УДК 004.93

В. Р. Стружко, С. В. Антоненко, Н. Є. Сегеда

Дніпровський національний університет імені Олеся Гончара

ОГЛЯД ІСНУЮЧИХ МЕТОДІВ ТА АЛГОРИТМІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ЦИФРОВИХ СИГНАЛАХ

В даній статті основну увагу приділено дослідженню існуючих методів та алгоритмів приховування інформації в цифрових сигналах з метою подальшого створення інформаційної технології приховування інформації в цифрових сигналах.

Ключові слова: *стеганографія, методи приховування даних, аудіосигнал, зображення.*

In this article, the main attention is paid to the research of existing methods and algorithms for hiding information in digital signals with the aim of further creating information technology for hiding information in digital signals. Steganographic studies are based on insufficient reliability of the cryptographic systems themselves and the ambitions to full secrecy in an open system environment. Governments in many countries have passed laws that limit the reliability of cryptosystems or forbid them altogether. Badly that this leaves most of the internet community with enough weak and often faulty encryption algorithms, or generally without them. That's why steganography comes to the rescue. You can use steganography to hide sensitive data in some file and only sides who wish to receive the message know that the message is secret. The development of computer technology in recent decades has given a new impetus to the development of computer steganography. Many new areas of application have appeared. Messages are now embedded in digital data, usually analog in nature. These are speech, audio recordings, images, videos. There are also ideas for embedding information in text files and executable files, This science has generated a lot of interest in recent years, especially in the field of computer security, as it has been used by criminal and terrorist organizations. However, this is nothing new, as it has been in use since ancient times and has traditionally been used by police, military and intelligence agencies, as well as criminals or civilians wishing to escape state control, especially in tyrannical regimes. Classical steganography was solely based on ignoring the covert channel in use, whereas in the modern era, digital channels (image, video, audio, and communication protocols) are also used to achieve the goal. In many

cases, the container object is known, but the algorithm for inserting information into the specified object is unknown.

Key-words*: steganography, data hiding methods, audio signal, image***.**

Стеганографічні дослідження базуються на недостатній надійності самих криптографічних систем і прагненні до повної секретності у відкритому системному середовищі. Уряди багатьох країн прийняли закони, які обмежують надійність криптосистем або взагалі забороняють їх. Погано, що це залишає більшість інтернет-спільноти з досить слабкими і часто несправними алгоритмами шифрування або взагалі без них. Тому на допомогу приходить стеганографія. Стеганографію можна використовувати, щоб приховати конфіденційні дані в якомусь файлі, і лише ті сторони, які бажають отримати повідомлення, знають, що повідомлення секретне.

Вступ. Швидке зростання інформаційних та комунікаційних технологій в останні роки призвело до повсякденного використання цих технологій у нашому повсякденному житті: від обміну інформацією з нашими друзями та сім'єю через загальнодоступний канал передачі, такий як Інтернет, до здійснення платежу за допомогою нашої кредитної картки в інтернет-магазині. Однією з найпоширеніших проблем, із якими стикаються засоби зв'язку, є безпека передачі. З моменту зародження людства було надзвичайно важливо мати можливість безпечно передавати важливу інформацію, тому для вирішення цієї проблеми з'явилося кілька методів. Більшість цих рішень посідає використання криптографії. Стеганографія є альтернативним вирішенням цієї проблеми, оскільки, використовуючи цю техніку, можливо підтримувати секретне чи непомітне спілкування третіх осіб, які хочуть проникнути у спілкування.

Приховування даних у зображеннях. Кодування секретних повідомлень у цифрових зображеннях є, безумовно, найпоширенішим із усіх методів у сучасному цифровому світі. Це пояснюється тим, що він може використовувати переваги обмеженої потужності зорової системи людини. Майже будь-який простий текст, зашифрований текст, зображення та будь-який інший носій, який можна закодувати в бітовий потік, можна приховати в цифровому зображенні. З безперервним зростанням високої потужності графіки в комп’ютерах і дослідженнями стеганографії на основі зображень ця галузь продовжуватиме розвиватися дуже швидкими темпами.

Приховування даних зазвичай включає методи приховування даних у просторовій області, наприклад, вбудовування найменшого значущого біта (LSB) [1], який передбачає зміну значень пікселів

зображення для вбудовування прихованого повідомлення або даних або методи частотної області, які змінюють дані таким чином, що прихована інформація стає непомітною для людського ока. Нижче розглянемо методи LSB, частотний діапазон [2] та Patchwork [3].

