CRYPTOLOGY

DOI 10.20535/2411-1031.2022.10.1.261079
УДК 621.391

ІВАН САМБОРСЬКИЙ,
АНАСТАСІЯ ТОЛСТОВА

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ СТЕГАНОГРАФІЇ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Наразі необхідно забезпечувати стійку, неперервну та приховану передачу інформації, тому доцільно розглядати приховування самого факту передачі повідомлення. Таким чином, суттєво зменшується ризик потрапляння інформації не за призначенням. Поряд з цим додатково повідомлення можуть бути зашифровані. Таким чином, стеганографія – наука, яка забезпечує обмін інформацією в такий спосіб, що приховується сам факт існування конфіденційного повідомлення. Вона доповнює криптографію (шифрування даних) ще одним рівнем безпеки, а не замінює її. На сьогоднішній день використання стеганографії передбачає низку методів захисту інформаційних ресурсів. Вона поділяється на лінгвістичну та технічну. В свою чергу лінгвістична стеганографія поділяється на: семаграми, відкриті коди та закриті шифри. Технічна стеганографія поділяється на stego-text, stego-audio, stego-video та stego-image. Для цього використовуються такі носії повідомлення як зображення, текст, аудіо або відео. Повідомлення-носій та повідомлення, яке потрібно приховати, розбивається на біти, і ці біти прихованої інформації розташовуються в потоці бітів повідомлення-носія. Інформація шифрується шляхом зміни різних властивостей. Технічна стеганографія використовує спеціальні методи захисту сигналів, які доцільно реалізувати у засобах цифрового зв'язку. Один із шляхів підвищення прихованості факту передачі цифрового повідомлення стеганографічними методами – застосування потокової електромагнітної стеганографії. Це відносно нове поняття передбачає передачу малопотужного цифрового сигналу одночасно з випромінюванням суттєво потужнішого легітимного джерела. Таким джерелом, наприклад може бути передавач цифрового радіомовлення. Алгоритм передачі приховуваного повідомлення складається з трьох основних етапів: 1) формування електромагнітного випромінювання, що містить приховане повідомлення, 2) адитивне лінійне додавання електромагнітного випромінювання, що містить приховане повідомлення і потокового електромагнітного контейнера у просторі, 3) демодуляція сумарного сигналу з наступним виділенням приховуваного повідомлення. Електромагнітна стеганографія як незалежне відгалуження в загальній теорії stego, зі створенням теорії багатокористувацького детектування має перспективи якісно нового розвитку. Підходи зазначеної теорії дозволяють маскувати приховане повідомлення не шляхом зменшення спектральної щільності потужності за рахунок використання широкосмугових сигналів, а завдяки забезпеченню можливості приховування огинної спектру випромінювача прихованого повідомлення під огинною енергетичного спектру випромінювання.

Ключові слова: електромагнітна стеганографія, stego, контейнер, телекомунікації.

Постановка проблеми. Використовувати прихований інформаційний обмін у телекомунікаційних системах наразі актуально. А саме, забезпечувати приховування змісту повідомлення за рахунок шифрування (криптографія) або приховування самого факту передачі інформаційного повідомлення (стеганографія). Необхідність забезпечувати стійку, неперервну, гнучку та приховану передачу інформації засобами зв'язку спонукає до того, що доцільніше розглядати приховування самого факту передачі відомостей. Такий підхід суттєво

зменшує ризики того, що інформація потрапить до зловмисника. А у випадку потрапляння так званого контейнера не за призначенням, зловмисник не зможе побачити в отриманих повідомленнях нічого цінного. Тому розглянемо концептуальні аспекти стеганографії.

Стеганографія – це приховування факту передачі повідомлень, шляхом вбудовування інформації у відкритих повідомленнях. Акцентуємо увагу на термінологічних аспектах стеганографії. Термін стеганографія походить від грецьких слів “stegein” означає “обкладинка”, а “grafein” означає “писати”. Отже, стеганографію можна вважати процедурою або технологією “закритого письма” [1].

В останні десятиліття приховування факту передачі інформації стало популярним і застосовується у ряді сфер. При цьому інформацію передбачається “вставляти” в текстові повідомлення, аудіо- та відеосигнали чи світлини. У результаті створюються stego-text, stego-audio, stego-video та stego-image повідомлення відповідно. Зараз для підвищення ступеня захисту конфіденційної інформації при передачі її телекомунікаційними засобами використовуються спільно стеганографічні та криптографічні підходи.

Таким чином, стеганографія є наукою, що забезпечує обмін інформацією в такий спосіб, що приховується сам факт передачі повідомлення. Вона доповнює криптографію (шифрування даних) ще одним рівнем безпеки, а не замінює її. Потрібно використовувати такі методи цієї науки, щоб виявити приховане повідомлення (ПП) було неможливо, але якщо це станеться, то інформація може бути ще й додатково зашифрована.

Аналіз останніх досліджень і публікацій. Проаналізовано джерела [2] - [10]. У [2] розглянуто техніку стеганографії зображень, використовуючи довільний вибір пікселів зображення, які застосовуються для вбудовування прихованого повідомлення всередину нього, а також за допомогою методу найменшого значущого біта (LSB) для вбудовування даних усередину зображення та за допомогою гібридних нечітких нейронних мереж з метою покращення якості зображення після процесу вбудовування.

У [3] запропоновано метод, який використовує алгоритм стиснення на основі “словника” (LZW) для мінімізації розміру прихованого повідомлення та за допомогою алгоритму емпіричної модової декомпозиції (EMD) та Knight tour (задача про хід коня) для вбудовування цього повідомлення всередину зображення.

