DOI: 10.18372/2310-5461.62.18714
УДК 004.622: 517.927

О. В. Слободянюк
Кам'янець-Подільський національний університет
імені Івана Огієнка
orcid.org/0000-0001-5195-3053
e-mail: slobodianiuk@kpnu.edu.ua;

А. І. Костромицький, канд. техн. наук, доцент
Харківський національний університет радіоелектроніки
orcid.org/0000-0003-3434-0815
e-mail: andrii.kostromytskyi@nure.ua;

В.Б. Чебаненко, мол. наук. співр.
Харківський національний університет
Повітряних Сил імені Івана Кожедуба
orcid.org/0009-0005-5650-5547
e-mail: viktor.chb.2018@gmail.com;

М. М. Дігтярь,
Харківський національний університет Повітряних Сил
Імені Івана Кожедуба
orcid.org/0000-0001-9208-7593
e-mail: degtiar@gmail.com;

П. М. Онипченко, канд. пед. наук, доцент
Харківський національний університет Повітряних Сил
orcid.org/0000-0003-4497-327X
e-mail: onipchenko.pm@gmail.com

LSB МЕТОДИ ПРИХОВАНОЇ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ (ОГЛЯД)

Вступ

Методи приховування повідомлень мають на меті забезпечити безпеку передачі конфіденційної інформації, роблячи її недоступною для незаконного доступу та виявлення. Один із таких методів – стеганографія, який є досить неочевидним та майбутнім напрямком в цій області.

У стеганографії використовуються мультимедійні дані для приховування секретних повідомлень. Найчастіше в якості контейнерів для цього використовуються зображення або текстові документи, але також можуть використовуватися аудіодані. Суть методу полягає у вбудовуванні конфіденційної інформації в видимий текст, не змінюючи самого тексту або файлу. Призначенням стеганографії є забезпечення такого приховування, щоб навіть існуючий файл або повідомлення не викликали підозри у наявності прихованої інформації.

Принциповою перевагою стеганографії є те, що вона доповнює шифрування, роблячи дані менш очевидними для виявлення. Цей метод дозволяє підвищити рівень безпеки передачі інформації, забезпечуючи додатковий рівень захисту.

Згадані вище аспекти стеганографії – місткість, безпека та надійність – визначають її ефективність. Місткість вказує на здатність методу вміщати в себе достатню кількість секретної інформації без помітного збільшення розміру контейнера. Безпека означає здатність забезпечити високий рівень невидимості прихованих даних для сторонніх користувачів. Надійність полягає в забезпеченні стійкості до будь-яких змін або атак на приховану інформацію під час передачі.

Постановка проблеми

Стеганографія, так само як і криптографія, призначена для захисту повідомлень та даних від несанкціонованого доступу, але вони використовують альтернативні методи забезпечення безпеки. Іншим важливим аспектом є відеостеганографія, яка використовується для приховування будь-яких файлів у текстових, аудіо- або відеофайлах. Розділення відео на аудіо та зображення

або кадри дозволяє підвищити ефективність методу, роблячи його менш помітним для недобросовісних користувачів.

Мета даного дослідження полягає у подальшому розвитку та вдосконаленні методів стеганографічного приховування даних на основі аналізу найменш значущого біту повідомлення в контейнерах з мультимедійними даними. Пропонується новий метод стеганографічного маскування інформації у файлах, що містять звукові та графічні дані. Проведені дослідження спрямовані на збільшення ефективності та надійності процесу приховування конфіденційної інформації у мультимедійних файлах, що дозволить зберігати та передавати дані з вищим рівнем захищеності. Проводиться розробка нового методу стеганографічного маскування інформації у файлах, що містять звукові та графічні дані.

Аналіз останніх досліджень і публікацій

Методи приховування повідомлень, які гарантують, що їх неможливо розшифрувати та виявити, включають в себе багато підходів та напрямків. Одним із найбільш неявних і перспективних є стеганографічний метод приховування. Мультимедійні дані зазвичай використовуються для передачі секретних повідомлень. Найпоширеніші контейнери для передачі прихованих даних – це зображення або текстові документи. Однак для цього також можна використовувати аудіодані. Метод стеганографії передбачає приховування конфіденційної інформації у відкритому тексті, не секретному файлі або повідомленні, щоб її неможливо було виявити. Потім конфіденційна інформація буде вилучена з відкритого файлу або повідомлення до місця призначення, таким чином уникаючи виявлення. Стеганографія – це додатковий крок, який можна використовувати разом із шифруванням для приховування або захисту даних.