Least Significant Bit (LSB) Insertion. Методи модифікації LSB є простими способами вбудовування інформації, але вони дуже вразливі навіть до невеликих змін контейнера (тобто зображення). Зловмисник може просто застосувати методи обробки сигналу, щоб повністю знищити секретну інформацію. У багатьох випадках навіть невеликі зміни в результаті стиснення з втратами призводять до повної втрати інформації. На початку розробки стеганографічних систем було зазначено, що вбудовування інформації в частотну область сигналу може бути набагато надійнішим, ніж правила вбудовування, що діють у часовій області. Більшість надійних стеганографічних систем, відомих сьогодні, фактично працюють у певному домені трансформації. Методи домену трансформації приховують повідомлення у значних областях зображення обкладинки, що робить їх більш стійкими до атак, таких як стиснення, кадрування та деяка обробка зображень, ніж підхід LSB. Однак, незважаючи на те, що вони більш стійкі до різних видів обробки сигналів, вони залишаються непомітними для сенсорної системи людини. Існує багато варіацій домену перетворення. Одним із методів є використання дискретного косинусного перетворення (ДКП) як засобу для вбудовування інформації в зображення; іншим було використання вейвлет-перетворень. Трансформації можуть бути застосовані, наприклад, до зображення цілком або до блоків у всьому зображенні. Однак існує компроміс між кількістю інформації, доданої до зображення, та отриманою надійністю. Багато методів домену перетворення не залежать від формату зображення та можуть витримувати перетворення між форматами без втрат і з втратами.

Двовимірне ДКП є «серцем» найпопулярнішої системи стиснення цифрових зображень із втратами, яка використовується сьогодні: системи JPEG. JPEG спочатку перетворює зображення, яке потрібно стиснути, у колірний простір YCbCr і розбиває кожну колірну площину на 8 x 8 блоків пікселів. Потім усі блоки перетворюються ДКП. На етапі квантування всі коефіцієнти ДКП діляться на деякі попередньо визначені значення квантування і округлюються до найближчого цілого числа (відповідно до фактора якості, значення квантування можуть бути масштабовані константою). Метою цього процесу є модулювання впливу різних спектральних компонентів на зображення. Зокрема, зменшується вплив найвищих коефіцієнтів ДКП: у них,

імовірно, переважатиме шум і не очікується, що вони внесуть суттєві деталі в картину. Отримані квантовані коефіцієнти ДКП стискаються за допомогою ентропійного кодера (наприклад, Хаффмана або арифметичного кодування). На етапі декодування JPEG усі коефіцієнти ДКП деквантуються (тобто множаться на значення квантування, які використовувалися на етапі кодування). Після цього для реконструкції даних виконується зворотний ДКП. Відновлене зображення буде близьким (але не ідентичним) оригінальному; але якщо значення квантування були встановлені належним чином, для людини-спостерігача не повинно бути помітної різниці.

Коли мова йде про цифрові зображення для використання зі стеганографією, типовими є 8-бітні та 24-бітові файли зображень на піксель. Обидва варіанти мають переваги та недоліки. 8-бітні зображення є чудовим форматом для використання через їх відносно невеликий розмір. Недоліком є те, що можна використовувати лише 256 можливих кольорів, що може бути потенційною проблемою під час кодування. Зазвичай колірна палітра сірої шкали використовується при роботі з 8-бітними зображеннями, оскільки поступову зміну кольору буде важче виявити після того, як зображення було закодовано секретним повідомленням. 24-бітні зображення пропонують набагато більшу гнучкість при використанні для стеганографії. Велика кількість кольорів (понад 16 мільйонів), які можна використовувати, виходять далеко за межі зорової системи людини, що робить дуже важко виявити секретне повідомлення, яке закодовано. Інша перевага полягає в тому, що набагато більший обсяг прихованих даних може бути закодований у 24-бітне цифрове зображення на відміну від 8-бітного цифрового зображення. Основним недоліком 24-розрядних цифрових зображень є їх великий розмір (зазвичай у МБ), що робить їх більш підозрілими, ніж набагато менші 8-бітні цифрові зображення (зазвичай у КБ), коли вони надсилаються через відкриту систему.

Частотний діапазон — це метод приховування даних у зображеннях, який передбачає маніпулювання частотними коефіцієнтами зображення за допомогою математичного процесу, що називається перетворенням Фур'є. У цій техніці зображення спочатку перетворюється в частотну область за допомогою двовимірного перетворення Фур'є. Це перетворює зображення з просторової області, де зображення представлено у вигляді піксельної сітки, у частотну область, де зображення представлено як набір частотних коефіцієнтів. Частотні коефіцієнти представляють вміст просторової частоти зображення, який можна розглядати як швидкість зміни інтенсивності

зображення по всьому зображенню. Маніпулюючи цими коефіцієнтами, можна вбудувати приховане повідомлення в зображення. Один із способів вбудувати повідомлення полягає в модифікації молодших бітів частотних коефіцієнтів.

