МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

АХМАМЕТЬЄВА ГАННА ВАЛЕРІЇВНА

УДК 004.056.5

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТЕГАНОАНАЛІЗУ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ І ВІДЕО

05.13.21 — системи захисту інформації

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Одеса — 2017

Дисертацією є рукопис.
Робота виконана в Одеському національному політехнічному університеті

Науковий керівник — доктор технічних наук, професор
Кобозєва Алла Анатоліївна,
Одеський національний політехнічний університет,
завідувач кафедри інформатики та управління
захистом інформаційних систем

Офіційні опоненти: — доктор технічних наук, професор,
Василіу Євген Вікторович
Одеська національна академія зв'язку
ім. О.С. Попова,
директор навчально-наукового інституту

кандидат технічних наук, доцент
Браіловський Микола Миколайович
Київський національний університет
ім. Т.Г. Шевченка,
доцент кафедри кібербезпеки та захисту інформації

Захист відбудеться «04» травня 2017 р. о 14:00 годині на засіданні спеціалізованої вченої ради К 41.052.11 в Одеському національному політехнічному університеті за адресою: 65044, м. Одеса, пр. Шевченка, 1, ауд. 400-А.

З дисертацією можна ознайомитись у бібліотеці Одеського національного політехнічного університету за адресою: 65044, м. Одеса, пр. Шевченка, 1.

Автореферат розісланий «30» березня 2017 р.

Вчений секретар
спеціалізованої вченої ради — О.О.Фомін

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Сучасні розробки в області стеганографії, новітні підходи до розробки стеганографічних систем, нетрадиційне використання існуючих стеганографічних методів (СГМ) та алгоритмів сприяють їх широкому розповсюдженню в інформаційному просторі. Вільним доступом до мережі Internet та ресурсів з науковими розробками користуються і зловмисники з метою здійснити антидержавні дії та скрити сліди злочину, у тому числі за допомогою стеганографії, яка дозволяє передавити додаткову інформацію (ДІ) по відкритому каналу зв'язку, забезпечуючи приховування самого факту її присутності у контейнері. В якості контейнерів в сучасній стеганографії можуть виступати цифрові зображення (ЦЗ), аудіо та відео послідовності (ЦВ). Результат вбудови ДІ у контейнер будемо називати стеганоповідомленням (СП).

В умовах найжорсткішої конкуренції, наявності випадків тероризму прихована комунікація може призвести до значних збитків для компаній, до катастрофічних наслідків терактів для суспільства взагалі. З метою попередження зловмисних дій з використанням сучасної цифрової стеганографії актуальним є розвиток та підвищення ефективності стеганоаналізу, основною задачею якого є виявлення факту наявності/відсутності прихованої інформації у будь-якому інформаційному контенті, зокрема цифровому (ЦК), в якості якого в роботі розглядаються ЦЗ та ЦВ.

Розробки в області стеганоаналізу ведуть вчені всього світу: І.І. Бобок, І.А. Узун, А.А. Кобозєва, A.D. Ker, J. Fridrich, Udit Budhia, Q.Z. Liu, S.R. Visavalia, Xikai Xu та інші, але остаточного рішення задача виявлення ДІ в ЦЗ/ЦВ не отримала і досі.

Серед існуючих СГМ широке розповсюдження отримав метод модифікації найменшого значущого біта (LSB) завдяки простоті реалізації, можливості забезпечення високої пропускної спроможності прихованого каналу зв'язку (ППС), використанню як у просторовій області, так і в області перетворень ЦК. Довголіттю даного методу сприяє його «нетрадиційне» використання сьогодні, коли вбудова ДІ виконується з малою ППС, що значно ускладнює процес стеганоаналізу.

Велика кількість стеганоаналітичних розробок спрямована на детектування наявності/відсутності ДІ, вбудованої методом LSB, у ЦЗ. Але сучасні стеганоаналітичні методи (САМ) часто виявляються недієздатними в умовах ППС ≤ 0.25 біт/піксель, навіть не тестуються в таких умовах.