Стеганографія і криптографія призначені для захисту повідомлень і даних від несанкціонованого доступу на найфундаментальнішому рівні. Однак вони використовують альтернативні засоби безпеки.

Відеостеганографія – це метод приховування будь-яких файлів у текстовому, аудіо- чи відеофайлі. Поділ відео на аудіо та зображення або кадри призводить до підвищення ефективності методу.

Три основні аспекти стеганографії - це місткість, безпека та надійність [2, 4, 5, 7]. Безпека пов’язана зі здатністю забезпечення відповідного рівня надійності маскування секретних даних. Такого, щоб перехоплювачі таємного повідомлення не могли помітити наявні вбудовані секретні дані. Отримувач та відправник для надійності використовують той самий ключ кодування та декодування. Це пов’язано із стійкістю до модифікації прихованої інформації при передачі у відкритих канал мережі Інтернеті та локальних чи публічних мережах.

Останні дослідження в галузі LSB (Least Significant Bit) методів стеганографії свідчать про постійний розвиток цього напрямку та пошук нових можливостей для покращення ефективності та безпеки приховування інформації. Наразі активно досліджується використання алгоритмів машинного навчання для оптимізації LSB методів та зменшення відкритих текстурних артефактів. Деякі дослідження фокусуються на використанні LSB методів у різних медичних застосуваннях, зокрема у передачі медичних зображень та даних пацієнтів з використанням стеганографії.

Одним зі значущих досліджень у цій області є стаття «A Survey on Least Significant Bit Based Steganography Techniques and Algorithms» [5], яка систематизує та аналізує різноманітні методи та алгоритми LSB стеганографії. Дослідження зосереджується на порівнянні різних підходів та їх ефективності з точки зору стійкості до атак та якості приховування.

Ще одним важливим джерелом є публікація «A Comprehensive Review on LSB based Steganography Techniques» [3], де автори детально розглядають різноманітні методи та їх застосування в різних областях, включаючи зображення, відео та аудіо дані. Дослідження вказує на потенційні переваги та обмеження LSB методів, а також на можливі шляхи подальшого розвитку.

Певного вкладу у дослідження LSB методів стеганографічного приховування інформації також доклали й наші українські науковці. О. К. Юдін у статті «Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів» [2] та О.І. Стасюк у роботі «Сучасні стеганографічні методи захисту інформації» [1] провели аналіз та навели основні аспекти розробки й особливості та використання LSB-методів у стеганографії.

Інші дослідження, такі як [4, 7, 8, 9] зосереджуються на аналізі LSB стеганографії в контексті аудіо даних та впливі різних бітових площин на якість та стійкість прихованого повідомлення.

Актуальність розробки нового методу стеганографічного приховування полягає в постійній потребі в покращенні ефективності та безпеки передачі конфіденційної інформації. З розвитком технологій та зростанням кількості цифрових даних, виникають нові виклики у забезпеченні

захищеності цих даних від несанкціонованого доступу та виявлення. Таким чином, створення нового методу стеганографічного приховування, який би відповідав сучасним вимогам безпеки та ефективності, має велике значення. Розробка нових методів стеганографічного приховування повинна включати такі кроки як: аналіз існуючих методів, аналіз їх необхідності та визначення потреб для конкретної прикладної задачі чи випадку та власне розробка алгоритму.

Класифікація методів стеганографії, що працюють з аудіоконтейнерами

При створенні нових алгоритмів стеганографічного приховування необхідно закладати вимоги щодо обов'язкового врахування й ідентифікації потреб кінцевих користувачів та вдосконалення існуючих підходів, проведення тестування нових методів на різнотипних наборах даних та аналізу їх ефективності в порівнянні з існуючими методами. Оцінка безпеки нового методу також є обов'язковою вимогою, яка дозволяє визначити рівень його стійкості до різних видів атак та забезпечення конфіденційності прихованої інформації.

Одним із найперспективніших напрямків розвитку стеганографії на даний момент є біостеганографія. Будь яке повідомлення можна зашифрувати та приховати його у мікро крапки. Однак у цьому випадку це не графічні примітиви у зображенні на папері чи екрані графічного дисплею, а мікро крапки, що поміщені у код ДНК. При цьому текстове повідомлення, спочатку шифрується, а потім усі літери, з яких складається зашифроване повідомлення, перетворюються на комбінації тиміну (T), аденіну (A), цитозину (C) і гуаніну (G). При цьому створюються синтетичні нитки ДНК. Тобто ми створюємо синтезовану ДНК з аденіном, цитозином, гуаніном і тиміном у послідовності, що відповідає порядку бітів у цифровому файлі. Крихітний шматочок ДНК із повідомленням потім поміщають у звичайний шматочок ДНК, який потім змішують із ланцюжками ДНК такої ж довжини. Потім суміш сушиться на папері, який можна розрізати на мікрокрапки, кожна з яких містить мільярди ниток ДНК. Це дуже важко виявити, і лише одна нитка з мільярдів ниток у мікрокрапці містить повідомлення.

