроблених для відеотехніки, реалізована система водяних знаків із широкосмуговим кодуванням за таким алгоритмом [37]. Нехай мається двійковий сигнал $\{a_j\}$, де $a_j \in \{-1,1\}$. Із сигналу a_i шляхом його розтягування в часі будується сигнал b_i: $b_{i=}\ a_j$, де $j \cdot cr \le i < (j+1) \cdot cr$ і cr – швидкість чіпа. Водяний знак w_i, який буде безпосередньо внесений у зображення v_i, отримується шляхом модуляції сигналу b_i псевдовипадковою послідовністю p_i: $w_i = \alpha b_i\, p_i$, де α - множник, який впливає на завадостійкість і видимість водяного знака. Таким чином, формула для вбудовування водяного знака в зображення має вигляд $\tilde{v}_i = v_i + \alpha b_i\, p_i$. Для витягання водяного знака з зображення $\tilde{v}_i$ необхідно демодулювати отриманий сигнал і до кожного його компонента додати відповідні величини:

$$s_j = \sum_{i=jcr}^{(j+1)cr-1} p_i \tilde{v}_i = \sum_{i=jcr}^{(j+1)cr-1} p_i v_i + \sum_{i=jcr}^{(j+1)cr-1} p_i^2 \alpha b_i \ .$$

Враховуючи, що середнє значення сигналу p_i дорівнює нулеві і він статистично незалежний від v_i, $s_j \approx cr \alpha a_j$, випливає, що $a_j = sign(s_j)$.

Низькочастотні водяні знаки. Зазвичай вважається, що вбудований водяний знак повинен витримувати всілякі маніпуляції доти, поки дане зображення ще зберігає хоч які-небудь споживчі властивості. Багато маніпуляцій із зображенням базуються на низькочастотній фільтрації (JPEG-ущільнення, зміна розмірів та ін.). З цієї причини розробляються «низькочастотні» водяні знаки, хоча вони, як правило, можуть залишати видимі сліди в зображенні.

Схема створення низькочастотного водяного знака з використанням дискретного перетворення Фур'є може виглядати таким чином (рис. 5.8) [38]. Нехай є водяний знак $w_{вих}(i,j)$, який має розміри захищуваного зображення. На основі $w_{вих}(i,j)$ будується водяний знак $w_{ущ}(i',j')$ зі зменшеними розмірами і для нього обчислюється ДПФ $W_{ущ}(u,v)$. Після цього $W_{ущ}(u,v)$ доповнюється нулями до початкових розмірів і обчислюється зворотне ДПФ, у результаті чого буде отримано зображення водяного знака $w_{нч}(i,j)$, у якому гарантовано будуть присутні тільки низькі частоти.

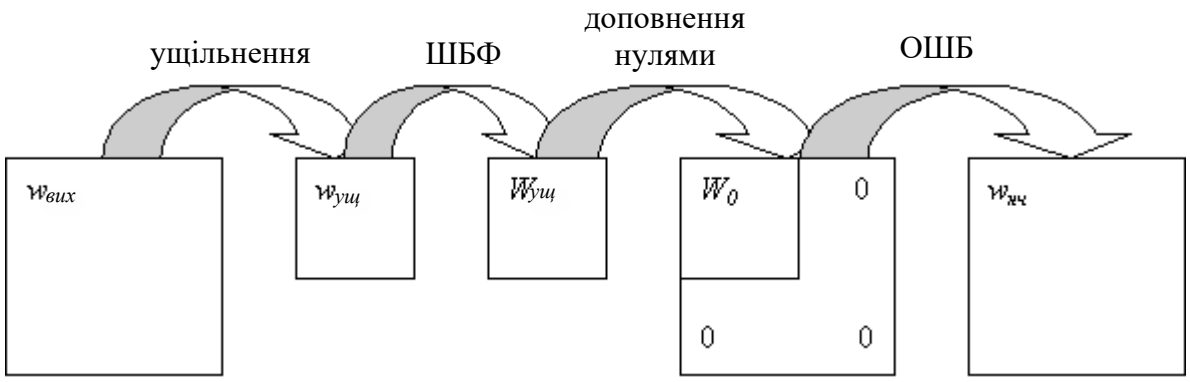


Рисунок 5.8 – Етапи побудови низькочастотного водяного знака

Коди з виправленням помилок використовуються в системах ЦВЗ для вирішення проблеми завадостійкості водяних знаків до впливу випадкових і навмисних перекручувань [39]. У даному випадку, за аналогією з передаванням інформації каналом з перешкодами, зображення розглядається як канал зв'язку, а різного виду атаки - як перекручування, внесені шумом. Слід відзначити, що на відміну від класичної задачі кодування каналу, де моделлю перекручування є нормально розподілений шум, системи водяних знаків повинні враховувати різні види атак, яким

відповідають моделі шумів різної природи, не завжди розподілених за законом Гауса. У цьому контексті, дуже важко створити унікальний код, який би протистояв різним типам атак, і ця проблема дотепер не вирішена. Слід зазначити, що не завжди існує можливість збільшення об'єму водяного знака в зображенні (тому що на відміну від аудіо і відео, воно статично і кінцево) для того, щоб скористатися кодом з виправленням помилок, тому при використанні коригувальних кодів важливу роль відіграє співвідношення між об'ємом інформації зображення і водяного знака.

5.5.4 Способи внесення водяного знака в цифровий об'єкт

Внесення водяних знаків можна проводити за допомогою *фазової і амплітудної модуляції* [40, 41]. Будь-яке зображення I за допомогою дискретного перетворення Фур'є можна представити амплітудною і фазовою складовою. Відомо, що амплітудна складова ШПФ не має значного впливу на якість зображення, тоді як фазова складова сильно впливає на його розбірливість. Крім цього, фазові компоненти завадостійкі до шуму і нечутливі до зміни контрасту в зображенні. Таким чином, якщо вносити водяний знак у фазові компоненти ШПФ, то під час його несанкціонованого видалення якості зображення буде нанесений відчутний збиток.

Для того, щоб за допомогою фазової модуляції внести в зображення водяний знак, необхідно змінити частотні компоненти зображення в такий спосіб:

$$\phi(k_1,k_2) \leftarrow \phi(k_1,k_2) + \delta$$

$$\phi(N_1-k_1,N_2-k_2) \leftarrow \phi(N_1-k_1,N_2-k_2) - \delta,$$

де δ – рівень, що відповідає водяному знакові (позначення відповідають розд.3). Для водяного знака достатньо вибрати ті коефіцієнти ШПФ, енергія яких достатньо висока для істотного впливу на зображення, тобто таких, що

$$A(k_1,k_2)^2 / \sum_{r_1=1}^{N_1-1} \sum_{r_2=1}^{N_2-1} A(r_1,r_2)^2 > \varepsilon .$$

Це гарантує небажані втрати в якості зображення під час атак на водяний знак.

Амплітудну модуляцію можна провести безпосередньо з зображенням або його частиною. Для прикладу розглянемо амплітудну модуляцію компонента синього кольору зображення. Нехай кольорове зображення представляється у вигляді $I=(R,G,B)$, де $p=(i,j)$ - випадкове місце розташування піксела в зображенні і $m=\{0,1\}$ – біт водяного знака. Тоді новий компонент синього кольору B’ з водяним знаком можна отримати з B за таким співвідношенням: $\mathbf{B}'_{ij} \leftarrow \mathbf{B}_{ij} + (2m-1)qY_{ij}$, де Y – компонента яскравості і q – константа, що впливає на оптимальне співвідношення завадостійкості і видимості. Слід зазначити, що відповідно до цієї формули велика яскравість краща для надійності водяного знака, тому що зір людини має низьку чутливість при великій яскравості.