У [4] представлено метод менш значущих кадрів (LSF). Вибір кадру, який має ПП, залежить від його переміщення з використанням особливостей оптичного потоку.

У [5] представлено метод заснований на переміщенні кадру, де ПП вставляється в вектори руху рухомих кадрів.

У [6] представлено техніку, яка використовує симетричний алгоритм блокового шифрування (AES-128) для кодування зображення. Після цього LSB був використаний для вбудовування закодованого зображення усередину відео.

У [7] представлено метод у відеостеганографії, з використанням криптографічного алгоритму з відкритим ключем (RSA) і випадкової послідовності “хорошої” якості для шифрування ПП. Після цього закодоване повідомлення стискається за допомогою кодування Хаффмана. Потім із залученням дискретного косинусного перетворення (2D DCT) вбудовується ПП, для підвищення захисту.

У [8] представлені порівняння двох різних технік. Перша використовує LSB без шифрування або стиснення, а в другій ПП спочатку шифрується. Біти ПП розміщуються в зображення обкладинки у просторовій області до того, як створюється стеганографічне зображення. Тоді як алгоритм 2D DCT використовується так, щоб біти корисного навантаження були приховані в частотні компоненти зображення обкладинки.

У [9] техніка представлена за допомогою процедури диференціювання і заміни. Зображення розділяється на блоки 3×3 без перекриття і для кожного пікселя кожного блоку застосовується LSB. Тоді як різниця значень застосовується до залишку в 6 біт.

У [10] розроблено два алгоритми. В першому 2 біти ПП розміщається в позиціях LSB обкладинки звуку на основі старшого біт байту (MSB), у другому також використовується 2 біти ПП, розміщається в LSB обкладинки звуку.

Усі ці методи використовуються для підвищення надійності та безпеки під час вибору пікселів для вбудовування ПП всередину, а також для збереження якості stego-text, stego-audio, stego-video та stego-image та створення їх схожими на обкладинку.

Метою статі є надання пропозиції щодо визначення місця та методів електромагнітної стеганографії в загальній теорії стеганографії.

Виклад основного матеріалу дослідження. На сьогодні стеганографія передбачає використання низки методів захисту інформаційних ресурсів. Застосовуються відомі і розробляються нові методи, що базуються на результатах різноманітних областей науки. Фундаментальна проблема в реалізації процесу приховування даних полягає у вбудові інформації, зберігаючи якість об'єкта прикриття (контейнера), що вимагає ефективних методів, які приховують корисне навантаження та забезпечують стійкість цих методів проти дій зловмисників.

Стеганографія поділяється на дві широкі категорії – технічна та лінгвістична. Розглянемо їх більш детально [10] - [22].

1. Лінгвістична стеганографія.

Цей тип стеганографії використовується, щоб приховати повідомлення в тексті, при цьому застосовують семаграми (визначники), які, в свою чергу, використовують символи, зображення та знаки, щоб приховати інформацію. Лінгвістична стеганографія поділяється на:

1.1 Семаграма.

- візуальна семаграма. Вона використовує фізичні об'єкти, які застосовуються для передачі інформації кожного дня. Наприклад: зміни (перестановка) у робочій зоні, позиціювання товарів на конкретному сайті, а також зміна зовнішнього вигляду сайту. Ці знаки важко розпізнати і вони мають перевагу звичайності;
- текстова семаграма. Використовується для приховування повідомлення шляхом зміни зовнішнього вигляду переданого тексту. Є можливість застосувати такі зміни як тип і розмір шрифту, змінити шляхом додаткового простору між словами, за допомогою різних замін у літери рукописного тексту (наприклад, великі літери, виділення та цікаве написання).

1.2 Відкриті коди.

Стеганографія відкритого коду приховує повідомлення в легітимному фрагменті тексту способами, неочевидними для спостерігача. Це означає, що відкритий код – це текст, який можна читати. Цей текст містить послідовності слів, речень, які можуть бути приховані у вертикальному або зворотному порядку. ПП може бути розміщене у будь-якому місці тексту. Цей тип стеганографії можна розділити на жаргонні коди, орфографічні помилки та фонетику [11]. Відкритий код використовує жаргон, який розуміє група людей, але не зрозумілий для інших читачів. Заздалегідь узгоджені значення або термінологія можуть приховати справжній зміст повідомлення. Бажано підбирати слова та значення таким чином, щоб повідомлення носія залишалося розбірливим і зрозумілим. Можливості використання жаргону обмежені лише запасом відомих слів та значень сторін, що спілкуються [12].

1.3 Закриті шифри.

Використовують спеціальну техніку, щоб приховати інформацію у відкритому повідомленні, наприклад, вставити повідомлення в слова оператора. Цей тип стеганографії поділяється на:

- нульові шифри. Вони використовують серію символів і слів, призначених для заплутування. Повідомлення виглядає як безглуздий набір слів, але його можна розшифрувати до змістовного повідомлення. Це стародавня форма зашифрованого зв'язку, в якій повідомлення оточується великою кількістю зайвих символів (відомих як нульові шифри). Відомо, що ця форма спілкування використовувалася німецькою армією під час Другої світової війни;
- решітка. У так званій решітці лист з вирізаними з нього вузькими прямокутниками різної ширини кладеться на чисту сторінку, а в місцях (прямокутниках) записується приховане повідомлення. Потім аркуш видаляється, а решта пробілів заповнюються оманливим текстом.