Класичну схема типового алгоритму приховування даних за допомогою стегонографічного підходу можна представити у вигляді схеми, показаної на рис. 1.

В аудіо стеганографії використовується недосконаліть слухової системи людини та наявність надлишкової службової інформації у форматах аудіофайлів [2].

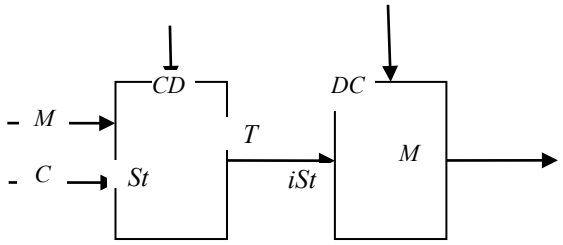

Рис. 1. Схема приховування секретного повідомлення для передачі в каналах зв'язку:
M – секретне повідомлення; *C* – обкладинка даних; *CD* – стегокодер; *DC* – стего-декодер; *T* – канал передачі; SMF – файл із зашифрованим повідомленням; *St* – стегофункція; *iSt* – обернена стегофункція [3]

Залежно від методу, який використовується для обробки сигналу, стеганографічні методи для приховуваня даних в аудіо можна розділити на ті, що працюють у часовій області та методи, що використовують частотні спектри. У техніках часової області фактичні зразки сигналу повідомлення модифікуються таким чином, щоб вставити сигнал повідомлення, який потрібно приховати. До цієї категорії підпадають такі методи, як заміна LSB, приховування ехосигналів та тимчасове маскування. З іншого боку, у методах перетворення спектру об'єкт покриття змінюється на інший для того, щоб отримати коефіцієнти трансформації. Ці коефіцієнти видозмінюються і в подальшому проводиться вбудовування в них секретного повідомлення. При цьому використовуються такі відомі перетворення як як швидке перетворення Фур'є (FFT), дискретне косинусне перетворення (DCT), дискретне вейвлет-перетворення (DWT) тощо. Деякі з часто використовуваних методів перетворення у часовій області – це частотне маскування, метод розширеного спектру та методи фазового кодування [4, 7].

1) Методи, засновані на принципах HAS.

Методи, засновані на принципах HAS (human auditory system), базуються на здатності сприйняття слухової системи людини і психоакустичних властивостях мови. Техніка звукових водяних знаків, заснована на принципах HAS, практикується із самих ранніх етапів розвитку стеганографії. Наслідками HAS по відношенню до стеганографії є часове маскування та частотне маскування. Техніка маскування, в якій звуковий сигнал з меншою інтенсивністю по обидва боки від гучного маскування стає нечутним для людського вуха відомий як тимчасове маскування. Якщо ми почуємо звук імпульсу, нашому вуху потрібен короткий час, щоб почути тихий звук після нього. Ми не можемо почути тихий звуковий сигнал протягом такого короткого часу після цього інтенсивного звуку. Таким чином, інтенсивний звуковий сигнал можна використовувати

для негайного маскування цього тихого сигналу після нього. З іншого боку, маскування частоти відбувається, коли звук, амплітуда якого знаходиться в межах чутного діапазону, маскується звуком із сусідньою частотою. Також зазначені методи часто використовують характеристики чутливості HAS. Під час обробки даних застосовується амплітудне дискретне перетворення Фур'є (ДПФ) відносно фазової області несучої сигналу та характеристики шуму, які присутні в оригінальних вихідних звукових сигналах для включення повідомлення, яке потрібно приховати. Ці методи надійні для стиснення аудіорівня з експертної групи рухомих зображень (MP3) і забезпечують високу ємність вбудовування. Але у них погана непомітність.

Також до даної групи методів відносяться алгоритми, які визначають декілька аудіорозташувань у сигналі приймача на основі часових характеристик HAS. Ця техніка використовує оборотне двовимірне цілочисельне перетворення та використовує той факт, що помірні спотворення поблизу гучного звуку не чутні. Період часу маскування після звуку високої гучності зазвичай довший порівняно з попереднім. Тому кадр-кандидат вибирається у відносно тихому сегменті відразу після звуку високої гучності. Цей метод стійкий до стиснення MP3 і дозволяє ідеально відтворити вихідний сигнал.

