DOI: 10.32347/2412-9933.2021.46.48-54
УДК 004.021

Катаєва Євгенія Юріївна
Кандидат технічних наук, доцент, доцент кафедри програмного забезпечення автоматизованих систем, *orcid.org/0000-0003-1277-8031*
Черкаський державний технологічний університет, Черкаси
Ребріков Антон Георгійович
Аспірант кафедри програмного забезпечення автоматизованих систем, *orcid.org/ 0000-0002-4482-2415*
Черкаський державний технологічний університет, Черкаси

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ У ВІДЕОФАЙЛАХ

Анотація. *Проведено вивчення задач захисту інформації від небажаного доступу. В часи широкого застосування електронних засобів зв'язку, електронного підслуховування та шахрайства, розмаїття комп'ютерних вірусів та інших електронних небезпек, електронні системи висувають високі вимоги до захисту інформації. Отже, дослідження методів цифрової стеганографії є актуальною задачею. У ході дослідження розглянуто основні методи негласної передачі даних за допомогою комп'ютерної стеганографії, а саме: метод використання системно зарезервованих областей форматів цифрових даних, методи приховування інформації за допомогою спеціального форматування текстових файлів, які включають використання слова, речення або зсув абзацу, виділення певних позицій букв у тексті або використання властивостей системних полів, які не відображаються на екрані, метод використання функцій імітації, методи використання невикористаних дискових секторів, метод використання надлишкових медіа-файлів (аудіо, фото та відео). Нині, завдяки зростанню інформації та збільшенню пропускної здатності каналів зв'язку, проблема приховування інформації у відеопослідовностях стає все більш актуальною. Передача цифрового відео в останні роки є типовою подією і не викликає підозр. У процесі дослідження розглянуто особливості приховування інформації у відеофайлах, проведено порівняння наявних алгоритмів комп'ютерної відеостеганографії. Завданням є розроблення власного алгоритму вбудовування інформації до синього кольорового каналу відеофайлів, який володіє достатнім ступенем функціональності та захисту до різних перетворень і протистоїть засобам статистичного і візуального стегоаналізу.*

Ключові слова: стеганографія; захист інформації; медіафайли; канали зв`язку; синій колір

Вступ

Задачу захисту інформації від небажаного доступу намагались вирішити протягом всього часу існування людства. В часи широкого застосування електронних засобів зв'язку, електронного підслуховування та шахрайства, розмаїття комп'ютерних вірусів та інших електронних небезпек, електронні системи висувають високі вимоги до захисту інформації. Отже, дослідження методів захисту інформації є актуальною задачею.

Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на базі комп'ютерної техніки і програмного забезпечення в рамках окремих обчислювальних систем, корпоративних чи глобальних мереж, складають предмет вивчення цифрової стеганографії. Одним із видів стеганографії є стеганофонічні системи – це системи, в яких приховується факт передачі таємного повідомлення, а саме: повідомлення інкапсулюється у стек мережевих протоколів та передається у реальному масштабі часу. Вперше принципи та визначення комп'ютерної стеганофонії були сформовані польськими спеціалістами з Варшавського університету технологій у 2008 р., які запропонували декілька методів приховування даних у трафіку IP-телефонії.

Структура і принципи роботи систем комп'ютерної стеганофонії аналогічні до стеганографічних систем, тому часто ці галузі захисту даних порівнюють між собою. Актуальність досліджень у галузі комп'ютерної стеганофонії витікає з обмежень на використання криптографічних засобів та з необхідності розв'язування задач захисту прав власності на інформацію, яка представлена у цифровому вигляді. На сьогодні як інструменти для розвитку цієї галузі широко використовуються методи теорії ймовірностей та математичної статистики, теорії

11 швидких ортогональних перетворень, теорії апроксимації, теорії кодування, теорії складності, теорії похибок, цифрової обробки сигналів та зображень тощо [5].

Мета статті

Мета роботи дослідження існуючих методів прихованої передачі інформації, огляд особливостей стеганографії у відео та дослідження характеристик людського зорового апарату.

Аналіз останніх досліджень

Розглянемо деякі дослідження у сфері приховування інформації, які були викладені в літературних джерелах.