Внесення водяних знаків можна проводити шляхом *квантування коефіцієнтів* дискретного *косинусного перетворення* [42]. Припустимо необхідно вбудувати бітову послідовність водяного знака $\{m_k\}_{k=1,..,l(m)}$ у зображення. Для цього, у відповідності зі стегоключем, у зображенні вибирають k блоків розміру 8×8. Один біт водяного знака вставляється в один блок зображення. Для кожного вибраного блоку обчислюються коефіцієнти ДКП $\{a_{i,j}\}_{i,j=1,\ldots,8}$... Процес впровадження біта водяного знака відбувається шляхом введення певного відношення між двома коефіцієнтами ДКП одного блоку в такий спосіб. Для всіх бітів водяного знака $k=1,...,l(m)$ виконуються такі операції. Якщо ($m_k=1$ і $(a_{1,2)k}>(a_{2,1)k}$) або ($m_k=0$ і $(a_{1,2)k}<(a_{2,1)k}$), то необхідне відношення між коефіцієнтами вже існує і немає необхідності в проведенні модифікацій; інакше, для збереження відповідного співвідношення проводиться обмін значень між коефіцієнтами ДКП. Для всіх змінених блоків зображення обчислюється зворотне дискретне косинус перетворення.

Для витягання водяного знака необхідно досліджувати співвідношення між коефіцієнтами $(a_{1,2})_k$ і $(a_{2,1})_k$. Якщо $(a_{1,2})_k<(a_{2,1})_k$, то k-ий біт водяного знака дорівнює нулеві, інакше – одиниці.

Метод внесення водяного знака *із збереженням середньої яскравості* [43] базується на класифікації областей зображення шляхом кластеризації пікселів за однорідним набором. Алгоритм вбудовування водяного знака можна представити в такий спосіб:

1. У відповідності зі стегоключем вибираються блоки зображення, куди буде вбудовуватися водяний знак.

2. Пікселі кожного блоку класифікуються в залежності від їхньої контрастності (великої, середньої і низької); у кожнім блоці виділяються дві області R_1 і R_2, для яких обчислюються середні значення яскравості.

3. Кожну область R_1 і R_2 певним чином розбивають на дві області (позначимо їх A і B). Таким чином, отримані чотири підобласті $R_{1,A}$, $R_{1,B}$, $R_{2,A}$ і $R_{2,B}$, у кожній з них знаходиться відповідно $n_{1,A}$, $n_{1,B}$, $n_{2,A}$ і $n_{2,B}$ пікселів, середня яскравість яких оцінюється як $Y_{1,A}$, $Y_{1,B}$, $Y_{2,A}$ і $Y_{2,B}$.

4. Нехай m – це біт водяного знака, який необхідно приховати в блоці. Операція приховування може бути описана як:

$$\text{якщо } m=0, \text{ то } \tilde{Y}_{1,A} - \tilde{Y}_{1,B} = -l \text{ і } \tilde{Y}_{2,A} - \tilde{Y}_{2,B} = -l,$$

$$\text{якщо } m=1, \text{ те } \tilde{Y}_{1,A} - \tilde{Y}_{1,B} = l \text{ і } \tilde{Y}_{2,A} - \tilde{Y}_{2,B} = l,$$

де l – рівень приховування. Оскільки середні значення яскравості R_1 і R_2 повинні бути збережені, можна визначити два інших рівняння:

$$\frac{n_{1,A}\tilde{Y}_{1,A} + n_{1,B}\tilde{Y}_{1,B}}{n_{1,A} + n_{1,B}} = Y_1 \text{ і } \frac{n_{2,A}\tilde{Y}_{2,A} + n_{2,B}\tilde{Y}_{2,B}}{n_{2,A} + n_{2,B}} = Y_2.$$

Ці рівняння дозволяють обчислити середні значення яскравості $\tilde{Y}_{1,A}$, $\tilde{Y}_{1,B}$, $\tilde{Y}_{2,A}$ і $\tilde{Y}_{2,B}$ відповідно до чергового приховуваного значення b біта водяного знака.

5. Усі пікселі однієї області модифікуються в такий спосіб:

$$\delta_{i,j} = \tilde{Y}_{i,j} - Y_{i,j}.$$

Перші три етапи алгоритму витягання водяного знака аналогічні алгоритмові вбудовування ВЗ. Потім обчислюються значення $\sigma_1 = \tilde{Y}_{1,A} - \tilde{Y}_{1,B}$ і $\sigma_2 = \tilde{Y}_{2,A} - \tilde{Y}_{2,B}$, за якими можна визначити значення біта b. А модуль цих величин дозволяє оцінити правильність відновленого біта водяного знака.

Внесення водяного знака на основі фрактального кодування [44]. Фракталом називається структура, що складається з частин, які в певному розумінні є подібними. Фрактальне кодування – це математичний процес, застосовуваний для кодування растрів, які містять реальне зображення, в сукупність математичних даних, які описують фрактальні властивості зображення. Фрактальне кодування ґрунтується на тому факті, що всі

природні і більшість штучних об’єктів містять надлишкову інформацію у вигляді однакових, повторюваних малюнків, що називаються фракталами.

Нехай необхідно ущільнити зображення I_{orig}. Позначимо через $d(I,J)$ – міру розбіжності між двома зображеннями I і J. Відображення τ одного зображення в інше будемо називати ущільнювальним, якщо $d(\tau(I),\tau(J))<\sigma\cdot d(I,J)$, де σ – коефіцієнт ущільненості, $0<\sigma<1$. Відповідно до теореми про ущільнювальне відображення, перетворення $\tau^n(I)$ збігається до точки притягання I_a при $n\to\infty$, тобто незалежно від початкового зображення система завжди збігається до якогось стабільного зображення. Відомо також (теорема про колаж), що для ущільнювального перетворення τ з коефіцієнтом ущільненості σ і властивістю $d(I_{\text{orig}},\tau(J))<\varepsilon$ справедливе співвідношення

$$d(I_{\text{orig}},I_a)<\varepsilon/(1-\sigma). \qquad (5.1)$$

Таким чином, деяке зображення можна певним чином описати за допомогою ущільнювальних перетворень, які, бувши застосованими багаторазово на будь-якому початковому зображенні, зрештою дадуть вихідне зображення. Як правило, опис такої процедури ущільнення менше опису самого зображення, тому його вигідніше передавати каналами зв'язку замість зображення і потім відновлювати.

Задача фрактального кодера полягає в побудові такого перетворення τ (називається IFS-кодом або системою ітераційних функцій), яке при обмежених розмірах забезпечує найкращу подібність між $\tau(I_{\text{orig}})$ і I_{orig}. IFS-код складається з набору афінних перетворень (лінійні перетворення разом з паралельним перенесенням). Кодер по одному для кожного блоку R_i визначає перетворення зображення I_{orig} як суму афінних перетворень τ_i. Перетворення τ_i відображає певний домен у відповідний блок R_i. Розходження блоку і домену лише в їхніх розмірах: зазвичай квадратні блоки мають розмір $B\times B$, а домени – вдвічі більший – $2B\times 2B$ (B – це 8 пікселів). Для кожного блоку кодер шукає найбільш відповідний колаж з перетвореного й обраного доменного блоку. Під час пошуку можливих доменів над ними проводяться такі перетворення: ізометричні зміни, масштабування і зсув значень яскравості (рис. 5.9).

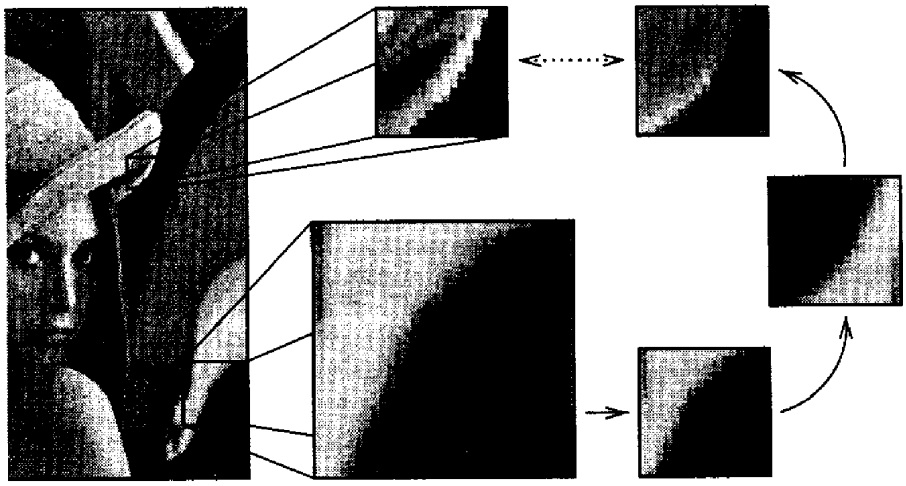


Рисунок 5.9 – Фрактальне кодування: приклад встановлення відповідності між блоками за допомогою операцій обертання й інвертування яскравості

Під час декодування, на основі отриманого IFS-коду τ обчислюється точка притягання I_a відновлюваного зображення. Спочатку, застосовуючи до довільного початкового зображення I_0 отриманий IFS-код τ, формується зображення I_1. Потім, повторюючи процес, з I_1 отримується I_2; і так далі, доти, поки не вийде I_a. Зазвичай, для забезпечення збіжності потрібно не менше десяти ітерацій. Помилки, що виникають під час відновлення зображення, мають верхню границю, яка відповідає співвідношенню (5.1).