2) Методи, засновані на лінійному прогнозуючому кодуванні (LPC).

LPC (linear predictive coding) — це цифровий метод, у якому безперервний сигнал, що змінюється в часі, кодується шляхом передбачення певного значення сигналу з попереднього значення сигналу за допомогою лінійної функції. Він використовується в області обробки мови для зображення стиснутої форми спектральної несучої цифрового голосового сигналу. Запропонована методика є потужною методикою аналізу мовлення. Це важливий спосіб кодування високоякісних мовних сигналів із низькою швидкістю передачі даних. Однак метод LPC страждає від недоліку зниження якості голосового сигналу, а дані пошкоджуються та стають нерозбірливими, якщо вони передаються на велику відстань через певну кількість проміжних комутуючих вузлів.

3) Методи на основі обробки вейвлет-доменів.

Це методи доменної трансформації Серед усіх цих методів дискретне вейвлет перетворення (DWT) вважається одним із найкращих методів для приховування даних, оскільки за допомогою нього отримується частотний вміст функції як функцію часу. DWT не дає жодної інформації про час, тоді як DCT створює проблеми з артефактами. Ці методи домену перетворення порівняно менш стійкі до шуму.

Інший метод кодування мовних сигналів за допомогою вейвлет-перетворення пропонує наступний алгоритм. Зашифроване приховане повідомлення вставляється в цілочисельні коефіцієнти вейвлет-перетворення оригінального звукового сигналу. Цей метод має обмеження щодо максимальної кількості бітів, які можна вставити в ці коефіцієнти без відчутного спотворення звуку хоста. Далі проводиться розрахунок порогу слуху в цілочисельній області. Потім, застосовуючи зворотне цілочисельне вейвлет-перетворення до змінених коефіцієнтів, обчислюється новий звуковий (стего) сигнал [7, 9].

Цей метод характеризується великим корисним навантаженням, високою якістю аудіо (більші значення SNR) і повним відновленням вбудованого прихованого сигналу. Проблема простої стеганографії домену вейвлетів полягає в тому, що результуючі коефіцієнти не є цілими числами. При застосуванні цих вейвлетів до цілочисельного сигналу, такого як мова. Відбувається накопичення помилок в операціях округлення, відкидання дробових частин та перекодування у двійкову послідовність. Це в результаті призводить до деяких помилок. Щоб вирішити цю проблему для отримання вейвлетів Int2Int використовується схема підйому. Схема підйому – це техніка, яка проектує вейвлет і виконує DWT. Int2Int позначає цей вейвлет коефіцієнти для цілого вхідного сигналу також є цілими і отже масштабування коефіцієнтів не потрібне. Помилки в процедурі вбудовування в цьому випадку є незначною.

4) Методи квантової стеганографії (QAS). Ці методи змінюють найменший значущий кубіт LSQb (least significant qubit – найменш значущий кубіт) головного квантового аудіосигналу, який кодується як аудіовміст FRQA (flexible representation of quantum audio – гнучке представлення квантового аудіо). Перший метод побудований на основі обміну між кубітами, що кодують квантове аудіоповідомлення, та LSQb інформації про амплітуду в хост-зразках квантового аудіо. У другому протоколі процедура вбудовування полягає в усвідомленні того, що вона імплантує інформацію з квантового звуку повідомлення глибоко в накладене обмеженням найбільш значущий кубіт зразків квантового аудіо (MSQb) [7].

Приклад розробки алгоритму маскування даних на основі LSB

Використання відеофайлів як носія для стеганографічного приховування є більш прийнятним порівняно з іншими методами через їх розмір і вимоги до пам'яті. Вбудовування стеганографічних даних у відео дуже схоже на зображення. Однак існує багато відмінностей між прихову-

ванням даних у зображеннях і відео. Однією з важливих відмінностей стегозахисту є розмір контейнеру. Інформація у криптографії перетворюється на нерозбірливий шифротекст. При перехопленні повідомлення можна відразу визначити чи було використано криптошифрування чи ні. Стеганографія приховує повідомлення, не змінюючи його початкового формату.

В аудіо стеганографії як і в стеганографії текстовій використовується недосконаліть людських органів чуттів. Однак слухова система людини є більш точною. Тому методи приховування даних мають бути більш досконалими ніж ті, що використовуються в оптичній області.

Найпоширеніші методи стеганографії використовують наступні підходи:

– метод безпечної обкладинки;

– метод найменшого значущого біту;

– палітрові методи [3].