Коли одержувач накладає ту саму сітку на папір у тому самому положенні, приховане повідомлення виявляється. Прочитати повідомлення одержувачу можливо лише за умови, якщо в нього є ідентична сітка.

2. Технічна стеганографія.

Цей тип використовує спеціальні інструменти, пристрої чи наукові методи, щоб приховати повідомлення. У цьому типі можна використовувати невидимі чорнила, мікроточки, комп'ютерні методи, щоб забезпечити захист від несанкціонованого розповсюдження (витоку) повідомлень. Це передбачає створення "невидимого стеганографічного сховища". При цьому використовуються такі носії повідомлення, як зображення, текст, аудіо або відео. Повідомлення-носій та повідомлення, яке потрібно приховати, розбивається на біти, і ці біти прихованої інформації розташовуються в потоці бітів повідомлення-носія. Інформація шифрується шляхом зміни різних властивостей повідомлення-носія [13].

Оскільки носієм повідомлення може бути текст, відео, зображення та аудіо тому можна виділити принаймні чотири типи стеганографії:

2.1 Стеганографія тексту.

Для приховування інформації використовується кількість табуляцій, пробіли, великі літери, азбука Морзе [14].

У цьому підході повідомлення-носій (контейнер) використовує деяку випадкову кількість послідовностей символів, змінюючи слова в тексті або формат існуючого тексту, щоб приховати повідомлення. Стеганографія тексту вимагає менше пам'яті, оскільки вона може зберігати лише текстові файли. Але вона містить велику кількість зайвих даних [15].

2.2 Стеганографія відео.

Стеганографія відео застосовується при розподілі відео на аудіо та зображення або кадри. Це дозволяє ефективно приховати дані. Використання відеофайлів як носія для стеганографії є більш придатним у порівнянні з іншими методами. Відео – це набір кадрів, і кожен кадр – це зображення. Отже, якщо "витягнемо" всі кадри з відео, зможемо використовувати цей метод для збереження даних за допомогою LSB і "зшити" ці кадри назад у відео з ПП. Цей метод використовується також в комбінації з іншими методами.

2.3 Стеганографія зображення.

Цей тип стеганографії став дуже популярним, ніж інші через велику кількість електронних зображень, які є доступною інформацією. Ці зображення можна використовувати як повідомлення-носій. Є можливість включати приховування інформації в природній шум зображення (шум відноситься до недоліків, властивих процесу відтворення аналогового зображення). У стеганографії зображення можемо приховати повідомлення у пікселях зображення [16].

Оригінальні зображення, які несуть інформацію, називаються зображенням обкладинки в стеганографії, а вставлена в повідомлення прихована інформація у зображення обкладинки називається stego-зображенням. Різні методи стеганографії зображень виконуються з використанням просторової та частотної областей наступним чином:

- просторова область (домен). Безпосередньо вбудовує ПП в інтенсивність вихідних пікселів зображення. В основному LSB використовується для цієї області, коли повідомлення обкладинки або носія розкладається на бітові площини, а потім LSB бітової площини замінюються ПП. Цей метод заміни включає вбудовування з мінімальним зважуваним бітом, оскільки це не вплине на піксель вихідної інформації або на обкладинку повідомлення. Єдиним недоліком схеми LSB є те, що третя сторона може негайно витягти ПП;
- частотна область (домен). Частотний домен також відомий як домен трансформації, де зображення перетворюються, а потім вбудовується приховане повідомлення. У цьому домені ПП розташовано в певній області повідомлення, що унеможливлює атаку, наприклад стиснення, метод обрізання або стиснення зображення. У частотній області доступні різні формати. Техніка 2D DCT грає важливу роль у техніці стиснення JPEG. 2D DCT дозволяє

розбити зображення на три діапазони частот, а саме: низькочастотний діапазон, смуга високих частот та смуга середніх частот. У цьому підході ПП вбудовуються в блоки 2D DCT, що містять середню частоту компоненти піддіапазону, тоді як високочастотний компонент піддіапазону залишається невикористаним. Це покращує ємність і якість stego-зображень. Потім використовується дискретне вейвлет-перетворення (DWT) – це процес декомпозиції з роздільною здатністю в термінах розкладання зображення в набір базисної функції Вейвлета. За допомогою DWT зображення розкладається на чотири піддіапазони:

- піддіапазон LL – приблизне представлення вхідного зображення, це низькочастотний піддіапазон;
- піддіапазон LH витягує горизонтальні риси вихідного зображення;
- піддіапазон HL надає вертикальні характеристики;
- піддіапазон HH надає діагональні характеристики [17].

2.4 Аудіостеганографія.

Аудіостеганографія є однією з популярних методик приховування даних, яка вбудовує ПП в звукові сигнали. Цей тип стеганографії має такі основні застосування як захист аудіосигналів, захищених авторським правом, спілкування між абонентами, приховування даних [18]. Ефективна аудіостеганографія повинна мати наступні характеристики для успішного вбудовування та вилучення даних: перцептивна прозорість (тобто обкладинка та об’єкти stego повинні бути непомітними), висока швидкість передачі даних і надійність вбудованих даних [19].