У статті С. А. Сейеди і Р. Х. Садихова «Порівняння методів стеганографії в зображеннях» були розглянуті деякі з основних методів стеганографії зображень. Всі основні формати графічних файлів мають різні методи приховування повідомлень зі своїми сильними і слабкими сторонами. Вибір методу з великою надійністю протистоїть методу з високою швидкістю опрацювання. Наприклад, патч-підхід має дуже високу стійкість по відношенню до більшості видів атак, але він може приховати лише дуже невелику кількість інформації. Тому, більш розумно приховувати інформацію в додаткових перетвореннях, а не у вихідних файлах. Перетворення дискретними вейвлетами більш надійно, тому що дає змогу приховати повідомлення в області частот. Ця область менш помітна для людського зору. Автори пропонують використовувати нові методи стеганографії, а саме алгоритми вставки прихованого повідомлення в зображення з використанням ДВП. Ці методи можуть враховувати багатосторонні вимоги користувача, що висуваються до якості зображення з прихованим повідомленням великого обсягу [2].

Одне з найперших видань у сфері стеганографії є «Комп'ютерна стеганографія. Теорія і практика» Г. Ф. Конаховича і О.Ю. Пузиренко [6]. У ній викладені теоретичні і практичні основи комп'ютерної стеганографії. Представлено особливості використання сучасної системи символьної математики MathCAD v.12 з метою стеганографічного захисту інформації. Розглянуто приклади практичної реалізації приховання даних у нерухомих зображеннях, аудіосигналах і текстах.

У книзі А. І. Полежаєва «Стеганографія, цифрові водяні знаки» подано загальні представлення про наявні засоби, алгоритми і математичні моделі комп'ютерної стеганографії. Описано моделі прихованого зберігання і передачі інформації в інформаційно-обчислювальних мережах, архітектури програмних комплексів стеганографічного перетворення інформації. Наведено аналіз практичних аспектів реалізації програмних комплексів прихованої передачі даних і методів стеганографічного перетворення.

У книзі В. Г. Грибуніна «Цифрова стеганографія» перелічені деякі завдання, які можна вирішити із застосуванням методів цифрової стеганографії. Наголошено на необхідності розроблення математичних моделей мультимедійних контейнерів: мови, зображення, відео, а також на важливості подальшого розвитку методів теорії розпізнавання образів. Особливо в зв'язку з появою таких нових математичних інструментів, як нейронні мережі, генетичні алгоритми, нечітка логіка. Автор звертає увагу на необхідність введення в розгляд інших критеріїв перевірки статистичних гіпотез у стегоаналізі. Для тестування якості послідовностей, що генеруються псевдовипадковим генератором випадкових чисел, на сьогодні відомі десятки різних критеріїв. Можливо, багато з них знайдуть застосування в стеганографії [1].

У статті О. Ю. Сторожука «Аналіз методів приховування інформації в контейнерах типу JPEG-файли» розглянуто стеганографічні методи приховування інформації в частотній області JPEG контейнера, оскільки дані в просторовій області зображення є нестійкими до більшості відомих видів спотворень. Наприклад, виконання операції стиснення із втратами (наприклад JPEG-компресії) призводить до часткового або повного знищення розміщеної у контейнері інформації. Також проведено аналіз основних алгоритмів прихованої передачі даних, таких як алгоритми Коча, Кокса і Барні за такими критеріями: достовірність відновлення, стійкість до фільтрації, до геометричних перетворень, до стиснення, та стійкість до методів статичного аналізу. Виявлено, що алгоритм Кокса стійкий до стиснення і геометричних перетворень, алгоритм Коча – до однозначного відновлення, алгоритм Барні – до фільтрації, стиснення і методів статичного аналізу.

Книга Basar and G. J. Olsder «Dynamic Noncooperative Game Theory» містить огляд аналізу динамічних та диференційних ігор із нульовою сумою і з ненульовою сумою. Підкреслює роль різних форм інформації в теорії ігор та теорії імовірності. Також містить огляд рандомізованих стратегій, кінцевих ігор з інтегрованими рішеннями і уточнення рівноваги Неша. Висвітлені теми включають статичні і динамічні некооперативні ігри, з акцентом на взаємозв'язку між динамічними інформаційними шаблонами і структурними властивостями декількох різних типів рівноваг, концепції рішення Неша і Штакельберга, мульти- та одноактні ігри та аналіз парадоксу Браєса.