Одним з типових алгоритмів стеганографічного приховування даних у мультимедійних контейнерах є метод LSB (Least Significant Bit), який використовується для приховування інформації у найменш значущих бітах (LSBs) пікселів чи аудіо-семплів. Нижче наведений опис типового алгоритму застосування методу LSB для стеганографії в зображеннях:

1) Вибір контейнера: Обирається зображення, яке виконуватиме роль контейнера для приховання секретної інформації. Зазвичай обираються зображення з високою роздільною здатністю та низькою стисненістю, щоб зберегти якість інформації після приховування.

2) Вибір і приховування даних: Секретна інформація кодується у бітах найменш значущих пікселів зображення. Найпоширеніший метод – заміна найменш значущих бітів кожного каналу кольору (червоного, зеленого та синього) зображення на біти секретного повідомлення. Це може бути виконано шляхом заміни LSB кожного пікселя зображення на відповідний біт секретного повідомлення.

3) Збереження ключа (опціонально): Якщо потрібна можливість витягнути секретне повідомлення з контейнера, може бути збережений ключ, який вказує на те, як саме було виконане приховування даних. Це може бути необхідно, якщо контейнер буде передано отримувачу, який має доступ до ключа для витягнення секретної інформації.

4) Валідація та тестування: Після приховування секретного повідомлення важливо перевірити, чи можна витягнути цю інформацію без втрати та спотворення. Зазвичай проводиться тестування на невеликій вибірці зображень, щоб переконатися у правильності алгоритму та забезпечити стійкість прихованого повідомлення до атак.

5) Видобуття секретного повідомлення: Якщо передбачається можливість видобуття секретного повідомлення з контейнера, призначений отримувач використовує ключ або алгоритм для вилучення інформації з LSB каналів зображення.

При вбудовуванні текстової інформації в будь-який аудіофайл спочатку звуковий сигнал перетворюється у біти. Потім повідомлення, яке потрібно вставити, перетворюється згідно з однією із вищезгаданих стратегій [3]. Застосовуючи алгоритм LSB, повідомлення вбудовується в 16-бітний або 8-бітовий звуковий зразок. Продуктивність оцінюється шляхом застосування алгоритму LSB у різних позиціях, тобто 1-LSB, 2-LSB тощо. На стороні приймача беруться перші п'ять байтів. Якщо ці байти збігаються з байтами наших контрольних символів, тоді визначається наступний регістр символів.

Алгоритм кодування може приймати наступного вигляду:

1. Вводиться вихідний текст.

2. Виконується перетворення вихідного тексту у 5-бітний код. При цьому проводиться перевірка надлишковості у двійковому коді алфавітів та цифр.

3. Зчитується аудіофайл як файл обкладинки.

4. Вибирається звуковий зразок і приховуємо перетворений 5-бітний код тексту в аудіофайл за допомогою алгоритму найменш значущого біту.

5. Проводиться крок 4 до тих пір, поки повідомлення не буде вбудовано в аудіо блоки.

Алгоритм декодування схожий на алгоритм кодування і складається із наступних етапів:

1. Зчитується стегоповідомлення/стегоблок.

2. Проводиться виокремлення блоків повідомлення. Для цього виявляються контрольні символи у зразках.

3. Зчитується/проводиться аналіз LSB.

Висновки

Розробка та застосування методів приховування даних у блоках аудіо повідомлень є доволі перспективним напрямком науково-практичних досліджень. Низький рівень вимог та проста реалізація методів на основі методу найменш значущого біту може знайти собі широке коло застосування у реальних системах передачі даних.

Методи приховування повідомлень мають на меті забезпечити безпеку передачі конфіденційної інформації, роблячи її недоступною для незаконного доступу та виявлення. Один із таких методів – стеганографія, який є досить неочевидним та майбутнім напрямком в цій області.

Використання в якості контейнера секретних повідомлень мультимедійних даних дозволяє гнучко комбінувати різноманітні методи стеганo-

графічного приховування секретних повідомлень. Найчастіше в якості контейнерів для цього використовуються зображення або текстові документи, але також можуть використовуватися аудіодані. Суть методу полягає у вбудовуванні конфіденційної інформації в видимий текст, не змінюючи самого тексту або файлу.

Принциповою перевагою стеганографії є те, що вона доповнює шифрування, роблячи дані менш очевидними для виявлення. Цей метод дозволяє підвищити рівень безпеки передачі інформації, забезпечуючи додатковий рівень захисту.

Згадані вище аспекти стеганографії – місткість, безпека та надійність – визначають її ефективність. Місткість вказує на здатність методу вміщати в себе достатню кількість секретної інформації без помітного збільшення розміру контейнера. Безпека означає здатність забезпечити високий рівень невидимості прихованих даних для сторонніх користувачів. Надійність полягає в забезпеченні стійкості до будь-яких змін або атак на приховану інформацію під час передачі.