Системи водяного знака використовують фрактальне кодування з додатковим обмеженням: вводяться області можливого пошуку доменів. Наприклад, замість сканування цілого зображення воно ділиться на дві складові частини і, в залежності від значення приховуваного біта, розглядається тільки одна зі складових частин.

Більш точно процес внесення водяного знака в зображення можна представити в такий спосіб. Нехай m – послідовність бітів, які необхідно приховати з надлишковістю U. Відповідно до секретного ключа для кожного біта m_k вибираються U блоків, при цьому

– якщо m_k=1, то блок R_k кодується шляхом пошуку для нього відповідного домену D_k у тій частині зображення, яка позначена «0»;

– якщо m_k=0, то блок R_k кодується пошуком домену D_k у частині зображення, яка позначена «1».

Блоки R_k , що *залишилися,* кодуються, як і у випадку «класичного» фрактального кодування зображення, під час пошуку *доменів* D_k по всьому зображенню. Після цього обчислюється точка притягання I_a.

Процес витягання водяного знака складається з двох кроків:

1.Для I_a і кожного блоку R'_k, вибраного відповідно до секретного ключа, шукається пов'язаний з ним домен D'_k. Якщо домен D'_k належить до частини зображення, позначеного «1», то внесений біт дорівнює «1», в іншому випадку – «0».

2. Рішення про значення кожного біта m_k приймається за більшістю «0» або «1» у наборі U.

* * *

Якщо розглядати комерційні застосування стеганографії, то одним з найбільш перспективних напрямків її розвитку бачиться саме розвиток і застосування невидимих цифрових водяних знаків для захисту авторських прав на цифрові вироби. Поміщені у файл цифрові водяні знаки можуть бути розпізнані спеціальними програмами, які витягнуть з файлу багато корисної інформації: коли створений файл, хто має авторські права, як вступити в контакт з автором.

Ринок засобів захисту інтелектуальної власності, розповсюджуваної в Інтернеті і на інших цифрових носіях, тільки створюється. Але при тому повальному злодійстві, яке відбувається в мережі, користь цієї технології – очевидна.

5.6 Питання для самоконтролю знань

1. В чому полягає проблема захисту авторського права?
2. Посніть термін «цифрові водяні знаки».
3. Поясніть поняття «відбиток пальця» та «маркування».
4. Сформулюйте вимоги до систем цифрових водяних знаків.
5. Розкрийте поняття видимі, напіввидимі, невидимі та крихкі водяні знаки.
6. Як здійснюється внесення та витягання цифрових водяних знаків у цифровий об'єкт за допомогою плагіну Digimarc графічного редактора Photoshop?
7. Наведіть приклади можливого використання систем цифрових водяних знаків.
8. Наведіть узагальнену модель системи цифрових водяних знаків.
9. На які типи діляться системи цифрових водяних знаків?

10. Які аспекти повинні враховуватись у системах цифрових водяних знаків?

11. Розкрийте основні вимоги до систем цифрових водяних знаків.

12. Наведіть вимоги IFPI до стійкості водяних знаків у звукові.

13. На які групи поділяють перекручування, яким піддаються об’єкти з ЦВЗ?

14. Які існують перекручування та атаки на ЦВЗ?

15. Охарактеризуйте методи вибору місця розташування ЦВЗ.

16. Охарактеризуйте методи вибору простору для представлення водяного знака.

17. Охарактеризуйте методи попереднього форматування водяного знака.

18. Охарактеризуйте способи внесення водяного знака в цифровий об’єкт.

19. Яким чином здійснюється внесення водяного знака на основі фрактального кодування?

20. Які перспективні напрямки розвитку комерційних застосувань стеганографії?

6 ЦИФРОВІ ВІДБИТКИ

Під терміном «відбиток пальця» (*fingerprint*) будемо розуміти деяку характеристику об'єкта, яка дозволяє відрізнити даний об'єкт від інших йому подібних. Ідентифікація об'єктів за відбитками застосовується здавна. Можна навести такі класичні приклади.

1. *Відбиток пальця людини* має унікальний відтиск, який широко використовується під час ідентифікації особистості. Відбитки пальця знімають практично у всіх ув'язнених, а в деяких країнах (Корея, Франція) передбачений обов'язковий відбиток пальця в посвідченні особи. Відбиток пальця, а також деякі інші біометричні характеристики (сітківка ока, голос) широко використовуються в системах керування доступом на секретні об'єкти.

2. *Серійні номери* виробів, будучи унікальними, використовуються як ознака відмінності між ними.

3. *Кодовані частинки вибухових речовин*. Деякі вибухові речовини виготовляються із вкрапленням маленьких кодованих частинок. Це допомагає під час вибухотехнічного аналізу ідентифікувати завод-виробник, а також тип і час випуску вибухового засобу.

До появи комп'ютерів розвивалися лише фізичні технології реєстрації відбитка. З розвитком телекомунікаційних і обчислювальних мереж технологія відбитка пальця (*fingerprinting*) стала застосовуватися для цифрових об'єктів (програм, текстових документів, зображень, відео, аудіо та ін.). Наприклад:

– У програмі шифрування PGP під час ідентифікації відкритих ключів використовується цифровий відбиток у вигляді значення хеш-функції, яка обчислюється за алгоритмом MD5 від бітів відкритого ключа, модуля і показника ступеня шифрування. Цей відбиток майже унікальний і використовується центром сертифікації як ідентифікатор у каталозі ключів.

– Методи цифрового відбитка застосовується в деяких цифрових і аудіозаписах для виявлення фактів незаконного розповсюдження копій, а в платному телебаченні – для відстеження незареєстрованих абонентів.

Методи цифрового відбитка пальця розробляються та вивчаються в рамках загальної теорії стеганографії, зокрема цифрових водяних знаків.

Нижче будуть розглянуті методи цифрового відбитка відносно проблеми захисту авторських прав на цифрові дані (об'єкти).

Слід зазначити, що цифрові відбитки не запобігають самій можливості несанкціонованого створення копій даних. Ця технологія дозволяє лише розрізнити копії цифрових об'єктів, виявити факти незаконного їхнього використання, а також у деяких випадках визначити коло осіб, які беруть участь у несанкціонованому виготовленні копій, і довести їхню провину.

6.1 Термінологія й основні положення

Під технологією цифрового відбитка пальця розуміють процес додавання відбитка в цифровий об'єкт (виріб) або ідентифікацію об'єкта, якщо мітка в ньому вже присутня. При описуванні систем цифрових відбитків застосовуються такі терміни:

– *цифрова мітка* – частина цифрового об'єкта (виробу), яка може приймати значення з деякої множини;

– *цифровий відбиток пальця* (цифровий відбиток) – це сукупність цифрових міток;

– *дистриб'ютор* (продавець) – уповноважений розповсюджувач цифрового об'єкта, в якому міститься цифровий відбиток;

– *зареєстрований користувач* (покупець) – індивідуум, який законно користується цифровим об'єктом, у якому знаходиться цифровий відбиток;

– *пірат* – індивідуум, який отримає вигоду від несанкціонованого використання виробу з цифровим відбитком;

– *зрадник* – зареєстрований користувач, який незаконно передає свій виріб з цифровим відбитком або проводить з ним несанкціоновані дії.

Для розуміння приведеної термінології розглянемо таку модель. *Дистриб'ютор*, який законно розповсюджує серед споживачів цифрові вироби (наприклад, DVD, Blue-Ray диски), навмисно додатково вносить у кожну легально продану копію приховані дані (*цифрові мітки*). Сукупність усіх цих міток складає *цифровий відбиток*. Деякі зареєстровані користувачі (*зрадники*) можуть піти на таємну змову: провести порівняння копій своїх виробів і виділити всі цифрові мітки. У цьому випадку вони

можуть віддати (або продати) дану інформацію сторонньому – *піратові*, який може налагодити виробництво незаконних копій.