Застосування ЦВ-контейнерів в стеганографії дозволяє за рахунок великої кількості кадрів передавати з використанням LSB-методу значний об'єм даних навіть при малій ППС, що робить такі контейнери широко використовуваними. Але кількість і якість розробок, присвячених стеганоаналізу ЦВ, є недостатніми, існуючі САМ не забезпечують бажану ефективність, зокрема в умовах малої ППС, практично не розглядається задача стеганоаналізу ЦВ в випадку, коли стеганоперетворення зазнають лише деякі кадри ЦВ, що можна пояснити значною складністю задачі та неспроможністю існуючих підходів до її рішення.

Таким чином, задача розробки нових ефективних САМ і алгоритмів, направлених на виявлення наявності ДІ, вбудованої методом LSB, в тому числі, при малих значеннях ППС, у ЦЗ та ЦВ є важливою, а тема дисертації «Підвищення ефективності стеганоаналізу для цифрових зображень і відео» актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконувалася відповідно до пп. 1.2.1.1, 1.2.1.2, 1.2.3.4, 1.2.6.9 і 1.2.8 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014–2018 роки», визначених постановою Президії НАН України від 20.12.2013 № 179; відповідає перелі-

ку пріоритетних тематичних напрямків наукових досліджень і науково-технічних розробок на період до 2015 року, затвердженому Постановою Кабінету Міністрів України №942 від 7 вересня 2011р. Обраний напрямок дослідження відповідає пп. 4.11, 4.12 «Стратегії національної безпеки України», затвердженої Указом Президента України № 287/2015 від 26 травня 2015 р.

Дисертаційна робота виконана в Одеському національному політехнічному університеті відповідно до планів науково-дослідної роботи на тему «Розробка методів підвищення ефективності комплексної системи захисту інформації» (№ держреєстрації 0115U000834).

Мета і задачі дослідження. *Метою* роботи є підвищення ефективності стеганоаналізу для цифрових зображень і цифрових відео шляхом розробки методів, що детектують в них вкладення конфіденційної інформації LSB-методом, ефективних, у тому числі, при малих значеннях пропускної спроможності прихованого каналу зв'язку.

Ефективність стеганоаналізу оцінюється за допомогою: помилок першого (пропуск СП) та другого (визначення контейнеру як СП) роду; точності детектування ДІ (AD); інтегрального параметра ρ, що визначається за допомогою метода аналізу ROC-кривих.

Під малими значеннями ППС розуміються значення, не більші 0.25 біт/піксель.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Провести аналіз сучасного стану рішення задачі детектування наявності додаткової інформації, вбудованої в цифрові зображення/відео методом LSB.

2. Розробити теоретичний базис для методів детектування наявності додаткової інформації, вбудованої методом LSB в цифрових контентах, у тому числі, з малими значеннями пропускної спроможності прихованого каналу зв'язку, в ході чого обґрунтувати вибір області цифрових контентів для здійснення процесу стеганоаналізу.

3. Розробити стеганоаналітичні методи, направлені на виявлення наявності додаткової інформації у цифрових відео та стеганоаналітичний метод, що здійснює стеганоаналіз окремих кадрів цифрових відео та окремих цифрових зображень, за умови вбудови додаткової інформації методом LSB в одну постійну колірну складову контейнера, ефективні, у тому числі, в умовах малої пропускної спроможності прихованого каналу зв'язку, такі, що здійснюють аналіз просторової області контенту.

4. Розробити метод, який використовує для аналізу просторову область контенту, що дозволяє відокремлювати цифрові контенти, перезбережені з формату з втратами у формат без втрат, від контентів, що спочатку зберігалися у форматі без втрат, який є складовою частиною розроблюваного комплексного стеганоаналітичного методу.