Стеганографія, так само як і криптографія, призначена для захисту повідомлень та даних від несанкціонованого доступу, але вони використовують альтернативні методи забезпечення безпеки. Іншим важливим аспектом є відеостеганографія, яка використовується для приховування будь-яких файлів у текстових, аудіо- або відеофайлах.

ЛІТЕРАТУРА

[1] Бараннік В. В., Бабенко Ю. М., Бараннік В. В., Колесник В. О. Метод кодування значимих за впливом на семантичну цілісність відеосегментів для забезпечення доступності. *Наукоємні технології*. 2022. № 2 (54). С. 118–126. doi: 10.18372/2310-5461.54.16749.

[2] Odarchenko R., Gnatyuk V., Gnatyuk S., Abakumova A. Security key indicators assessment for modern cellular networks. *System Analysis & Intelligent Computing (SAIC)*: proceedings of the IEEE First International Conference, 2018. P 1–7. doi: 10.1109/SAIC.2018.8516889.

[3] Козловський В., Савченко А., Толстікова О., Клобукова Л. Критерії вибору спектрально-ефективних сигналів у бездротових інформаційних мережах. *Наукоємні технології*. 2022. № 4 (56). С. 286–273. doi: 10.18372/2310-5461.56.17125.

[4] Одарченко Р., Іванова М., Рябенко М., Аль-Мудхафар Акіл Абдулхусейн М. Метод аналізу взаємодії параметрів QOE та QOS на основі алгоритмів керування машинами. *Наукоємні технології*. 2022. № 4 (56). С. 305–316. doi: 10.18372/2310-5461.56.17130.

[5] Huang S.-Y., Lo A.-h., Juan J.S.-T. XOR-Based Meaningful (n, n) Visual Multi-Secrets Sharing Schemes. *Applied Sciences, MDPI*. 2022. Vol. 12, iss. 20. Id. 10368. P. 1–22. doi: 10.3390/app122010368.

[6] Zia U., McCartney M., Scotney B. et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*. 2022. Vol. 21. P. 917–935. doi: 10.1007/s10207-022-00588-5.

[7] Cao X., Huang Y., Wu H.-T., Cheung Y.-m. Content and Privacy Protection in JPEG Images by Reversible Visual Transformation. *Applied Sciences, MDPI*. 2020. Vol. 10, iss. 19. Id. 6776. P. 1–12. doi: 10.3390/app10196776.

[8] Latif A., Mehrnahad Z. A Novel Image Encryption Scheme Based on Reversible Cellular Automata. *Journal of Electronic & Information Systems*. 2019. Vol. 1, iss. 1. P. 18–25. doi: 10.30564/jeisr.v1i1.1078.

[9] Barannik V. Technology of Structural-Binomial Coding to Increase the Efficiency of the Functioning of Computer Systems, *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine. 2022. P. 96–100, doi: 10.1109/ ATIT58178. 2022.10024205.

[10] Бараннік В. В., Ігнатьєв А. А., Бабенко Ю. М., Бараннік В. В., Сидченко Е. С. Технологія компоновочного кодування мікросегментів для підвищення безпеки відеоресурсів в інфокомунікаційних системах. *Безпека інформації*. 2020. № 3. С. 181–190.

[11] Belikova T. and Sidchenko S. The Method Drawing up the Text with the Set Suggestive Orientation to Create a Hidden Channel, *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT),* Kyiv, Ukraine. 2022. P. 106–110. doi: 10.1109/ATIT58178.2022.10024206.

[12] Babenko Y., Barannik V., Barannik V., Khimenko A., Kulitsa O., Matviichuk-Yudina O. Significant Microsegment Transformants Encoding Method to Increase the Availability of Video Information Resource. *IEEE Advanced Trends in Information Theory (ATIT):* proceedings of 2nd Intern. Conf. (Kyiv, Ukraine, November 25–27, 2020). Kyiv, 2020. P. 52–56. doi: 10.1109/ATIT50783.2020.9349256.

[13] Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*. 2011. Vol. 91, Iss. 1. P. 90–97. doi: 10.1016/j.sigpro.2010.06.012.

[14] Onyshchenko R., Krasnorutsky A., Barannik D. and Barannik V. The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity. *2022 IEEE 4th International Conference on Advanced Trends in Information*

Theory (ATIT), Kyiv, Ukraine, 2022. P. 53–56, doi: 10.1109/ATIT58178.2022.10024208.