На даний час поширені такі види аудіостеганографії, які використовують різні типи приховування інформації у файлах [20] - [22]:

- кодування найменшого значущого біта здійснюється шляхом заміни кожної точки вибірки, представленої в двійковій послідовності. Це дозволяє приховати значний обсяг інформації. Однак, головним недоліком методу є слабка стійкість до сторонніх впливів. Вбудована інформація може бути зруйнована через наявність шумів в каналі в результаті передискретизації вибірки [20];
- метод фазового кодування, що полягає в заміні фази вихідного звукового сегмента на опорну фазу, характер зміни якої відображає собою дані, які необхідно приховати. Для того щоб зберегти різницеву фазу між сегментами, фази останніх відповідним чином узгоджують. Істотна зміна співвідношення фаз між кожними частотними складовими призводить до значного розсіювання фази. Але поки модифікація фази в достатній мірі мала, може бути досягнуто приховування, невідчутне на слух. Модифікація може бути малою по відношенню до звичайного спостерігача, однак фахівці зі спектрального аналізу здатні виявити такі зміни;
- метод розширення спектру, що реалізується в наступному: сигнал даних множиться на сигнали несівної і псевдовипадкової шумової послідовності, що характеризується широким частотним спектром. У результаті цього спектр даних розширюється на всю доступну смугу. Надалі послідовність розширених даних послаблюється та додається до вихідного сигналу як адитивний випадковий шум. Це система, яка використовує реалізацію кодування LSB, випадковим чином розподіляє біти повідомлення по всьому звуковому файлу. Це дозволяє приймати сигнал, навіть якщо є завади на деяких частотах;
- приховування даних з використанням луна-сигналу полягає у введенні в звуковий файл додаткового луна-сигналу. Дані ховаються при зміні трьох параметрів луна-сигналу: початкової амплітуди, швидкості загасання і зсуву. Коли зсув (затримка) між первинним і луна-сигналом зменшується, починаючи з деякого значення затримки, слухова система людини (ССЛ) стає нездатною виявити різницю між двома сигналами, а луна-сигнал сприймається тільки як додатковий резонанс. Дане значення важко визначити точно, оскільки воно залежить від якості звукозапису, типу звуку та від слухача. У загальному випадку для більшості звуків і більшості слухачів змішування відбувається при затримці приблизно в одну мілісекунду. Окрім зменшення часу затримки для забезпечення непомітності також можна змінювати рівні початкової амплітуди та час згасання, які б не перевищували поріг чутливості

ССЛ. Для того щоб у первинний сигнал закодувати більше одного біта, сигнал розкладається на менші сегменти. Кожен сегмент при цьому розглядається як окремий сигнал і в нього може бути вбудований шляхом луна-відображення один біт інформації;

- приховування за допомогою вставки тонів ґрунтується на поганій чутності та нечіткості низьких тонів у присутності компонент значно вищого спектра. Метод вставки тону може протистояти таким атакам, як фільтрація низьких частот і скорочення бітів до низької потужності вбудовування. Вбудовані дані можуть бути зловмисно вилучені після вставки [21];
- потокова електромагнітна стеганографія (ПЕМС). Один із шляхів підвищення прихованості факту передачі цифрового повідомлення стеганографічними методами – застосування так званого електромагнітного маскування. Це поняття передбачає передачу малопотужного цифрового сигналу одночасно з випромінюванням суттєво потужнішого легітимного джерела. Таким джерелом, наприклад, може бути передавач цифрового радіомовлення. Отже, це область застосування стеганографічних методів, коли ПП вбудовується у повідомлення прикриття без обмежень на його довжину безпосередньо в просторі. Вибір такого stego обумовлений тим, що людина сприймає лише видиме електромагнітне випромінювання світла, тому вибір цього методу в першу чергу буде визначатися можливостями апаратури аналізу електромагнітного спектру і відповідних демодуляторів, а вже потім – можливостями ССЛ.

Алгоритм передачі приховуваного повідомлення складається з трьох основних етапів: 1) формування електромагнітного випромінювання, що містить ПП (ЕПП), 2) адитивне лінійне додавання ЕПП і потоковий електромагнітний контейнер (ПЕК) у просторі, 3) демодуляція сумарного сигналу з наступним виділенням ПП [22]. Розглянемо кожен з виокремлених етапів.

1. Процес формування ЕПП включає процедури криптографічного шифрування (за необхідності), надлишкового завадостійкого кодування, стеганографічного кодування (що визначає закон вбудовування ПП в ЕПП) і переносу результату в смугу частот випромінювання повідомлення прикриття (на його частоту).

З метою досягнення максимально можливої енергетичної прихованості ЕПП огинні енергетичних спектрів ЕПП і ПЕК повинні за формою співпадати. А саме, всі неінформаційні параметри ПЕК (частота, форма огинної несівного коливання, закон і швидкість маніпуляції). Тобто, між неінформаційними параметрами ЕПП і ПЕК повинен дотримуватися жорсткий взаємозв'язок, аж до тотожності частини з них (наприклад, несівних частот і швидкостей маніпуляції).

2. Процес вбудовування ЕПП в ПЕК є складанням у просторі та визначається параметрами відповідних передавачів, антен і властивостями середовища розповсюдження. Складання у просторі можна описати таким чином:

$$I_w(x,y,z) = \varphi(x_0,y_0,z_0,x,y,z) \circ I + \psi(x_П,y_П,z_П) \circ W,$$

де $\varphi(x_0,y_0,z_0,x,y,z) \circ ()$ – оператор випромінювання ПЕК, породжуваного в точці (x,y,z) передавачем прикриття, розташованим в точці (x_0,y_0,z_0);

$\psi(x_П,y_П,z_П) \circ ()$ – оператор випромінювання ЕПП від передавача, який знаходиться в точці $(x_П,y_П,z_П)$.