5. Провести аналіз ефективності алгоритмічних реалізацій розроблених стеганоаналітичних методів, у тому числі, порівняльний, на основі якого розробити практичні рекомендації для застосування окремих методів, з врахуванням яких розробити комплексний стеганоаналітичний метод виявлення результатів вбудови ДІ LSB-методом в ЦВ.

Об'єкт дослідження – процеси організації й виявлення стеганографічного каналу зв'язку.

Предмет дослідження – стеганоаналітичні методи для цифрових зображень і відео.

Методи дослідження. При формуванні теоретичного базису розроблюваних САМ використані загальний підхід до аналізу стану і технології функціонування інформаційних систем (ЗПАІС), матричний аналіз, теорія збурень, чисельні методи, методи обробки ЦЗ. При розробці САМ для ЦВ за умови вбудови ДІ методом LSB в одну постійну колірну складову контейнера використані матричний аналіз, теорія збурень. При розробці метода, спрямованого на детектування наявності ДІ в окремих кадрах ЦВ та окремих ЦЗ за умови вбудови ДІ методом LSB в одну довільну колірну складову контейнера, використані методи обробки ЦЗ. Для оцінки обчислювальної складності алгоритмічних реа-

лізацій розроблених методів використовувалася теорія алгоритмів.

Наукова новизна одержаних результатів полягає у наступному:

1. *Отримав подальший розвиток* загальний підхід до аналізу стану і технології функціонування інформаційних систем шляхом отримання критерію приналежності ненульового сингулярного числа блоку матриці одиничного рангу цифрового зображення/кадру відеопослідовності множині натуральних чисел, що визначає відповідність між характерними властивостями параметрів просторової області і області перетворення цифрових контентів. Це дозволило побудувати теоретичний базис для розроблених стеганоаналітичних методів для цифрових відео, які здійснюють аналіз просторової області контенту, що забезпечило їх високу ефективність при виявленні вкладень додаткової інформації LSB-методом, у тому числі в умовах малих значень пропускної спроможності прихованого каналу зв'язку, за рахунок відсутності додаткового накопичення обчислювальної похибки при переведенні цифрових контентів в область перетворень.

2. *Вперше* на основі побудованого теоретичного базису з врахуванням виявлених відмінностей у відносних змінах середньої кількості блоків з однаковими значеннями яскравості у колірній складовій в послідовності цифрових зображень/кадрів цифрових відео в результаті первинної та повторної вбудови додаткової інформації LSB-методом розроблені стеганоаналітичні методи для відеопослідовностей, ефективність яких перевищує ефективність сучасних аналогів, у тому числі при малій пропускній спроможності прихованого каналу зв'язку і малому розмірі кадрів, що дозволило підвищити ефективність стеганоаналізу цифрового відео.

3. *Вперше* на основі виявлених характерних властивостей послідовних тріад колірних триплетів для оригінальних цифрових зображень та зображень-стеганоповідомлень, побудованих за допомогою методу LSB, розроблено стеганоаналітичний метод, ефективність якого для цифрових зображень та окремих кадрів відеопослідовності в умовах вбудови додаткової інформації в одну довільну колірну складову контейнера, у тому числі, з малою пропускною спроможністю прихованого каналу зв'язку, перевищує сучасні аналоги, що дозволило підвищити ефективність стеганоаналізу для цифрових зображень/окремих кадрів цифрових відео.

4. *Вперше* на основі розроблених практичних рекомендацій щодо застосування побудованих методів стеганоаналізу цифрових зображень і відео, заснованих на отриманих оцінках їх ефективності, і розробленого методу відокремлення цифрових контентів, перезбережених в формат без втрат з формату з втратами, від контентів, що спочатку зберігалися в форматі без втрат, розроблений комплексний стеганоаналітичний метод виявлення вкладень додаткової інформації LSB-методом в цифрові відео, який, на відміну від існуючих, залишається ефективним для малих значень пропускної спроможності прихованого каналу зв'язку, при різній кількості колірних складових контейнера, що використовуються для стеганоперетворення, у тому числі, для контейнерів в градаціях сірого, незалежно від формату цифрового відео-контейнеру (з/без втрат).