У даному випадку метою дистриб'ютора є пошук та ідентифікація зареєстрованих користувачів (зрадників), які пішли на компроміс з піратом, а метою пірата – запобігання можливості своєї ідентифікації дистриб'ютором.

До систем реєстрації відбитка пальця зазвичай висувають такі основні вимоги:

– *стійкість до змови*: якщо той, хто атакує, має доступ до деякої кількості копій цифрового об'єкта, то шляхом їхнього загального аналізу він не повинен знайти, видалити або замінити цифрові відбитки;

– *збереження якості виробу*: цифрові мітки, що вставляються, не повинні значно погіршувати якість об'єкта;

– *стійкість до модифікацій виробу*: якщо той, хто атакує, змінює цифровий об'єкт, то відбиток дистриб'ютора повинен зберігатися в ньому доти, поки рівень перекручувань не зробить сам об'єкт непридатним до застосування.

У системах реєстрації відбитка пальця використовуються різні підходи, класифікацію яких можна провести за такими ознаками.

1. Класифікація на основі представлення даних

– *Фізична реєстрація відбитка*, коли виріб має власні фізичні характеристики, які використовуються як відмітні ознаки (райдужна оболонка ока, голос та ін.).

– *Цифрова реєстрація відбитка*, коли виріб представлений у цифровому форматі і можлива комп'ютерна обробка відбитка.

2. Класифікація на основі рівня чутливості виявлення відбитка

– *Точна реєстрація відбитка* відповідає випадку, коли будь-яка зміна цифрового об'єкта робить відбиток невпізнанним, а сам об'єкт – непридатним до цільового застосування.

– *Статистична реєстрація відбитка* висуває менш суворі вимоги. Для того, щоб правильно ідентифікувати «пірата», потрібно обробити не одну, а досить велику кількість піратських копій. При цьому остаточний результат ідентифікації має певну імовірність.

– *Гранична реєстрація відбитка* є змішаним типом двох попередніх. У цій схемі передбачений певний поріг, який вказує на допустиму кількість користувачів незаконною копією. Якщо кількість виготовлених піратських копій менше заданого порогу, то копії неможливо виявити. Якщо ж число копій перевищить цей поріг, то існує можливість відстежити пірата.

3. Класифікація на основі методу

– *Схема розпізнавання* призначена для реєстрації і перевірки таких відбитків, які є невід'ємною частиною об'єкта (наприклад, відбитки пальця людини).

– *Схема стирання* видаляє деяку початкову частину цифрового об'єкта в процесі вставляння відбитка.

– *Схема накладення* додає деяку нову частину в цифровий об'єкт. Ця додаткова частина може якимось чином інтерпретуватися або бути безглуздою.

– *Схема модифікації* проводить зміну в деяких місцях цифрового об'єкта.

4. Класифікація на основі вигляду відбитка

– *Дискретні відбитки*: відбиток може приймати тільки дискретні значення (наприклад, хеш-значення цифрового файлу).

– *Безперервні відбитки*: відбиток може приймати будь-яке можливе значення (фізичні відбитки).

6.2 Приклади схем реєстрації цифрового відбитка

Розглянемо деякі найбільш типові моделі систем реєстрації цифрового відбитка пальця, які можна застосувати для вирішення задач захисту авторських прав. Дані моделі дають тільки загальне уявлення про підходи до вирішення оголошеної задачі. У дійсності запропоновані й інші схеми, які забезпечують захист авторських прав в галузі електронної торгівлі.

6.2.1 Статистична реєстрація відбитка

В основі статистичної схеми реєстрації відбитка лежить статистична перевірка гіпотез [46]. Суть даної процедури така. Припустимо, що дистриб'ютор продає користувачам m копій певного виробу. Нехай дані

дійсні числа $v_1,v_2,\ldots,v_n$, де число n досить велике для того, щоб провести статистичну перевірку гіпотез. Нехай для кожного v_j є таке значення $\delta_j>0$, що його δ_j-*окіл* не перетинається з δ_i-*околом* v_i, для всіх $i\neq j$. Кожному користувачеві відповідає одне число з інтервалу $[v_j-\delta_j,\ v_j+\delta_j]$, за яким він буде відрізнятися від інших користувачів. Приблизно половина значень, отриманих користувачами, буде знаходитися в інтервалі $[v_j,\ v_j+\delta_j]$, а інша половина – у $[v_j-\delta_j,\ v_j]$. Позначимо через v_{ij} j-ту копію цифрового об'єкта, передану *i-му користувачеві*.

Припустимо, що дистриб'ютор зміг виділити з піратської копії значення $v_1',v_2',\ldots,v_n'$. У цьому випадку його метою буде перевірка гіпотези, що джерелом для даної копії була копія, продана i-му користувачеві, для всіх $1\le i\le m$.

Розглянемо для даного i функцію правдоподібності

$$L_{ij} := \frac{v'_j - v_{ij}}{\delta_j},\ 1\le j\le n, \tag{6.1}$$

де $(L_{ij})_{1\le j\le n}$ – нормована різниця між значеннями v' піратської копії і значеннями v, які були видані i-му користувачеві.

Для конкретного i розглянемо значення $(L_{ij})_{1\le j\le n}$ двох непересічних підмножин. Нехай μ_i^h – значення тих L_{ij}, для яких v_{ij} більше з двох копій v_j, проданих різним користувачам, і μ_i^l – для тих L_{ij}, при яких v_{ij} менше. Тоді $\mu_i^l\le 0$ і $\mu_i^h\ge 0$.

Нехай $\mu_i:=\mu_i^l-\mu_i^h$. Припустимо, що пірат не робив ніяких змін у тиражованих копіях. Тоді, якщо він отримав виріб від i-го користувача, то $\mu_i=\mu_i^l=\mu_i^h=0$. Якщо ж він отримав їх ще від когось, тоді

$$\mu_i^h\approx -0.5,\ \mu_i^l\approx 0.5 \text{ і } \mu_i^l-\mu_i^h\approx 1. \tag{6.2}$$

Таким чином, якщо в копії не було зроблено ніяких змін, то при досить великих n пірат повинен бути відразу ідентифікований.

Якщо в копії проводилися деякі зміни, то співвідношення $\mu_i^h\approx 0$ більше виконуватися не буде (оскільки середнє значення цих змін, в основному, відрізняється від нуля). Таким чином, якщо i-тий користувач передав свою копію піратові, то μ_i може бути близьким до нуля. З іншого боку, якщо i-тий користувач не передавав свою копію піратові, то для великих n справедливо

$$\mu_i=\mu_i^l-\mu_i^h\approx 1. \tag{6.3}$$

Отже, можна застосувати такий алгоритм. Для кожного i обчислюється різниця μ_i між двома найбільшими значеннями. Якщо для деякого i значення μ_i близьке до нуля, а для всіх інших μ_k, де $k \neq i$, – близьке до одиниці, то тоді має́ться доказ того, що i-тий користувач є «зрадником». Перевіряючи значення μ_i для всіх i, можна виявити коло санкціонованих користувачів, які незаконно передали піратові свою інформацію.

Слід зазначити, що дана схема базується на перевірці гіпотез, тому впевненість в отриманому результаті має деяку імовірність.