3. Процес обробки заповненого ПЕК $I_w(x,y,z)$ в точці (x,y,z); визначається процедурами обробки в приймальному пристрої, включаючи демодуляцію-розділення сигналів одночасно випромінюваних передавачами повідомлення покриття і ПП, а також декодування, що виправляє помилки і дешифрування.

На особливу увагу заслуговує задача кодування, яка є специфічною для застосування щодо електромагнітної стеганографії. Процедура кодування тут може виконувати як найменш дві задачі – власно виправлення помилок, і приховування ЕПП під ПЕК шляхом розширення спектру. Наприклад, можна представити байти (напівбайти) ПП квазіортогональми послідовностями Голда, Касамі, Камалетдінова або бент-функціями.

Зсув тактових точок (моментів можливої зміни дискретних параметрів (ДП) ЕПП) відносно тактових точок ДП ПЕК з метою їх співпадання в точці прийому може виконуватися на основі використання координат розміщення джерел випромінювання ПЕК (x_0, y_0, z_0), джерела ЕПП $(x_П, y_П, z_П)$ і точки прийому (x, y, z) їх адитивної суміші в радіоканалі.

Розглянемо приклад, коли в спостереженні присутні 2 двійкових сигнала відносно фазової модуляції (таким джерелом, наприклад може бути передавач цифрового радіомовлення), що відрізняються за потужністю на 6дБ або більше. В такому випадку потужніший сигнал слід демодулювати класично (когерентно або автокореляційно) без урахування малопотужного, а останній – некогерентно, квадратурно, із залученням процедури компенсації впливу потужнішого на синфазну складову. Модель спостереження може бути надана в вигляді:

$$y(t) = (-1)^{r_1^{k-1}} s_1\left[t \in \left[t_{k-2}, t_{k-1}\right)\right] + (-1)^{r_1^{k}} s_1\left[t \in \left[t_{k-1}, t_{k}\right)\right] + (-1)^{r_2^{k-2}} s_2\left[t \in \left[t_{k-3}+\tau, t_{k-2}+\tau\right)\right] +$$
$$+(-1)^{r_2^{k-1}} s_2\left[t \in \left[t_{k-2}+\tau, t_{k-1}+\tau\right)\right] + (-1)^{r_2^{k}} s_2\left[t \in \left[t_{k-1}+\tau, t_{k}+\tau\right)\right] + n(t),$$

де $r_{1,2}^{r-2,r-1} \in \{0,1\}$ – дискретні параметри сигналів на $k-2, k-1, k-x$ тактових інтервалах;

τ – зсув між тактовими точками сигналів;

$n(t)$ – адитивний білий гаусівський шум.

Вважаємо, що потужнішим є другий сигнал $S_2(t)$ Тоді правило прийняття рішень (ППР):

$$r_1^* = rect\{-[-b_{1s}^{k-1} + Arth(thb_2^{k-2} th2R_1^{k-1}) + Arth\left(thb_2^{k-1} th2R_2^{k-1}\right)] \times$$
$$\times [-b_{1s}^{k} + Arth\left(thb_2^{k-1} th2R_1^{k}\right) + Arth\left(thb_2^{k} th2R_2^{k}\right)] - b_{1q}^{k-1} b_{1q}^{k}\}$$
$$rect(x \ge 0) = 1;\ rect(x < 0) = 0;\ r_1^* \in \{0,1\} \qquad (1)$$

При $h_2^2 >> h_1^2$ (1) можна суттєво спростити:

$$r_1^* = rect\left\{-\left[-b_{1s}^{k-1} + 2R_1^{k-1} signb_2^{k-2} + 2R_2^{k-1} signb_2^{k-1}\right] * \left[-b_{1s}^{k} + 2R_1^{k} signb_2^{k-1} + 2R_2^{k} signb_2^{k}\right] - b_{1q}^{k-1} b_{1q}^{k}\right\} \quad (2)$$

У (1), (2) застосовані значення:

$$b_{1s}^{k-1} = \frac{2}{N_0} \int_{t_{k-2}}^{t_{k-1}} y_t A_{1s} \cos(\omega t + \varphi_2) dt;$$

$$b_{1s}^{k} = \frac{2}{N_0} \int_{t_{k-1}}^{t_{k}} y_t A_{1s} \cos(\omega t + \varphi_2) dt;$$

$$b_{2}^{k-2} = \frac{2}{N_0} \int_{t_{k-3}+\tau}^{t_{k-2}+\tau} y_t A_{2} \cos(\omega t + \varphi_2) dt;$$

$$b_{2}^{k-1} = \frac{2}{N_0} \int_{t_{k-2}+\tau}^{t_{k-1}+\tau} y_t A_{2} \cos(\omega t + \varphi_2) dt;$$

$$b_{2}^{k} = \frac{2}{N_0} \int_{t_{k-1}+\tau}^{t_{k}+\tau} y_t A_{2} \cos(\omega t + \varphi_2) dt;$$

$$R_1^{k-1} = \frac{1}{N_0} \int_{t_{k-2}}^{t_{k-2}+\tau} A_2 A_{1s} \cos^2(\omega t + \varphi_2) dt;$$

$$R_2^{k-1} = \frac{1}{N_0} \int_{t_{k-2}+\tau}^{t_{k-1}} A_2 A_{1s} \cos^2(\omega t + \varphi_2) dt;$$

$$R_1^{k} = \frac{1}{N_0} \int_{t_{k-1}}^{t_{k-1}+\tau} A_2 A_{1s} \cos^2(\omega t + \varphi_2) dt;$$

$$R_2^{k} = \frac{1}{N_0} \int_{t_{k-1}+\tau}^{t_{k}} A_2 A_{1s} \cos^2(\omega t + \varphi_2) dt;$$

$$b_{1q}^{k-1} = \frac{2}{N_0} \int_{t_{k-2}}^{t_{k-1}} y_t A_{1q} \sin(\omega t + \varphi_2) dt;$$

$$b_{1q}^{k} = \frac{2}{N_0} \int_{t_{k-1}}^{t_k} y_t A_{1q} \sin(\omega t + \varphi_2) dt .$$