Це схоже на техніку вбудовування LSB, яка використовується в просторовій області, але замість зміни значень пікселів модифікуються частотні коефіцієнти. Після того, як повідомлення було вбудовано в частотні коефіцієнти, зображення перетворюється назад у просторову область за допомогою зворотного перетворення Фур'є. Отримане зображення виглядає майже ідентично оригінальному зображенню, але містить приховане повідомлення. Техніка частотної області є більш складною, ніж техніка вбудовування LSB, але забезпечує більш високий рівень безпеки, оскільки її важче виявити. Однак цей метод також потребує більшої обчислювальної потужності та може бути більш вразливим до атак, характерних для частотної області.

Patchwork. Цей метод використовує псевдовипадковий генератор для вибору n пар пікселів і трохи збільшує або зменшує їх яскравий контраст. Таким чином, контраст цього набору збільшується без будь-яких змін у середній яскравості зображення. З відповідними параметрами Patchwork навіть витримує стиснення за допомогою JPEG. У своїй основній формі цей алгоритм здатний кодувати та декодувати одну конкретну позначку або біт у зображенні. Цей знак можна інтерпретувати як незалежне кодування, яке вказує, чи містить відповідне зображення водяний знак чи існує як частина більшої схеми кодування, наприклад контрольний номер. Щоб вставити більше, можна спочатку розділити зображення на частини, а потім застосувати вбудовування до кожної з них.

Однією з найважливіших характеристик Patchwork є його стійкість до більшості негеометричних модифікацій зображення, таких як корекція гами та шкали тонів, які зазвичай змінюють яскравість пікселів, не порушуючи печворк, який використовує міру різниці для роботи. Але Patchwork руйнується будь-яким афінним перетворенням, таким як обертання чи масштабування.

Приховування даних у аудіосигналах. Кодування секретних повідомлень у аудіо є найскладнішою технікою, яка використовується під час роботи зі стеганографією. Це тому, що слухова система людини (ССЛ) має такий динамічний діапазон, що вона може слухати. ССЛ сприймає в діапазоні потужностей понад один мільярд до одного та в діапазоні частот понад тисячу до одного. Чутливість до адитивного випадкового шуму також є гострою. Збурення у звуковому файлі можна

виявити лише в одній частині з десяти мільйонів. Однак у цьому діапазоні перспективи є деякі «діри», де дані можуть бути приховані. Хоча ССЛ має великий динамічний діапазон, він часто має досить малий диференціальний діапазон. У результаті гучні звуки мають тенденцію маскувати тихі звуки. Існують деякі викривлення навколишнього середовища настільки поширені, що слухач у більшості випадків ігнорує їх.

Розглянемо методи модифікації фази [4], розширення спектру [5] та приховування відлуння [3].

Метод модифікації фази. Метод фазового кодування працює шляхом заміни фази початкового сегмента аудіо на опорну фазу, яка представляє дані. Фаза наступних сегментів регулюється, щоб зберегти відносну фазу між сегментами. Це один із найефективніших методів кодування з точки зору співвідношення сигнал/шум, що сприймається. Коли фазове співвідношення між кожною частотною складовою різко змінюється, виникне помітна фазова дисперсія. Однак, поки модифікація фази досить мала, можна досягти нечутного кодування. Для процесу декодування синхронізація послідовності виконується перед декодуванням. Одержувачу мають бути відомі довжина сегмента, точки дискретного перетворення Фур'є та інтервал даних. Значення базової фази першого сегмента визначається як 0 або 1, що представляє закодований двійковий рядок.

Однією з потенційних переваг цього методу є те, що зловмиснику може бути дуже важко виявити наявність вбудованої інформації. Це пов'язано з тим, що для зловмисника, який не знає про конкретні частоти та алгоритми, що використовуються для вбудовування, модифікований аудіосигнал може здатися невідрізним від оригінального аудіосигналу. Однак один потенційний недолік цього методу полягає в тому, що він може внести спотворення та артефакти в аудіосигнал, що може вплинути на якість звуку.

Розширення спектру. Основна ідея розширення спектру полягає в тому, щоб поширити секретне повідомлення в широкому діапазоні частот, щоб підслухувачу було важко виявити та вилучити повідомлення. У режимі приховування звуку розширений спектр досягається додаванням шумового сигналу низького рівня до звукового сигналу. Сигнал шуму призначений для поширення в широкому діапазоні частот і модулюється секретним повідомленням. Результатом є модифікований аудіосигнал, який містить як оригінальний аудіовміст, так і приховане повідомлення, але його неможливо відрізнити від оригінального сигналу.