6.2.2 Схема асиметричної реєстрації відбитка

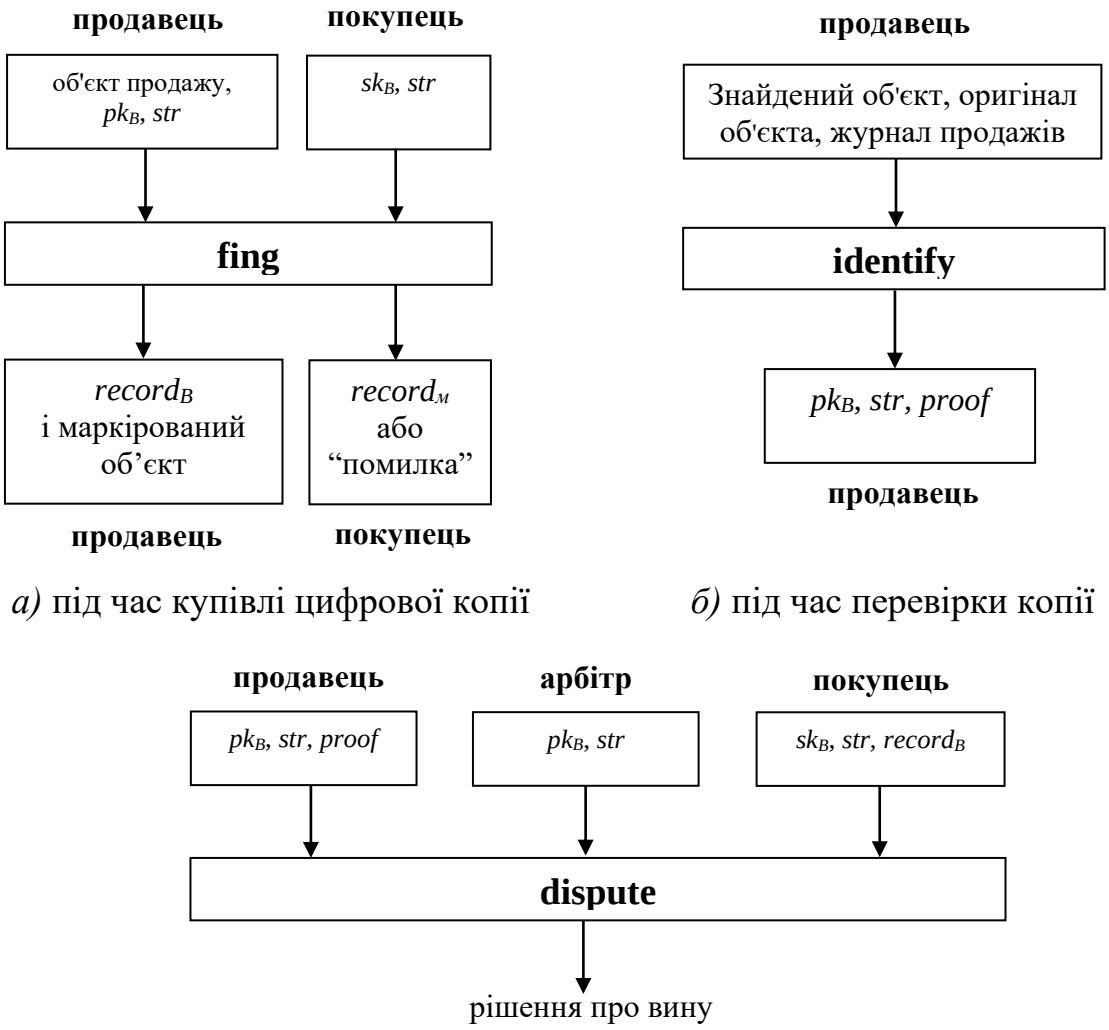
Зазвичай схеми реєстрації відбитка є симетричними. У рамках таких систем у користувача немає можливості відмовитися від копії, де проставлені його відбитки. В електронній торгівлі ця властивість породжує ситуацію, коли не можна довести хто виготовив незаконну копію – продавець чи покупець. Для вирішення такої проблеми запропонована схема асиметричної реєстрації відбитка [47], в якій реалізовані такі положення:

– тільки санкціонований користувач знає всю інформацію, приховану у відбитку цифрового об’єкта;

– якщо дистриб’ютор знайде де-небудь незаконну копію, то він зможе ідентифікувати того покупця, кому дана копія була продана, і довести це третій особі.

У розглянутій схемі (рис.6.1) передбачається реалізація чотирьох протоколів: «генерація ключа» (*Key_gen*), «реєстрація відбитка» (*Fing*), «ідентифікація» (*Identify*) і «вирішення суперечки» (*Dispute*).

Розглянемо процедуру купівлі цифрового виробу. Кожен покупець повинен відповідно до протоколу *Key_gen* згенерувати для себе відкритий і секретний ключі (відповідно, pk_B та sk_B) і зареєструвати ключ pk_B у центрі сертифікації. Здійснення покупки проводиться відповідно до протоколу *Fing* (рис. 6.1,*а*). Продавець вводить у продаваний виріб відкритий ключ pk_B і рядок *str*, який містить атрибути покупки. Покупець вводить свій секретний ключ sk_B і рядок *str*, у результаті чого у виріб, що купується, вноситься відповідний відбиток. Покупець і продавець також отримують чеки про здійснену угоду $record_B$ і $record_м$, відповідно. Покупець може зберігати цей чек на випадок виникнення можливих суперечок, а в продавця ведеться реєстр усіх продажів даного виду виробу.



а) під час купівлі цифрової копії *б)* під час перевірки копії

в) у випадку вирішення суперечки

Рисунок 6.1 – Схема асиметричної реєстрації цифрового відбитка

Якщо продавець знайде піратську копію виробу і захоче ідентифікувати її першого покупця, то він повинен відповідно до протоколу *Identify* (рис. 6.1,*б)* провести аналіз знайденої копії і реєстру продажів. У результаті аналізу може бути ідентифікований ключ покупця pk_B і його рядок підпису *proof*, або ж видане повідомлення «невдача», яке свідчить про неможливість ідентифікації.

Вирішення суперечки відповідно до протоколу *Dispute* (рис. 6.1,*в)* може проходити між двома або трьома сторонами: продавцем, арбітром і, можливо, покупцем. Для цього у відповідний алгоритм продавець і арбітр вводять pk_B і *str*. Продавець також додатково вводить рядок *proof*. Якщо підозрюваний покупець також бере участь у судовому розслідуванні, то він вводить *str*, секретний ключ sk_B і повідомлення $record_B$. Результатом

роботи алгоритму є підказка арбітрові про можливу відповідність піратської копії тій копії, яку купив покупець з ідентифікаційним рядком *str*.

6.2.3 Схема анонімної реєстрації відбитка

Вважається, що електронна торгівля повинна надавати такий же рівень анонімності здійснення покупки, як і звичайна торгівля. Анонімність покупця буде порушена, якщо його змусять себе ідентифікувати. Розглянуті вище симетричні й асиметричні схеми реєстрації відбитка передбачали ідентифікацію покупця під час купівлі. За аналогією з криптографічною схемою сліпого підпису, яка дає можливість отримати від абонента підпис на дані без розкриття їхнього змісту, розроблена схема анонімної реєстрації відбитка [48].

У цій схемі для ідентифікації покупця передбачена «третя довірена особа», яка має назву *центр реєстрації*, без якого продавець не зможе провести ідентифікацію покупця. При такій схемі покупець може анонімно купувати цифровий об’єкт. Однак існує можливість його ідентифікації у випадку, якщо він незаконно передасть кому-небудь цифровий об’єкт (рис.6.2).

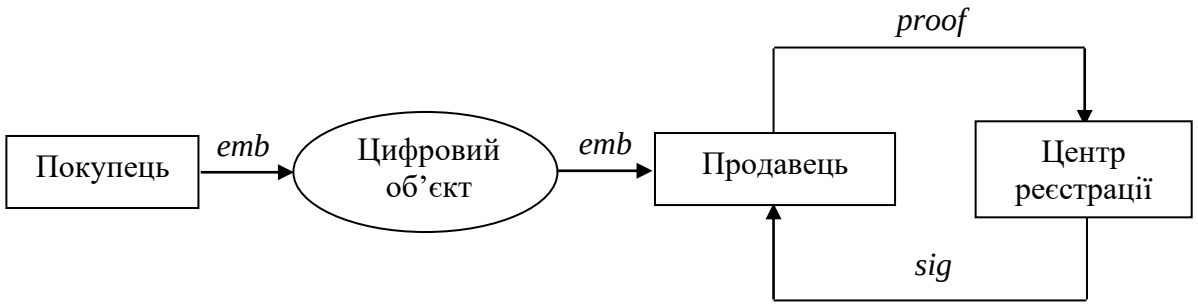


Рисунок 6.2 – Схема анонімної реєстрації відбитка

Суть основної ідея анонімної реєстрації відбитка така: покупець вибирає собі псевдонім, а саме, ключову пару для підпису (sk, pk_B), підписує його істинним ім’ям і отримує з центру реєстрації сертифікат на свій псевдонім. Тим самим покупець бере на себе відповідальність за цей псевдонім.