ППР (1), (2) отримані за припущення, що складові їх аргументів, які містять множники виду $thb_2^{k-2} thb_{1s}^{k-1} thb_2^{k-1}$, $thb_2^{k-1} thb_{1s}^{k} thb_2^{k}$ можна спростити як такі, що суттєво не впливають на ефективність розділення–демодуляції.

Із сучасної теорії багатокористувацького детектування за умов, коли два випромінювання суттєво відрізняються за потужністю, а вид модуляції, несівна частота у них співпадають, потенційна завадостійкість малопотужного сигналу виявляється такою ж як і в каналі без суттєвого потужнішого маскувального сигналу. Окрім того виявляється, що за умови співпадіння в точці прийому тактових точок сигналів, що взаємозаважають, та некогерентного прийому малопотужного, амплітуду та початкову фазу останнього оцінювати не треба. З другого боку, за суттєвого перевищення потужності легітимного джерела над малопотужним суттєво спрощуються задачі якісної оцінки його неінформаційних параметрів.

Висновки. Потокова електромагнітна стеганографія, як незалежне відгалуження в загальній теорії стеганографії, на методах теорії багатокористувацького детектування (БКД) має перспективи якісно нового розвитку. Підходи зазначеної теорії дозволяють маскувати ПП не традиційним шляхом зменшення спектральної щільності потужності за рахунок використання широкосмугових сигналів, а завдяки забезпеченню можливості приховування огинної спектру ПП під огинною потужного енергетичного спектру маскувального випромінювання.

Потокова електромагнітна стеганографія за своєю фізичною сутністю факторизована від інших можливостей стеганографії. Тому її можна застосовувати спільно (сумісно, одночасно) з будь якими іншими методами стеганографії.

Мета стеганографії – приховування самого факту передачі ПП, що спонукає на постановку та розв’язання задач в галузі БКД, коли миттєва потужність так званого “контейнера” суттєво перевищує миттєву потужність випромінювання ПП. Це може спростити поточні задачі оцінювання неінформаційних неперервних параметрів передавача – “контейнера”, що співпадають з параметрами джерела ПП.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] N. Johnson, and S. Jajodia, “Exploring steganography: seeing the unseen”, *IEEE Computer*, vol. 31, no. 2, pp. 26-34, February 1998, doi: https://doi.org/10.1109/MC.1998.4655281.

[2] A. Saleema, and T. Amarunnishad, “A new steganography algorithm using hybrid fuzzy neural networks”, in *Proc. International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST-2015)*, vol. 24, Trissur (India), 2016, pp. 1566-1574, doi: https://doi.org/10.1016/j.protcy.2016.05.139.

[3] S. A. Alhaj, A. M. Shaheen, and T. M. Al-Kharoubi, “Multi-layers Video Steganography: A Novel Technique for Image Hiding”, *Transactions on Networks and Communications* vol. 4, no. 6, pp. 43-52, 2016, doi: http://dx.doi.org/10.14738/tnc.46.2529.

[4] A. Solichin, and Painem, “Motion-based less significant frame for improving lsb-based video steganography”, in *Proc. IEEE International Seminar on Application for Technology of Information and Communication (ISemantic)*, Semarang, Indonesia, 2016, pp. 179-183, doi: http://dx.doi.org/10.1109/isemantic.2016.7873834.

[5] K. Rezagholipour, and M. Eshghi, “Video steganography algorithm based on motion vector of moving object”, in *Proc. IEEE 2016 Eighth International Conference on Information and Knowledge Technology (IKT)*, Hamedan, Iran, 2016, pp. 183-187, doi: http://dx.doi.org/10.1109/ikt.2016.7777764.

[6] A. Putu, and M. Gusti, “MP4 video steganography using least significant bit (LSB) substitution and advanced encryption standard (AES)”, *Journal of Theoretical and Applied Information Technology,* vol. 95, no. 21, pp. 5805-5813, November 2017.

[7] S. Mumthas, and A. Lijiya, "Transform domain video steganography using RSA, random DNA encryption and Huffman Encoding", in *Proc. 7th International Conference on Advances in Computing and Communications*, vol. 115, pp. 660-666, 2017, doi: http://dx.doi.org/10.1016/j.procs.2017.09.152.

[8] O. F. Abdel Wahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, A. A. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms", *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol 17, no. 3, pp. 1168-1175, 2019, doi: http://dx.doi.org/10.12928/telkomnika.v17i3.12230.

[9] G. Swain, "Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution", *Arabian Journal for Science and Engineering,* vol. 44, no. 4, pp. 2995-3004, 2018, doi: http://dx.doi.org/10.1007/s13369-018-3372-2.

[10] S. P. Rajput, K. P. Adhiya, and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio", in *Proc. 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, 2017, pp. 122-137, doi: http://dx.doi.org/ 10.1109/iccubea.2017.8463948.