У статті Навроцького Д. О. "Дослідження результатів стеганографічного приховування

повідомлень у файлах зображень, як засобу забезпечення захисту інформації " він демонструє синергію стеганографічного та криптографічного алгоритмів шифрування, що забезпечує надійну основу для безпеки. Він порівнює і досліджує системи приховування повідомлень у просторовій та частотній областях зображення. У статті розглядаються такі питання:

– процес стиснення JPEG;

– структура перетворень JPEG;

– практичні рекомендації щодо вбудовування даних у файли зображень;

– метод найменш значущих розрядів (просторова площа);

– метод відносного заміщення коефіцієнтів DCT (діапазон частот);

– запакування та розпакування прихованого повідомлення;

– зображення візуальних спотворень при зміні параметрів системи.

У статті N. Provos «Defending Against on Statistical Steganalysis» представлено вдосконалені способи приховування інформації. Розглянуто методи, які використовують імовірнісні вкладення, щоб звести до мінімуму зміни в статистиці контейнера. Представлені виправлення в програмних кодах деяких алгоритмів, які дають змогу організувати процес вбудовування даних із вибірковим модифікуванням бітів стегоконтейнера, що знижує ймовірність виявлення факту наявності секретних даних. Крім того, розглядаються методи приховування кількох наборів секретних даних в єдиному файлі, що їх містить [5].

Аналіз предметної області

Відомо два основні напрями вирішення завдання прихованої передачі даних: криптографія та стеганографія. Метою криптографії є обмеження доступу до інформації шляхом її шифрування. На відміну від криптографії, стеганографія допомагає приховати сам факт наявності прихованих даних. Бурхливий розвиток інформаційних технологій в останні роки дав суттєвий поштовх для появи і покращення методів комп'ютерної стеганографії. З'явились нові варіанти застосування – приховані повідомлення вбудовують у графічні, аудіо- та відеоматеріали, текстові файли і навіть у файли програм [1].

Комп'ютерна стеганографія базується на двох принципах:

– файли, що містять зображення чи звукові матеріали можуть бути, до певної міри, змінені без втрати функціональності;

– органи чуття людини не здатні відрізнити незначні зміни в кольорі або якості звуку.

Другий принцип можливо успішно використовувати з огляду на надлишковість деяких сучасних аудіо- та графічних форматів: наприклад, зміна найменш значущих бітів 24-бітного зображення, які відповідають за колір конкретного пікселя, не призводить до явних змін у зображенні.

Стеганографічна система складається із двох основних компонентів: вбудовування і вилучення повідомлення [2]. Типову структуру такої системи зображено на рис. 1.

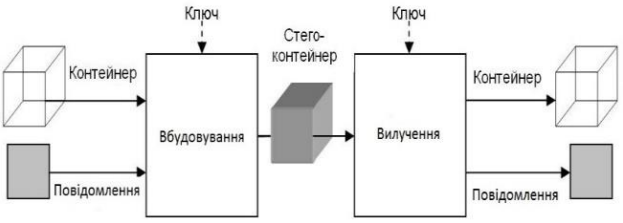

Рисунок 1 – Структура стеганографічної системи передачі даних

Описувана система складається із таких об'єктів:

– повідомлення – дані будь-якого типу;

– контейнер – будь-яка інформація, придатна для приховання в ній повідомлень;

– ключ – секретний ключ, що необхідний для шифрування та розшифрування повідомлень. Застосовується з метою посилення захисту.

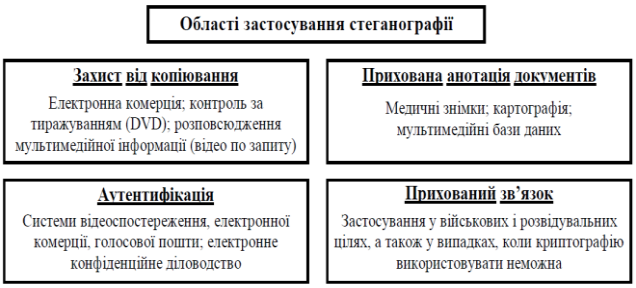

Рисунок 2 – Потенційні області застосування стеганографії

У процесі дослідження було розглянуто основні методи прихованої передачі даних із використанням комп'ютерної стеганографії (рис. 2), а саме:

1. Метод використання системно зарезервованих областей цифрових форматів даних. Зарезервовані поля, що існують в багатьох форматах файлів, часто заповнені нульовою інформацією та не використовуються. Перевагою методу є простота його застосування, а недоліком – низький об'єм даних, що передаються та низький ступінь захисту.