Наявність сертифіката центру реєстрації підтверджує те, що вся необхідна інформація про покупця йому відома (тобто можливо за псевдонімом ідентифікувати реальну людину).

Коли покупець робить покупку, то для повідомлення *текст*, у якому описується покупка, він обчислює підпис $sig:=sign(sk_B,текст)$ і вбудовує його в куплений виріб: $emb:=(текст,sig,pk_B,cert_B)$. А, продавець, таким чином, має «нульові знання» про покупця.

Якщо необхідно провести ідентифікацію покупця, то продавець витягає з виробу цифровий відбиток *emb* і надсилає в центр реєстрації повідомлення $proof:=(текст,sig,pk_B)$ із проханням про проведення процедури ідентифікації. У відповідь центр реєстрації повертає продавцеві підпис покупця. Маючи цей підпис, продавець може перевірити його та отримати докази для обвинувачення в суді.

Розглянуті приклади підтверджують, що технологія цифрових відбитків пальця в деяких випадках може виявитися простим і ефективним інструментом для вирішення проблем в галузі захисту авторських прав, моніторингу в мережі конфіденційної інформації і ряду інших задач. Дана технологія може успішно застосовуватися разом з іншими методами контролю цифрових об’єктів.

6.3 Питання для самоконтролю знань

1. Наведіть класичні приклади ідентифікації об’єктів за відбитком.
2. Наведіть приклади застосування технології відбитка пальця для цифрових об’єктів.
3. Наведіть терміни, які застосовуються під час описування систем цифрових відбитків.
4. Які вимоги висуваються до систем реєстрації відбитка пальця.
5. Наведіть класифікацію підходів до реєстрації відбитка пальця на основі представлення даних.
6. Наведіть класифікацію підходів до реєстрації відбитка пальця на основі рівня чутливості виявлення об’єкта.
7. Наведіть класифікацію підходів до реєстрації відбитка пальця на основі використовуваного методу.
8. Наведіть класифікацію підходів до реєстрації відбитка пальця на основі вигляду відбитка.
9. Розкрийте статистичну схему реєстрації відбитка.
10. Розкрийте асиметричну схему реєстрації відбитка.
11. Розкрийте анонімну схему реєстрації відбитка.
12. Що таке центр реєстрації?

ВИСНОВКИ

В даний час характерною тенденцією в галузі захисту інформації є повсюдне впровадження криптографічних методів. Донедавна вони вважалися найнадійнішими гарантованими методами захисту інформації. Однак на цьому шляху багато ще невирішених проблем, пов'язаних з руйнівним впливом на криптографічні засоби таких складових інформаційної зброї, як комп'ютерні віруси, логічні бомби, автономні репликативні програми і т.п.

З появою глобальних мереж телекомунікацій стали актуальними проблеми, що пов'язані з необхідністю приховування самого факту передавання конфіденційної інформації. Рівень розвитку сучасних стеганографічних технологій дозволяє вже зараз вирішувати більшість виниклих задач. Причому частина з них добре вирішується на базі комп'ютерної стеганографії, а інша частина вирішується методами традиційної стеганографії на базі нових мікроелектронних технологій (наприклад, голографії).

Можливість ефективного приховування інформації в комп'ютерних системах і мережах має різні практичні наслідки. Незважаючи на молодість комп'ютерної стеганографії, уже сьогодні будь-який тип даних може бути прихований і невидимо переміщений. Створюючи певні зручності для збереження таємниці, комп'ютерна стеганографія одночасно створює умови для масових неконтрольованих соціально небезпечних каналів.

Прогрес в галузі стеганографії може кардинально змінити існуючі підходи до проблеми захисту інформації. Відомо, що загальна інтеграція є основною тенденцією розвитку систем забезпечення безпеки і систем зв'язку. В даний час широко надаються інтегральні послуги забезпечення безпеки. Аналіз стеганографічних і криптографічних технологій показує, що в найближчому майбутньому досить ймовірно їхнє зближення і подальша взаємна інтеграція (як це і було протягом багатьох століть). Об'єднання методів комп'ютерної стеганографії і криптографії було б гарним виходом з положення, що створилося. У цьому випадку вдалося б усунути слабкі сторони відомих методів захисту інформації і розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки. Ця обставина зможе забезпечити новий істотний підйом рівня захисту інформації під час її збереження і передавання загальнодоступними каналами зв'язку. Очевидно одне – майбутнє за комплексними рішеннями.

КОРОТКИЙ СЛОВНИК СТЕГАНОГРАФІЧНИХ ТЕРМІНІВ

Стеганографія (англ.: *steganography*) – науковий напрям інформаційної безпеки, який вивчає принципи, методи, технології та засоби приховування факту існування захищуваної інформації, предметом якої є також розроблення стеганографічних систем.

Комп'ютерна с. – наукова дисципліна, що вивчає принципи, засоби і методи організації прихованого передавання та/або зберігання інформації, реалізовані на базі комп'ютерних технологій.

Клептографія (англ.: *kleptography*) – науковий напрям, який вивчає принципи, методи, технології та засоби виявлення або створення прихованих від законного користувача каналів передавання інформації, у тому числі про діючу систему захисту.

Контейнер (англ.: *cover-<datatype>*) – будь-яка інформація (потік даних, файл та ін.), призначена для приховування інформації стеганографічним перетворенням.

Стегоконтейнер (*стегоб'єкт*, *стеганограма*) – контейнер (стеганотекст, стеганозвук, стеганозображення і т.п.), отриманий у результаті стеганографічного перетворення і такий, що містить приховану інформацію.

Порожній к. – контейнер без вбудованого повідомлення.

Потоковий к. – безперервний потік даних, призначений для приховування інформації в реальному масштабі часу.

Довільного доступу к. – файл фіксованої довжини з відомим вмістом, призначений для приховування даних.

Систематичний к. – контейнер, у якому можна вказати які біти відносяться до приховуваних даних, а які до них не відносяться.

Несистематичний к. – контейнер, у якому заздалегідь не можна виділити конкретні «шумові» біти, тому що кожний з них може нести інформацію про захищувані дані.

Приховане повідомлення – повідомлення, вбудоване в контейнер.

Стеганограф – програмний засіб, що забезпечує процес приховування і витягання приховуваної (закамуфльованої) інформації.

Стеганографічний алгоритм – набір математичних і логічних правил і процедур, за допомогою яких проводиться стеганографічне перетворення.

Стеганографічний аналіз (*стеганоаналіз*) – науково-технічна дисципліна, яка вивчає методи аналізу стегосистем, контейнерів і стегоб'єктів з метою оцінювання стеганографічної стійкості, визначення факту наявності прихованої інформації, доведення цього факту «третій особі», витягання прихованої інформації, а також її видалення або руйнування.

Стеганоаналітик (*противник, що атакує, цензор, несанкціонований користувач*) – суб'єкт, який, використовуючи математичні методи, обчислювальні і технічні засоби, проводить стеганографічні атаки на систему або ж оцінює її стеганографічну стійкість.

Стеганографічна атака – дії, спрямовані на виявлення і (або) витягання прихованої інформації з використанням стеганограми, наявних науково-технічних засобів і, можливо, деякої додаткової інформації, а також зміну або видалення прихованої інформації з контейнера.

Пасивна с. а. – атака на стегосистему з метою виявлення факту присутності прихованих даних та їхнього витягання.

Активна с. а. – атака на стегосистему з метою руйнування або зміни прихованих даних, навіть якщо точно не відомий факт їхньої присутності.

Стеганографічний канал (*стегоканал*) – канал передавання прихованого повідомлення.

Стеганографічний ключ (*стегоключ*, англ.: *stegokey*) – додаткові секретні дані, які необхідні для керування стеганографічним перетворенням. Якщо для приховування і витягання захищуваних даних потрібен той самий ключ, то він називається симетричним, у іншому випадку - асиметричним.

Стеганографічний метод – принцип реалізації стеганографічного перетворення.

Сурогатний м. – реалізує заміщення бітів контейнера бітами приховуваних даних.

Селективний м. – проводить вибір контейнера, що задовольняє властивості захищуваних даних.