[11] F. Y. Shih, *Image Processing and Pattern Recognition: fundamentals and Techniques*. Hoboken, New Jersey, USA: John Wiley & Sons, 2010.

[12] M. Zelkowitz, *Security on the Web*. Cambridge, Massachusetts, USA: Academic Press, 2011.

[13] S. Bhattacharyya, and G. Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM)", *International Journal of Computer network & Information Security*, vol. 4, no. 7, pp. 27-40, 2012, doi: http://dx.doi.org/10.5815/ijcnis.2012.07.04.

[14] N. Johnson, and S. Jajodia, "Exploring steganography: seeing the unseen", *Computer,* vol. 31, no. 2, pp. 26-34, 1998, doi: http://dx.doi.org/10.1109/mc.1998.4655281.

[15] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, and Ki-H. Jung, "A Survey of Image Steganography Technique", *Signal Processing: Image Communication,* vol. 65, pp. 46-66, 2018, doi: http://dx.doi.org/10.1016/j.image.2018.03.012.

[16] S. V. Sharma, M. Raj, and S. Swathi, "A Survey of Text Steganography Methods", *International Journal of Scientific Research in Science and Technology,* 2021, pp. 238-241, doi: https://doi.org/10.32628/IJSRST.

[17] A. Nag, S. Biswas, and P. P. Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", *International Journal of Computer Science and Information Technology*, vol. 2, no. 3, pp. 103-112, 2010, doi: http://dx.doi.org/10.5121/ijcsit.2010.2308.

[18] D. Bhattacharyya, T. Kim, and P. Dutta, "A method of data hiding in audio signal", *Journal of the Chinese Institute of Engineers,* vol. 35, no. 5, pp. 523-528, 2012, doi: http://dx.doi.org/10.1080/02533839.2012.679054.

[19] H. B. Kekre, A. Athawale, and S. Rao, "Athawale U. Information Hiding in Audio Signals", *International Journal of Computer Application,* vol. 7, no. 9, pp. 14-19, 2010, doi: http://dx.doi.org/10.5120/1278-1623.

[20] D. N. Hmood, K. A. Khudhiar, and M. S. Altaei, "A New Steganographic Method for Embedded Image In Audio File", *International Journal of Computer Science and Security*, vol. 6, no. 2, pp.135-141, 2015.

[21] H. B. Kekre, and A. Athawale, "Information Hiding In Audio Signal", *International Journal of Computer Application,* vol. 7, no. 9, pp. 14-19, 2010, doi: http://dx.doi.org/10.5120/1278-1623.

[22] В. Ф. Єрохін, та А. В. Толстова, "Алгоритм когерентно-некогерентного розділення гомохронних сигналів двійкової відносної фазової маніпуляції", *Матеріали науково-практичної конференції Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання*, Київ, 2021, с. 167-168.

Стаття надійшла до редакції 21.01.2022.

REFERENCE

[1] N. Johnson, and S. Jajodia, "Exploring steganography: seeing the unseen", *IEEE Computer*, vol. 31, no. 2, pp. 26-34, February 1998, doi: https://doi.org/10.1109/MC.1998.4655281.

[2] A. Saleema, and T. Amarunnishad, "A new steganography algorithm using hybrid fuzzy neural networks", in *Proc. International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST-2015)*, vol. 24, Trissur (India), 2016, pp. 1566-1574, doi: https://doi.org/10.1016/j.protcy.2016.05.139.

[3] S. A. Alhaj, A. M. Shaheen, and T. M. Al-Kharoubi, "Multi-layers Video Steganography: A Novel Technique for Image Hiding", *Transactions on Networks and Communications* vol. 4, no. 6, pp. 43-52, 2016, doi: http://dx.doi.org/10.14738/tnc.46.2529.

[4] A. Solichin, and Painem, "Motion-based less significant frame for improving lsb-based video steganography", in *Proc. IEEE International Seminar on Application for Technology of Information and Communication (ISemantic)*, Semarang, Indonesia, 2016, pp. 179-183, doi: http://dx.doi.org/10.1109/isemantic.2016.7873834.

[5] K. Rezagholipour, and M. Eshghi, "Video steganography algorithm based on motion vector of moving object", in *Proc. IEEE 2016 Eighth International Conference on Information and Knowledge Technology (IKT)*, Hamedan, Iran, 2016, pp. 183-187, doi: http://dx.doi.org/10.1109/ikt.2016.7777764.

[6] A. Putu, and M. Gusti, "MP4 video steganography using least significant bit (LSB) substitution and advanced encryption standard (AES)", *Journal of Theoretical and Applied Information Technology,* vol. 95, no. 21, pp. 5805-5813, November 2017.

[7] S. Mumthas, and A. Lijiya, "Transform domain video steganography using RSA, random DNA encryption and Huffman Encoding", in *Proc. 7th International Conference on Advances in Computing and Communications*, vol. 115, pp. 660-666, 2017, doi: http://dx.doi.org/10.1016/j.procs.2017.09.152.

[8] O. F. Abdel Wahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, A. A. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms", *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol 17, no. 3, pp. 1168-1175, 2019, doi: http://dx.doi.org/10.12928/telkomnika.v17i3.12230.

[9] G. Swain, "Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution", *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 2995-3004, 2018, doi: http://dx.doi.org/10.1007/s13369-018-3372-2.

[10] S. P. Rajput, K. P. Adhiya, and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio", in *Proc. 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, 2017, pp. 122-137, doi: http://dx.doi.org/10.1109/iccubea.2017.8463948.