2. Методи приховування інформації шляхом спеціального форматування текстових файлів полягають у використанні зміщення слів, речень або абзаців, вибору певних позицій букв у тексті або

використання властивостей системних полів, що не зображуються на екрані. Недоліками цієї низки способів передачі даних є низька продуктивність, невеликий обсяг даних, що передаються та низький ступінь захищеності [3]. Іншим варіантом прихованої передачі даних, що базується на роботі з текстом, є метод використання імітуючих функцій. Суть методів полягає у модифікації повідомлення за принципом акровірша. Для передачі повідомлення створюють текст, що приховує саме повідомлення. Перевагою методу є те, що кінцевий текст не містить відступів і, як наслідок, не є підозрілим для систем моніторингу. Недоліком – порівняно низький обсяг даних, що передаються

3. Методи використання невикористовуваних секторів дисків. При застосуванні цього методу інформацію записують в ті сектори, що не задіяні при звичній роботі з оптичними або магнітними носіями, наприклад у нульовій доріжці. Перевагою методу є простота застосування, а недоліком – відносна легкість виявлення наявності прихованих даних.

4. Метод використання надлишковості медіа-файлів (аудіо, фото та відео). Суть методу полягає у використанні молодших розрядів (бітів), що містять дуже мало корисної інформації. Їх заповнення додатковими даними майже не впливає на якість сприйняття початкових медіа-матеріалів. Перевагами методу є можливість передачі великих об’ємів інформації, а також можливість захисту авторських прав, прихованої товарної марки тощо. Недолік цього методу – зміна статистичних характеристик цифрових потоків, що спрощує виявлення прихованих даних. Цей недолік може бути подоланий шляхом додаткового шифрування приховуваної інформації або застосування стеганографічних алгоритмів, що мінімізують зміну статистичних характеристик контейнера. Також серйозною проблемою є те, що контейнер із внесеною прихованою інформацією в процесі передачі може зазнати спотворень: додавання випадкового шуму, стиснення із втратами, а також навмисних спроб знищення прихованих даних. Необхідно передбачити стійкість стеганографічних алгоритмів до впливі такого роду.

Отже, найбільш збалансованим методом, що поєднує в собі і можливість передачі великих обсягів інформації, і відносну захищеність до виявлення, є метод використання надлишковості медіа-файлів.

Викладення основного матеріалу

Нині у зв'язку з ростом об'ємів інформації та збільшенням пропускної здатності каналів зв'язку все більшої актуальності має питання приховування інформації у відеопослідовностях. Передача цифрового відео в останні роки є типовою подією і не викликає підозр. Наприклад, сервіс YouTube нараховує сотні мільйонів відеофайлів, при чому один і той же відеоматеріал зустрічається в різних форматах. Велика кількість відеофайлів розміщується в P2P-мережах.

Розглянуто деякі особливості використання форматів відеофайлів для приховування інформації. Не дивлячись на те, що існує велика кількість відеоформатів, на практиці для приховування інформації використовуються формати MPEG-2 і MPEG-4.

Розглянемо три способи вбудовування інформації у файли формату MPEG-2: вбудовування на рівні коефіцієнтів, на рівні бітової площини і за рахунок енергетичної різниці між коефіцієнтами [1].

Метод вбудовування інформації на рівні коефіцієнтів. Біти приховуваної інформації вбудовуються в коефіцієнти дискретного косинусного перетворення (ДКП). Головною проблемою модифікації коефіцієнтів ДКП у стисненому потоці відео є накопичення зміщень та помилок. Спотворення, викликані зміною коефіцієнтів ДКП, можуть поширюватися в тимчасовій і в просторової областях. Тому для компенсації спотворень додають спеціальний сигнал. У силу обмеження бітової швидкості, при додаванні даних змінюються лише 10–20% коефіцієнтів ДКП. При використанні цього методу приховувана інформація зберігається при фільтруванні, зашумленні адитивним шумом і дискретизації [3].

Метод вбудовування інформації на рівні бітової площини. Цей метод відрізняється високою пропускною здатністю і невеликою обчислювальною складністю. Але є й істотний недолік: інформація, вбудована таким чином, може бути легко видалена. При повторному накладенні послідовності біт якість відео погіршиться незначно, а прихована інформація буде знищена.

Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами. В основі цього методу лежить диференціальне вбудовування енергії (ДВЕ). Складність алгоритму ДВЕ вище складності методу вбудовування на рівні бітової площини і значно нижче складності методу, заснованого на кореляції з компенсацією помилок передбачення. Метод ДВЕ може бути застосованим не лише до відеоданих MPEG, але і до інших алгоритмів стиснення відео. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП, і це має свої переваги. По-перше, в стиснений потік відеоданих не треба нічого додавати, можна обійтися без повторного стиснення відновленого потоку відео. По-друге, видалення високочастотних коефіцієнтів буде зменшувати розмір стегообразу потоку стиснених відеоданих у

порівнянні з вихідним потоком. Алгоритм ДВЕ вносить у відео менше спотворень, ніж метод вбудовування інформації на рівні бітової площини. Для видалення прихованої інформації потрібне проведення більш складних обчислювальних операцій, ніж вбудовування нової довільної бітової послідовності.

Тепер перейдемо до розгляду такої сфери дослідження, як особливості людського зорового сприйняття.

Зір – відчуття (сенсорне відчуття), що дає змогу сприймати світло, колір та зовнішню структуру навколишнього світу у вигляді зображення або картини. У тварин і людини органами зору є очі; втім зорова картина є також продуктом обробки первинної зорової інформації мозком. В оці людини містяться дві категорії фоточутливих елементів – рецепторів: високочутливі палички (рецептори) – такі, що відповідають за сутінковий (нічний) зір, і менш чутливі колбочки (рецептори) – такі, що відповідають за кольоровий зір.

У сітківці ока людини є три види колбочок, максимум чутливості яких припадає на червону, зелену і синю ділянки видимого спектру, тобто відповідає трьом „основним“ кольорам. Криві їх спектральної чутливості частково перекриваються, що забезпечує розпізнавання тисяч кольорів і відтінків у спектральному діапазоні довжин світлових хвиль 400—700 нм. Дуже сильне світло подразнює всі три типи рецепторів, а тому сприймається як випромінювання сліпучо-білого кольору (рис. 3).

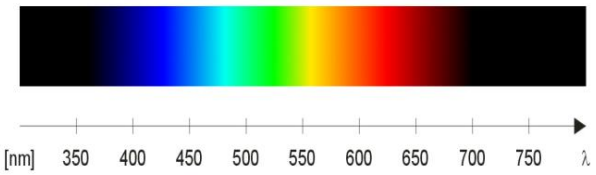

Рисунок 3 – Видимий спектр кольорів

Кольоровий зір працює через захоплення світла з різними довжинами хвиль і порівняння їх з метою визначення довжин хвиль, відбитих об'єктом (тобто його кольором). Синій колір сильніше стимулює рецептор, що сприймає короткі довжини хвиль, і слабше стимулює рецептор, що сприймає великі довжини хвиль, червоний колір справляє зворотний ефект. Порівнюючи відносну стимуляцію цих рецепторів, люди здатні розрізняти кольори.

Щоб найкращим чином сприймати світло різних довжин хвиль колбочки мають рівномірно розташовуватися по всьому прийнятному для людей спектру, від 400 до 700 нм. Якщо подивитись на розподіл колб у джмеля – він також володіє трихроматичним зором. Буде виявлено рівномірний розподіл. Сенсори цифрових камер теж мають бути правильно розташовані, щоб правильно сприймати кольорове зображення. Рівномірний розподіл колб/сенсорів забезпечує добре спектральне та хроматичне покриття для доступних довжин хвиль (рис. 4). Але людський зір працює не так (рис. 5).