Конструювальний м. – моделює властивості контейнера приховуваним повідомленням.

Структурний м. – використовує для приховування повідомлення семантичні і структурні параметри інформаційного середовища.

Стеганографічні перетворення – сукупність операцій, пов'язаних із приховуванням і витяганням приховуваної (закамуфльованої) інформації.

Приховування даних (*вбудовування*) – стеганографічне перетворення, проведене з захищуваними даними і інформаційним середовищем (контейнером) з метою отримання стеганограми.

Витягання даних - стеганографічне перетворення, що проводиться з метою витягання прихованих даних зі стеганограми.

Стеганотехнологія – сукупність методів підготовки, обробки, зміни стану і властивостей інформації, здійснюваних у процесі приховування та витягання переданого повідомлення.

Стеганографічна система (*стегосистема*, *стегозасіб*) – сукупність засобів і методів, що використовуються для формування прихованого каналу передавання або зберігання захищуваної інформації.

Теоретично стійка с. здійснює приховування інформації тільки в тих фрагментах контейнера, значення елементів яких не перевищують рівень шумів або помилок квантування, і при цьому теоретично доведено, що неможливо створити стеганоаналітичний метод виявлення прихованої інформації.

Практично стійка с. проводить такі модифікації контейнера, які у принципі можуть бути виявлені, але відомо, що на даний момент у противника поки відсутні необхідні засоби стеганографічного аналізу.

Нестійка с. приховує інформацію таким чином, що існуючі засоби стеганографічного аналізу дозволяють її виявити.

Стеганографічна стійкість – здатність стегосистеми протистояти атакам методами стеганалізу. У вузькому розумінні – це чисельна характеристика складності виявлення факту і витягання противником прихованих даних.

Цифрові водяні знаки (англ.: *digital watermarking*) – стеганографічна технологія, створена для захисту прав власності (*copyright marking*) стосовно до мультимедійної інформації.

Видимі ц.в.з. – візуальні мітки, які вставляються в цифрові дані (або записуються поверх них) для видимого «перекручування» цифрового об'єкта.

Напіввидимі ц.в.з. – мітки, які проставляються в цифрових об'єктах, не заважають сприйняттю, але у певних умовах можуть проявитися.

Невидимі ц.в.з. – мітки, які не призначені для загального огляду і використовується для полегшення роботи вузькоспеціалізованих пошукових систем для пошуку порушників авторських прав.

Крихкі ц.в.з. – мітки, які мають дуже обмежену стійкість до будь-яких змін, і використовуються для виявлення модифікацій маркірованих цифрових об’єктів.

Цифрові відбитки пальця (англ.: *digital fingerprinting*) – стеганографічна технологія, призначена для проставлення спеціальних міток у мультимедійні дані з метою здійснення контролю за їхнім розповсюдженням, дотримання ліцензійних угод і авторських прав, а також ідентифікації цифрових об’єктів, у яких мітка вже присутня.

Цифрова мітка – частина цифрового об’єкта, яка може приймати значення з деякої множини.

Цифровий відбиток – сукупність цифрових міток.

ЛІТЕРАТУРА

1. Шелест М. Е. Введение в компьютерную стеганографию : монографія / В.А. Хорошко, М.Е. Шелест. — К., 2002. — 139 с.
2. Хорошко Володимир Олексійович. Основи комп'ютерної стеганографії. Навчальний посібник / В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук. – Вінниця : ВДТУ. – 2003. – 143 с.
3. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.
4. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
5. Трубей А. И., Шелест М. Е. Обзор современных представлений о цифровой стеганографии // Научно-технический журнал «Проблемы защиты информации». – Минск: БГУ. 2007. – №3. С. 515
6. Задірака В. К. Аналіз стійкості стеганографічних систем в моделі пасивного противника / В. К. Задірака, Н. В. Кошкіна, О. С. Олексюк // Искусств. интеллект. — 2004. — N 3. — С. 801-805.
7. Конахович Г. Ф. Защита информации в телекоммуникационных системах / Г. Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. — К. : МК-Пресс, 2005. — 288 с.
8. Русин Б. П. Біометрична аутентифікація та криптографічний захист: монографія / Б. П. Русин, Я. Ю. Варецький; НАН України. Фіз.-мех. ін-т ім. Г. В. Карпенка. — Л. : Коло, 2007. — 287 с.
9. Кошкина Н. В. Анализ безопасности систем цифровых водяных знаков / Н. В. Кошкина // Компьют. математика: сб. науч. тр. — 2011. — Вып. 1. — С. 86-95. — Библиогр.: 15 назв. — рус.
10. Маракова И. И. Алгоритмы цифровых водяных знаков с точным восстановлением основных покрывающих сообщений / И. И. Маракова // Прав., нормат. та метрол. забезп. системи захисту інформації в Україні: наук.-техн. зб. — 2004. — Вип. 9. — С. 161-168.
11. Кобозева А. А. Анализ информационной безопасности: монографія / А. А. Кобозева, В. А. Хорошко. — К. : ГУИКТ, 2009. — 251 с.
12. Zheng L. Research on Vector Map Digital Watermarking Technology / L. Zheng, Y. Jia, Q. Wang. // First International Workshop on Education Technology and Computer Science – 2009. – P. 303 – 307.
13. *Cox I.J.* Secure spread spectrum watermarking for multimedia. Technical report, NEC institute, 2015.

14. *Wayner P.* If sb266 wants plaintext, give them plaintext // RISKS Digest, 11(71), may 1991.
15. *Wayner P.* Mimic function // Cryptologia v.XVI no 3 (july 1992), pp. 193-214.
16. *Moller S., Pfitzmann A., Stirand I.* Computer based steganography: how it works and why therefore any restriction on cryptography are nonsence, at best // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp. 7-21.
17. *Aura T.* Practical invisibility in digital communication // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp. 265-278.
18. *Fridrich J.* A new steganographic method for palette-based image // Proceedings of the ISBT PISP conference, Savannah, Georgia, Apr.1998, pp.285-289.
19. *Matsui K., Tanaka K.* Video-steganography: how to secret embed a signature in a picture // IMA intellectual property project proceeding, vol.1, no.1, 1994, pp.187-205.
20. *Zao J., Koch E.* Embedding robust labels into images for copyright protection // Proceeding of the international conference on intellectual property rights for information, knowledge and new techniques, Munchen-Wien, Verlag, 1995, pp.242-251.
21. *Smith J., Comiskey B.* Modulation and information hiding in image // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp.207-227.
22. *Pitas I.* A method for signature casting on digital images // International conference on image processing, vol.3, IEEE Press, 1996, pp.215-218.
23. Zheng L. Research on Vector Map Digital Watermarking Technology / L. Zheng, Y. Jia, Q. Wang. // First International Workshop on Education Technology and Computer Science – 2009. – P. 303 – 307.
24. Ohbuchi R. A shape-preserving data embedding algorithm for NURBS curves and surfaces / R. Ohbuchi, H. Masuda and M. Aono // Proc. Of Computer Graphics International'99[C], Canmore, Canada, 1999:170-177.
25. Sencar H. T. Data Hiding Fundamentals and Applications. / Husrev T. Sencar, Mahalingam Ramkumar, Ali N. Akansu. // Content Security İn Digital Multimedia Elsevier science and technology books, 2004. — 364 p.