[15] Kolesnyk V., Berchanov A., Krasnorutsky A., Barannik V., Kharchenko N. and Malko O. Method of Structural-Statistical Coding of Video Segments in Spectral-Cluster Space, 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine. 2022. P. 32–37, doi: 10.1109/ATIT58178.2022. 10024240.

[16] Barannik V., Tarasenko D. Method coding efficiency segments for information technology processing video. Problems of Infocommunications. Science and Technology (PIC S&T): proceedings of 4th International Scientific-Practical Conference. (Kharkov, Ukraine, October 10–13, 2017), Kharkov, 2017. P. 551–555. doi: 10.1109/INFOCOMMST.2017.8246460.

[17] Hsu W.-L., Tsai Ch.-L., Chen Ch.-J., Multi-morphological image data hiding based on the application of Rubik's cubic algorithm. Carnahan Conference on Security Technology (ICCST): proceedings of the IEEE International Conference. 2012. P. 135–139. doi: 10.1109/ CCST.2012.6393548.

[18] Onyshchenko R., Slobodyanyuk O., Krasnorutsky A., Bezruk V., Kolesnyk V. and Podlesny S. Approach to Coding with Improved Integrity of Video Information for Transmission in Wireless Infocommunication Networks, 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine. 2022. P. 38–42. doi: 10.1109/ATIT58178.2022. 10024245.

[19] Information technology – JPEG 2000 image coding system: Secure JPEG 2000. International Standard ISO/IEC 15444-8, ITU-T Recommendation T. 807, 2007. 108 p.

[20] Qi X. Minemura, K. Moayed, Z. Wong, K. Tanaka. JPEG image scrambling without expansion in bitstream size. Image Processing: proceedings of the 19 th IEEE International Conference, 2012. P. 261–264. doi:10.1109/ICIP.2012.6466845.

[21] Barannik V., Babenko Y., Barannik V., Kolesnyk V., Zhuikov D. Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process, 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine. 2022. P. 66-71, doi: 10.1109/ATIT58178.2022. 10024193.

[22] Barannik V., Khimenko V., Barannik N., Method of indirect information hiding in the process of video compression. Radioelectronic and Computer Systems. 2021. No 4. P. 119–131. doi: 10.32620/reks.2021.4.

[23] Barannik V., Sidchenko S., Barannik D. and Ignatyev O. The Concept Of Creating A Complex Cryptocompression Image Protection System In Infocommunications, 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine. 2022. P. 101–105, doi: 10.1109/ATIT58178.2022.10024210.

[24] Barannik V., Krasnorutsky A., Kolesnik V., Barannik V., Pchelnikov S., Zeleny P. Compression method in terms of ensuring the fidelity of video images in infocommunication networks. Radioelectronic and Computer Systems. 2022. no 4(100). P. 10–24. doi: 10.32620/reks.2022.5/09.

[25] Barannik, V. et al. A Method of Scrambling for the System of Cryptocompression of Codograms Service Components. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering. 2023. Vol 965. Springer, Switzerland, Cham. doi: 10.1007/978-3-031-24963-1 26.

[26] Barannik V., Karpenko S. Method of the 3-D image processing. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET): proceedings of Intern. Conf. (Lviv-Slavsko, Ukraine, February 19–23, 2008), Lviv-Slavsko, 2008. P. 378–380.

[27] Barannik, V. et al. (2023). Processing Marker Arrays of Clustered Transformants for Image Segments. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transfor-mation Age. TCSET 2022. Lecture Notes in Electrical Engineering, vol 965. Springer, Switzerland, Cham. doi: 10.1007/978-3-031-24963-1_25.

[28] Barannik V. and Shiryaev A. Quadrature compression of images in polyadic space, Proceedings of International Conference on *Modern Problem of Radio Engineering, Telecommunications and Computer Science*. 2012. P. 422–422. INSPEC Accession Number: 12713484

[29] Онищенко Р., Бараннік В., Шульгін С., Ушань В., Ігнатьєв О. Модель інформативного опису спектрального простору відеосегментів діагонально нерівномірною текстурою. *Наукоємні технології*. 2022. № 4 (56). С. 259–267. doi: 10.18372/2310-5461.56.17124.

[30] Barannik V., Hahanova I., Kulbakova N. Dynamic coding of transforms of the images in two - level polyadic space, 2008 International Conference on *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (TCSET). 2008. P. 320–325.

Слободянюк О. В., Костромицький А. І., Чебаненко В. Б., Дігтярь М. М., Онипченко П. М.