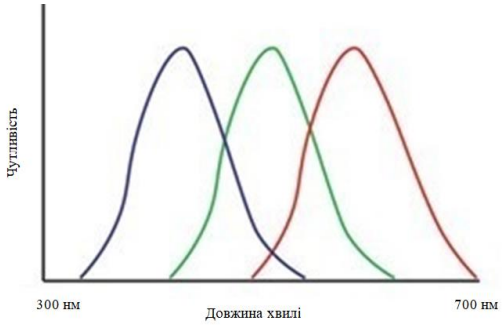

Рисунок 4 – Рівномірний розподіл колбачок

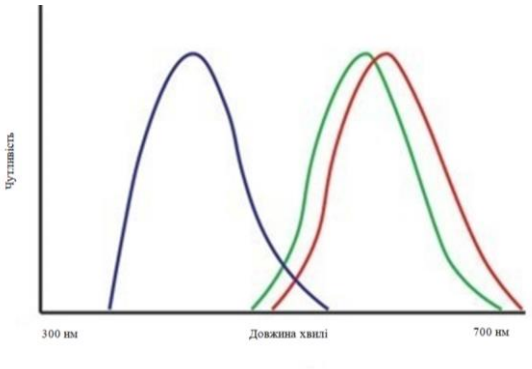

Рисунок 5 – Розподіл колбачок людського ока

Висновки

У людського зору немає рівномірного спектрального розподілу. У людей області дії червоних і зелених колб перетинаються. Це означає, що людський організм ставить пріоритет на розпізнавання декількох типів кольорів (конкретно, червоного і зеленого) за рахунок неможливості сприйняття більшої кількості кольорів [4]. Отже, відтінки синього кольору є найменш помітними для людського ока, тому вбудовування інформації саме в синій кольоровий канал є найбільш оптимальним рішенням.

У процесі дослідження було розглянуто особливості приховування інформації у відеофайлах, здійснено порівняння наявних алгоритмів комп’ютерної відеостеганографії, а також проаналізовано чутливість людського зору до відтінків різного кольору. Вирішено розробити власний алгоритм вбудовування інформації до синього кольорового каналу відеофайлів.

Список літератури

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. Москва : Солон-Пресс, 2009. 265 с.
2. Сейеди С., Садыхов Р. Сравнение методов стеганографии в изображениях. Компьютерные системы и сети: материалы 49-й научной конференции аспирантов, магистрантов и студентов (Минск, 6–10 мая 2013 г.). Минск, 2013. С. 66–75.
3. Вычислительные сети, теория и практика - Классификация и сравнение стеганографических методов. URL: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=9&pa=13&ar=1. (дата звернення: 08.01.2021).
4. Чувствительность к свету, чувствительность к цвету глаза. URL: http://www.simple-clerk.narod.ru/COLOR/d000.htm. (дата звернення: 05.01.2021).
5. Методи приховування інформації в графічних зображеннях. URL: https://ela.kpi.ua/bitstream/123456789/23826/4/ (дата звернення: 12.10.2020).
6. Конахович Г. Ф., Пузиренко А. Ю. Комп'ютерна стеганографія. Теорія та практика. Москва : МК-Пресс, 2006. 288 с.
7. Мельник С. В., Кондакова С. В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матер. наук.-практ. конф. Київ. С. 134–138.
8. Елтышева Е. Ю., Фионов А. Н. Построение стегосистемы на базе растровых изображений с учетом статистики младших бит. *Вестник СибГУТИ*. 2009. № 1. С. 67-84.
9. Жилкин М. Ю. Стегоанализ графических данных на основе методов сжатия. *Вестник СибГУТ*, 2008. № 2. С. 62–66.
10. Павлов К.А. Компьютерная безопасность. Криптографические методы защиты. Москва : ДМК Москва, 2010. 233 с.
11. Ростовцев А. Г., Михайлова Н. В. Методи криптоаналізу класичних шифрів. Київ : Наука, 2012. 142 с.
12. Саломан А. Криптографія з відкритим ключем. Київ: Наука, 2013. 342 с.
13. Серов Р. Е., Гончаров В. В. Основы современной криптографии. Москва : Горячая линия – Телеком, 2011. 443 с.
14. Чмора А. Л. Сучасна прикладна криптографія Москва : Геліос АРВ, 2012. 256 с.

Стаття надійшла до редколегії 23.05.2021

Kataieva Yevheniia
PhD (Eng.), Associate Professor, Department of software for automated systems, *orcid.org/0000-0003-1277-8031*
Cherkasy State Technological University, Cherkasy
Rebrikov Anton
Postgraduate student, Department of software for automated systems, *orcid.org/0000-0002-4482-2415*
Cherkasy State Technological University, Cherkasy