[11] F. Y. Shih, *Image Processing and Pattern Recognition: fundamentals and Techniques*. Hoboken, New Jersey, USA: John Wiley & Sons, 2010.

[12] M. Zelkowitz, *Security on the Web*. Cambridge, Massachusetts, USA: Academic Press, 2011.

[13] S. Bhattacharyya, and G. Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM)", *International Journal of Computer network & Information Security*, vol. 4, no. 7, pp. 27-40, 2012, doi: http://dx.doi.org/10.5815/ijcnis.2012.07.04.

[14] N. Johnson, and S. Jajodia, "Exploring steganography: seeing the unseen", *Computer*, vol. 31, no. 2, pp. 26-34, 1998, doi: http://dx.doi.org/10.1109/mc.1998.4655281.

[15] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, and Ki-H. Jung, "A Survey of Image Steganography Technique", *Signal Processing: Image Communication*, vol. 65, pp. 46-66, 2018, doi: http://dx.doi.org/10.1016/j.image.2018.03.012.

[16] S. V. Sharma, M. Raj, and S. Swathi, "A Survey of Text Steganography Methods", *International Journal of Scientific Research in Science and Technology*, 2021, pp. 238-241, doi: https://doi.org/10.32628/IJSRST.

[17] A. Nag, S. Biswas, and P. P. Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", *International Journal of Computer Science and Information Technology*, vol. 2, no. 3, pp. 103-112, 2010, doi: http://dx.doi.org/10.5121/ijcsit.2010.2308.
[18] D. Bhattacharyya, T. Kim, and P. Dutta, "A method of data hiding in audio signal", *Journal of the Chinese Institute of Engineers,* vol. 35, no. 5, pp. 523-528, 2012, doi: http://dx.doi.org/10.1080/02533839.2012.679054.
[19] H. B. Kekre, A. Athawale, and S. Rao, "Athawale U. Information Hiding in Audio Signals", *International Journal of Computer Application,* vol. 7, no. 9, pp. 14-19, 2010, doi: http://dx.doi.org/10.5120/1278-1623.
[20] D. N. Hmood, K. A. Khudhiar, and M. S. Altaei, "A New Steganographic Method for Embedded Image In Audio File", *International Journal of Computer Science and Security*, vol. 6, no. 2, pp.135-141, 2015.
[21] H. B. Kekre, and A. Athawale, "Information Hiding In Audio Signal", *International Journal of Computer Application,* vol. 7, no. 9, pp. 14-19, 2010, doi: http://dx.doi.org/10.5120/1278-1623.
[22] V. F. Yerokhin, and A. V. Tolstova, "Algorithm for coherent-incoherent separation of homochronous signals of binary relative phase manipulation", in *Proc. of the scientific-practical conference Information and telecommunication systems and technologies and cybersecurity: new challenges, new tasks,* Kyiv, 2021, pp. 167-168.

IVAN SAMBORSKYI,
ANASTASIIA TOLSTOVA

CURRENT STATE AND PROSPECTS OF STEGANOGRAPHY DEVELOPMENT IN TELECOMMUNICATION SYSTEMS

At present, it is necessary to ensure stable, continuous and hidden transmission of information, so it is advisable to consider the hiding of the very fact of the transmission of the message. Thus, the risk of access to information with limited access is significantly reduced. Along with this, additional messages can be encrypted. Thus, steganography is a science that provides information exchange in such a way that the very fact of the existence of a confidential message is hidden. It complements cryptography (data encryption) with another level of security rather than replacing it. To date, the use of steganography involves a number of methods for protecting information resources. It is divided into linguistic and technical. In turn, linguistic steganography is divided into: semagrams, open codes and closed ciphers. Technical steganography is divided into stego-text, stego-audio, stego-video and stego-image. For this purpose, such message carriers as images, text, audio or video are used. The media message and message (information) that needs to be hidden is broken down into bits, and these bits of information are hidden in each bit (in bits) of the media message. The information is encrypted by changing the different properties of the message carrier. Technical steganography uses special methods of signal protection, which it is advisable to implement in promising departmental means of digital communication. One of the ways to increase the hidden fact of the transmission of digital message by steganographic methods is the use of streamlined electromagnetic steganography. This concept involves the transmission of a low-power digital signal simultaneously with the radiation of a significantly more powerful legitimate source. Such a source, for example, can be a digital broadcasting transmitter. The hiding message transmission algorithm consists of three main stages: 1) the formation of electromagnetic radiation containing a hidden message 2) the additive linear addition of electromagnetic radiation containing a hidden message and stream electromagnetic container in space, 3) the demodulation of the total signal, followed by the release of the hidden message. Electromagnetic steganography, as an independent branch in the general theory of stego, with the creation of the theory of multiplayer detection has the prospects of qualitatively new development. The approaches of this theory allow to mask the hidden message not by reducing the

spectral power density due to the use of broadband signals, but by ensuring the possibility of concealment of the ocular spectrum of the hidden message emitter under the ambient energy spectrum of radiation.

Keywords: electromagnetic steganography, stego, container, telecommunications.

Самборський Іван Іванович, кандидат технічних наук, старший науковий співробітник, доцент кафедри спеціальних телекомунікаційних систем, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-5579-8740, i.i.samborskyi@gmail.com.

Толстова Анастасія Вадимівна, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-6411-9498, tolstova369@gmail.com.

Samborskyi Ivan, candidate of engineering sciences, senior researcher, associate professor of special telecommunication systems academic department, Institute of special communication and information security of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Tolstova Anastasiia, postgraduate student, Institute of special communication and information security of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.