26. Johnson N. F. İnformation Hiding: Steganography and Watermarking – Attacks and Countermeasures / Neil F. Johnson, Zoran Durič, Sushil Jajodia // Kluwer Academic Publishers, 2001. — 160 p.
27. Katzenbeisser S. İnformation Hiding Techniques for Steganography and Digital Watermark / Stefan Katzenbeisser, Fabien A. P. Petitcolas // Artech House Publishers, 1999. — 220 p.
28. Endoh U. Ueda and S. Endoh // in the IEEE International Conference on Multimedia and Expo 2002[C], Lausanne, Switzerland, 2002:577-580.
29. Sonnet H. Illustration watermarks for vector graphic" / H. Sonnet, T. Isenberg, J. Dittmann and T. Strothotte // Proceedings of 11th Pacific Conference on Computer Graphics and Applications, Canmore, Canada, 2003:73-82.
30. Voigt M. Watermarking 2D-vector data for geographical information system" / M. Voigt, and C. Busch // Proceedings of IS&T/SPIE Electron Imaging[C], Washington, America, 2002, 4675:621-628.
31. Voigt M. Feature-based watermarking of 2D-vector data" / M. Voigt and C. Busch. // Proceedings of SPIE[C], Santa Clara, 2003, 5020:359-366.
32. Schulz G. A high capacity watermarking system for digital maps" / G. Schulz and M. Voigt //ACM Mutimedia and Security Workshop 2004[C], Magdeburg, Germany, 2004:180-186.
33. Lianquan M. The digital watermark of vector geo-data / Min Lianquan // Bulletin of Surveying and Mapping, 2007,1:43-46.
34. Li Y. Copyright protection of the vector map using the digital watermark / Li Yuan-yuan and Xu Lu-ping // Journal of Xian University, 2004, 31(5):719-723.
35. Wang W. A robust watermarking algorithm for 2D vector graphics / Wang Wei and Li Ya // Journal of Image and Graphics, 12(2):200-205.
36. Shao C. Security issues of vector maps and a reversible authentication scheme / Shao Chengyong, Wang Xiaogong and Xu Xiaogang // Papers of 2005 Doctoral Forum of China, 2005, 326-331.
37. Jia P. Technical methods for encrypting and hiding digital watermark in GIS spatial data / Jia Peihong, Ma Jinsong, Shi Zhaoliang and Xu Zhizhong // Geomatics and Information Science of Wuhan University, 2004, 29(8):747-750.
38. Ma T. Watermarking algorithm on 2D vector digital maps / Ma Tallin, Gu Chong and Zhang Liangpei // Geomatics and Information Science of Wuhan University, 2006, 31(9):792-294.

39. Voigt M. Reversible watermarking of 2D vector data / M. Voigt, B. Yang and C. Busch // ACM Mutimedia and Security Workshop. – 2004, – P. 160 – 165.
40. Tie-Sheng F. Method of vector graphics digital watermarking based on B-spline / Fan Tie-Sheng, Meng Yao and Fang Xiao-bing // Computer Engineering and Applications, 2007, 43(17):69-70.
41. Wang X. A robust watermarking algorithm for vector digital mapping / Wang Xun, Lin Hai and Bao Hujun // Journal of computer-aided design & computer Graphics, 2004, 16(10):1377-1381.
42. Chang-qing Z. An anticompression watermarking algorithm for vector map data / Zhu Chang-qing, Yang Cheng-song and Li zhong-yua // Journal of Zhengzhou Institute of Surveying and Mapping, 2006, 23(4):281-283.
43. *Sandford M.T., Handel T.G., Ettinger J.M.* Data embedding method // Proceeding of the SPIE 2615, Integration issues in large commercial media delivery systems, 1996, pp.226-259.
44. *Коростиль Ю.М., Шелест М.Е.* Принципы построения стеганографических систем со структурной технологией // Праці VII міжнародної конференції з автоматичного управління «Автоматика-2000», Львів, вересень 2000 р., секція 7, частина 1. - Львів: ДНДІІІ. - С.286–273.
45. *Chang L., Moskowitz I.* Critical analysis of security in voice hiding techniques // First international conference «Information and communication security» ICIS’97, China, nov.11-14, 1997. Lecture notes in computer science, no.1334. - pp.203-215.
46. *Шелест М.Е.* Некоторые подходы к сокрытию информации в звуковой среде // Сборник научных трудов КМУГА «Защита информации». - Киев: КМУГА, 2000. – С.20–26.
47. *Мухачев В.А., Шелест М.Е.* Метод внедрения текстовых сообщений в звуковую среду музыкальных произведений // Збірник наукових праць Інституту проблем моделювання в енергетиці НАН України, вип.16. - Київ: ІПМЕ НАНУ, 2001.
48. *Мухачев В.А., Шелест М.Е.* Возможность скрытой передачи данных в криптопротоколах, основанных на свойствах эллиптических кривых // Науково-технічний збірник “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, вип.4. – Київ: КПІ, 2002.– С. 132–136.

49. *Kutter M., Petitcolas F.A.P.* Fair benchmarking for image watermarking system // Proceeding of the SPIE 3657, Security and watermarking of multimedia contents, 1999, p.226-239.
50. *Bender W., Gruhl D., Morimoto N.* Techniques for data hiding // Proceedings of the SPIE 2420, Storage and retrieval for image and video databases III, 1995, pp.164-173.
51. *Hartung F., Girod B.* Fast public-key watermarking of compressed video // International conference on image proceeding, Santa Barbara, California, oct.1997.
52. *Jonson N., Jajodia S.* Exploring steganography: seeing the unseen // IEEE Computer, vol.31, no.2, 1998, pp.26-34.
53. *Zhao J.* A WWW service to embed and prove digital copyright watermarks // Proceeding of the European conference on multimedia application, services and techniques, 1996, pp.695-709.
54. *O'Ruanaidh J., Pun T.* Rotation, translation and scale invariant digital image watermarking // International conference on image proceeding, Santa Barbara, California, oct.1997, pp.536-539.
55. *Antonini M.* Image coding using wavelet transform // IEEE Transactions on image processing, vol.1, no.2, 1992, pp.205-220.
56. *Xia X., Boncelet C., Arce G.* Wavelet transform based watermark for digital images // Optic express, vol.3, no.12, 1998, pp.497-511.
57. *Hartung F., Girod B.* Digital watermarking secure spread spectrum watermarking for multimedia // Proceeding of the IEEE International conference on acoustics, speech and signal processing, vol.4, Germany, Apr.1997, pp.2621-2624.
58. *Braudway G.* Protecting publicly-available image with an invisible image watermark // International conference on image proceeding, Santa Barbara, California, oct.1997.
59. *Delaige J.-F.* Digital image protection techniques in a broadcast framework: overview // Proceeding of the European conference on multimedia application, service and techniques, Louvain-la-Neuve, Belgium, May 1996, pp.711-728.
60. *Hayes M.H.* The reconstruction of a multidimensional sequence // IEEE Transactions on acoustics, speech and signal processing, Apr. 1992, pp.140-154.

61. *Kutter M., Jordan F., Bossen F.* Digital signature of color image using amplitude modulation // Proceeding of the SPIE 3022, storage find retraival for image and video database *V*, 1997, pp.518-526.
62. *Koch E., Zhao J.* Towards robust and hidden image copyright labeling // IEEE workshop on nonlinear signal and image processing, Thessaloniki, Greece, Oct. 1995, pp.452-455.
63. *Bruyndonckx O., Quisquater J.-J., Macq B.* Spatial method for copyright labeling on digital images // Nonlinear signal processing workshop, Thessaloniki, Greece, 1995, pp.456-459.
64. *Puate J., Jordan F.* Using fractal compression scheme to embed a digital signature into an image // Proceeding of the SPIE 2915, Video techniques and software for full-service network, 1996, pp.108-118.
65. "Talisman" <htpp://www.cordis.lu/espirit/src/talisman.htm>.
66. *Wagner N.R.* Fingerprint // Proceeding of the 1983 IEEE symposium on security and privacy, Oakland, California, USA, Apr.1983, pp.18-22.
67. *Pfitzmann B., Schunter M.* Asymmetric fingerprint // Advances in cryptology, Proceeding of EUROCRYPT'96, vol.1070 of lecture notes in computer science, Springer-Verlag, 1996, pp.84-95.
68. *Chaum D.* Blind signature for untraceable payment // Advances in cryptology proceeding of CRYPTO'82, Plenum press, 1983, pp.199-203.

Навчальне видання

Хорошко Володимир Олексійович
Яремчук Юрій Євгенович
Карпінець Василь Васильович

КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ

Навчальний посібник

Редактор В. Дружиніна

Оригінал-макет підготовлено В. Карпінцем

Підписано до друку
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк.
Наклад …. пр. Зам. № 2015-

Видавець та виготовлювач
Інформаційний редакційно-видавничий центр
ВНТУ, ГНК, к.114.
Хмельницьке шосе, 95.
м. Вінниця, 21021
Тел. (0432) 59-85-32, 59-87-38.
press.vntu.edu.ua;
kvic.vntu@gmail.com

Свідоцтво суб'єкта видавничої справи
Серія ДК №3516 від 01.07.2009 р.