URGENCY OF USING HIDDEN DATA TRANSMISSION IN VIDEO FILES

Abstract. *The article examines the problems of protecting information from unwanted access, which have tried to solve throughout the existence of mankind. Nowadays, the widespread use of electronic means of communication, electronic eavesdropping and fraud, a variety of computer viruses and other electronic hazards, electronic systems place high demands on the protection of information. Thus, the study of digital steganography is an urgent task. There are two main areas of hidden data transmission: cryptography and steganography. The purpose of cryptography is to restrict access to information by encrypting it. Unlike cryptography, steganography allows you to hide the very fact of the presence of hidden data. The study examined the main methods of covert data transmission using computer steganography, namely: the method of using system-reserved areas of digital data formats, methods of hiding information by special formatting of text files, which include the use of word, sentence or paragraph shift, selection certain positions of letters in the text or the use of properties of system fields that are not displayed on the screen, the method of using simulation functions, methods of using unused disk sectors, the method of using redundant media files (audio, photo and video). Currently, due to the growth of information and increasing the bandwidth of communication channels, the issue of hiding information in video sequences is becoming increasingly important. The transmission of digital video in recent years is a typical event and does not arouse suspicion. In the course of the research the peculiarities of hiding information in video files are considered, the comparison of existing algorithms of computer video steganography is made. The task is to develop your own algorithm for embedding information in the blue color channel of video files. The object of research is the transfer of hidden data in digital media files. The subject of research is the transmission of hidden data in the video stream. The purpose of research is to review the subject area, to examine the available methods of embedding information in media files in general and specifically in video files, to identify the advantages and disadvantages of existing algorithms, to develop their own algorithm of video steganography based on previously obtained research results. Research methods - methods of information theory, probability theory and mathematical statistics; methods of digital processing of signals, static images and video files; methods of vector analysis. The results of research - an overview of the features of hiding information in video files, compared existing algorithms of computer video steganography.*

Keywords: Steganography; information protection; media files; communication channels; blue color

References

1. Gribunin, V. G., Turincev, I. V. (2009). Digital steganography. Moscow: Solon-Press.
2. Seiedi, S., Sadihov, R. (2013). Comparison of Steganography Methods in Images. *Informatika*, 1.
3. Vichyslytelnie sety, teoryya y praktyka – Klassyfykacyya y sravnenye steganografycheskyx [electronic source]. Available: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=9&pa=13&ar=1.
4. Chuvstvytelnost k svetu, chuvstvytelnost k czvetu glaza [electronic source]. Available: http://www.simple-clerk.narod.ru/COLOR/d000.htm.
5. Metody pryxovuvannya informaciyi v grafichnyx zobrazhennyax [electronic source]. Available: https://ela.kpi.ua/bitstream/123456789/23826/4/
6. Konakhovich, G. F., Puzirenko, A. Yu. (2006). Computer steganography. Theory and practice. Moscow: MK-Press.
7. Melnyk, S. V., Kondakova, S. V. (2010). Global trends in the development of digital steganography in the context of the tasks of ensuring the information security of the state. Kiyv : Zb. mater. nauk.-prakt. konf.
8. Eltisheva, E. Iu., Fyonov, A. N. (2009). Construction of a stegosystem on the basis of raster images taking into account the statistics of the least significant bits. *Vestnyk SybHUTY*.
9. Zhylkyn, M. Yu. (2008). Stegoanalysis of graphic data based on compression methods. *Vestnyk SybHUTY*.
10. Pavlov, K. A. (2010). Cryptographic methods of protection. Moscow: DMK.
11. Rostovtsev, A. H., Mykhailova, N. V. (2012). Methods of cryptanalysis of classical ciphers. Kiyv : Nauka
12. Saloman, A. (2013). Public key cryptography. Kiyv: Nauka.
13. Serov, R. E., Honcharov, V. V. (2011). Fundamentals of modern cryptography. Moscow: Telecom.
14. Chmora, A. L. (2012). Modern applied cryptography. Moscow : Gelios.

Посилання на публікацію

APA Kataieva, Yevheniia & Rebrikov, Anton. (2021). Urgency of using hidden data transmission in video files. *Management of Development of Complex Systems*, 46, 48–54, dx.doi.org\10.32347/2412-9933.2021.46.48-54.

ДСТУ Катаєва Є. Ю., Ребріков А. Г. Актуальність використання прихованої передачі даних у відеофайлах. *Управління розвитком складних систем.* Київ, 2021. № 46. С. 48 – 54, dx.doi.org\10.32347/2412-9933.2021.46.48-54.