LSB МЕТОДИ ПРИХОВАНОЇ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ (ОГЛЯД)

Методи приховування повідомлень спрямовані на забезпечення безпеки передачі конфіденційної інформації, роблячи її недоступною для несанкціонованого доступу та виявлення. Одним із таких методів є стеганографія, яка використовує мультимедійні дані для приховування секретних повідомлень. Зображення, текстові документи та аудіодані найчастіше слугують контейнерами для стеганографічного приховування інформації. Основною перевагою стеганографії є її здатність доповнювати шифрування, роблячи дані менш очевидними для виявлення. Це дозволяє приховувати існування самого факту передачі секретної інформації, додаючи додатковий рівень захисту. Стеганографія використовує мультимедійні дані, такі як зображення, текстові документи або аудіодані, для вбудовування секретних повідомлень. За допомогою спеціальних алгоритмів, стеганографічні методи дозволяють вбудовувати інформацію у медіафайли таким чином, що її неможливо виявити без відповідних ключів або методів декодування. Вона доповнює шифрування, підвищуючи рівень безпеки передачі інформації завдяки додатковому рівню захисту. Шифрування перетворює дані на нечитабельний формат, зрозумілий лише тому, хто має відповідний ключ для дешифрування. Стеганографія, в свою чергу, дозволяє приховати сам факт існування закодованих даних, роблячи їх непомітними для потенційного зловмисника. Це значно ускладнює завдання для тих, хто намагається перехопити або втрутитися у процес передачі інформації. Ефективність стеганографії визначається такими аспектами, як місткість, безпека та надійність прихованих даних. Місткість вказує на здатність методу вміщати достатню кількість секретної інформації без помітного збільшення розміру контейнера. Це особливо важливо, оскільки значне збільшення розміру файлу може викликати підозру і привернути увагу. Безпека означає здатність забезпечити високий рівень невидимості даних, щоб прихована інформація залишалася непомітною для сторонніх спостерігачів. Надійність стосується стійкості до змін або атак на приховану інформацію, включаючи спроби виявлення та видалення прихованих даних.

Ключові слова. стеганографія, стиснення відеоданих, інфокомунікаційні системи, методи приховування інформації, якість відеозображень.

Slobodianiuk O., Kostromytskyi A., Chebanenko V., Digtiar M., Onypchenko P.

LSB METHODS OF COVERT MESSAGES TRANSMITION IN COMMUNICATION SYSTEMS (REVIEW)

In the article are analyzed and classified methods of hiding messages in container data blocks and proposes a scheme for implementing the method of hiding information in an audio stream using the concept of the least significant bit method. Message hiding methods are aimed at ensuring the security of confidential information transmission by making it inaccessible to unauthorized access and detection. One such method is steganography, which uses multimedia data to hide secret messages. Images, text documents, and audio data are the most commonly used containers for steganographic hiding of information. The main advantage of steganography is its ability to complement encryption, making the data less obvious for detection. This makes it possible to hide the existence of the fact that secret information was transmitted, adding an additional layer of protection. Steganography uses multimedia data, such as images, text, or audio data, to embed secret messages. Using special algorithms, steganographic methods allow information to be embedded in media files in such a way that it cannot be detected without the appropriate keys or decoding methods. It complements encryption, increasing the security of information transmission by adding an additional layer of protection. Encryption converts data into an unreadable format that can be understood only by those who have the appropriate decryption key. Steganography, in turn, allows you to hide the very fact of the existence of encoded data, making it invisible to a potential attacker. This greatly complicates the task for those trying to intercept or interfere with the process of information transmission. The effectiveness of steganography is determined by such aspects as the capacity, security, and reliability of the hidden data. Capacity indicates the ability of the method to hold a sufficient amount of secret information without a noticeable increase in the size of the container. This is especially important because a significant increase in file size can raise suspicion and attract attention. Security refers to the ability to provide a high level of data invisibility so that the hidden information remains invisible to outside observers. Robustness refers to the resistance to changes or attacks on hidden information, including attempts to detect and remove hidden data. The application of steganography can be extremely broad and includes not only military or governmental activities, but also personal data protection, commercial and corporate security. Today, when the issues of data privacy and security are extremely acute, steganography is becoming increasingly relevant. In addition to traditional media such as images and audio, steganography can also be used in other areas such as network protocols and Internet communications. Hiding information in data packets or using steganographic methods in network protocols can provide an additional layer of security for the transmission of information on the Internet.

Keywords: steganography, video compression, infocommunication systems, information concealment techniques, video image quality.

Стаття надійшла до редакції 05.05.2024 р.
Прийнято до друку 12.06.2024 р.