Техніка розширеного спектру має кілька переваг перед іншими методами приховування звуку. По-перше, він стійкий до різних типів перешкод і шумів сигналу, що робить його більш міцним і надійним. По-друге, важко виявити та витягти приховане повідомлення, навіть якщо підслухувач знає, що воно присутнє в звуковому сигналі. Нарешті, техніка є гнучкою і може бути адаптована до різних аудіоформатів і швидкості передачі даних, залежно від вимог програми. Існує декілька варіацій зв'язку з розширеним спектром, один з яких кодування з розширеним спектром прямої послідовності (DSSS) [6]. Метод DSSS розповсюджує сигнал шляхом множення його на чіп, псевдовипадкову послідовність максимальної довжини, модульовану з відомою швидкістю. Оскільки сигнали хоста є у форматі дискретного часу, ми можемо використовувати частоту дискретизації як частоту чіпу для кодування. Результатом є те, що найскладніша проблема в отриманні DSSS, а саме встановлення правильного початку та кінця квантів чіпа для цілей синхронізації фаз, вирішується дискретною природою сигналу. Отже, можлива набагато вища швидкість мікросхеми, а отже, і вища пов'язана швидкість передачі даних. Без цього можна використовувати різноманітні алгоритми блокування сигналу, але вони дорогі з точки зору обчислень

Приховування відлуння. Поширеним підходом до приховування даних у аудіо є представлення даних як шуму. Недоліком цього підходу є те, що алгоритми стиснення даних із втратами прагнуть видалити більшість непомітних артефактів, включаючи типовий шум із низьким рівнем дБ. Приховування відлуння вносить зміни в аудіосигнал хоста, характерні для умов навколишнього середовища, а не випадкового шуму, тому воно є надійним у світлі багатьох алгоритмів стиснення даних із втратою даних. Як і всі хороші стегонаграфічні методи, приховування відлуння спрямоване на вбудовування даних у медіа-потік із мінімальним погіршенням оригінального медіа-потоку. Під мінімальним погіршенням ми маємо на увазі, що зміна в обкладинці звуку є або непомітною, або просто відкидається слухачем як звичайне спотворення середовища, яке не викликає заперечень. Конкретне спотворення, яке ми вводимо, подібне до резонансів, які виникають у кімнаті через стіни, меблі тощо. Різниця між стего-аудіо та звуком контейнера подібна до різниці між прослуховуванням компакт-диска в навушниках і прослуховуванням з колонок. У навушниках ми чуємо звук таким, яким він був записаний. За допомогою динаміків ми чуємо звук і відлуння, спричинені акустикою приміщення. Правильно вибравши спотворення, яке ми вводимо для приховування відлуння, ми

можемо зробити такі спотворення невідрізними від тих, які кімната може внести у вищевказаний корпус динаміка. Однак при додаванні цих резонансів слід бути обережним. Існує момент, коли додаткові резонанси сильно спотворюють звук обкладинки. Можливо регулювати кілька параметрів відлуння, що дає нам контроль як над ступенем, так і над типом введеного резонансу. Завдяки ретельно підібраним параметрам додані резонанси можна зробити непомітними для звичайного слухача. Таким чином, можливо використовувати межі дискримінаційної здатності ССЛ приховувати дані в потоці аудіоданих.

Висновок. У цій роботі було проведено огляд існуючих рішень приховування інформації в цифрових сигналах. Були розглянуті методи LSB, частотний діапазон та Patchwork для роботи з зображеннями. Також були розглянуті методи модифікації фази, розширення спектру та приховування відлуння для роботи з аудіосигналами відповідно. Наступним кроком у цій праці буде розроблення інформаційної технології для експериментального підтвердження теоретичних аспектів стосовно приховування інформації, а саме реалізація модулю для приховування інформації в аудіосигналах.

Бібліографічні посилання

1. **Katzenbeisser S., Petitcolas F.A.P**. Information Hiding Techniques for Steganography and Digital Watermarking, – 2000.

2. **Broughton S.A., Bryan K.** Discrete Fourier Analysis and Wavelets: Applications to Signal and Image Processing, – 2008.

3. **Bender W., Gruhl D., Morimoto N., Lu A**. Techniques for data hiding, – 1996.

4. **Dong X., Bocko M.F., Ignjatovic Z.** Data hiding via phase manipulation of audio signals, – 2004.

5. **Malvar H., Florencio D**. Improved spread spectrum: a new modulation technique for robust watermarking, – 2004.

6. **Yu W., Fu X., Graham S., Xuan D., Zhao W**. DSSS-based flow marking technique for invisible traceback, – 2007.

Надійшла до редколегії 04.11.2022