Практичне значення одержаних результатів. Практична цінність роботи полягає у доведенні здобувачем отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані як складові комплексних систем захисту інформації будь-яких підприємств, організацій тощо.

Алгоритм, що реалізує розроблений САМ для ЦВ (як кольорових, так і в градаціях сірого), заснований на врахуванні відмінностей у відносних змінах середньої кількості блоків з однаковими значеннями яскравості колірної складової послідовності ЦЗ/кадрів ЦВ в результаті первинної і повторної вбудови ДІ, забезпечує ефективне виявлення СП, у тому числі, сформованого з малою ППС (аж до 0.125 біт/піксель) в одну (дві, три) колірні складові ЦВ, отриманих камерами мобільних пристроїв (*AD* для ППС 0.125

біт/піксель досягає 0.94, що на 1.2% перевищує найкращий з сучасних аналогів) та з ППС аж до 0.167 біт/піксель у випадку інших ЦВ (ефективність підвищено максимально на 7.5% (ППС 0.2 біт/піксель) у порівнянні з сучасними аналогами).

Стеганоаналітичний алгоритм (САА) виявлення результатів вбудови ДІ методом LSB з незначною ППС для ЦВ (як кольорових, так і в градаціях сірого), заснований на врахуванні відмінностей характеру змін кількості блоків з однаковими значеннями яскравості колірних складових послідовності ЦЗ/кадрів ЦВ в результаті первинної і повторної вбудови ДІ, забезпечує абсолютну ефективність (AD=1) виявлення СП, сформованих вбудовою ДІ з ППС не менше 0.167 біт/піксель в одну (дві, три) колірні складові ЦВ, що не досягалось сучасними аналогами. У випадку ЦВ з малим розміром кадрів висока ефективність забезпечується і для ППС 0.125 біт/піксель: помилки першого роду складають 6.12%, помилки другого роду 5.1%, що не забезпечується жодним з існуючих аналогів.

Алгоритм, що здійснює стеганоаналіз кольорових ЦЗ та окремих кадрів ЦВ забезпечує високу ефективність навіть при ППС 0.05-0.1 біт/піксель. Ефективність виявлення ДІ у ЦЗ при ППС 0.05/0.1 біт/піксель підвищена на 4.5/2.19 % відповідно (показник AD) і у 3.7/2.3 рази відповідно (показник ρ) у порівнянні з кращими аналогами. При стеганоаналізі ЦВ за допомогою САА, заснованому на аналізі послідовних тріад колірних триплетів, ефективність підвищено на 2.3% у порівнянні з кращими аналогами для ППС 0.1 біт/піксель, для ППС 0.0625 біт/піксель - на 14.93%, для ППС 0.05 біт/піксель досягається висока ефективність: $AD = 0.9391$, що не забезпечується жодним сучасним аналогом. У випадку покадрового стеганоаналізу ЦВ ефективність розробленого алгоритму на 5.5% перевищує сучасні аналоги у випадку ППС 0.1 біт/піксель при ступені заповнення кадрів 60-80%, та на 18/32% при ступені заповнення кадрів 40/20% відповідно.

Практичне значення отриманих результатів підтверджене актами впровадження у діяльність компанії «Планета Юг»; в навчальний процес кафедри інформатики та управління захистом інформаційних систем ОНПУ.

Особистий внесок здобувача. Результати дисертаційної роботи отримані автором самостійно. Роботи [1-4, 7-11] виконані без співавторів. В роботах, опублікованих у співавторстві, автору належить: встановлення властивостей блоків матриці ЦК в просторовій області, що відповідають наявності ненульового натурального сингулярного числа блока; розробка основних кроків САМ для виявлення результатів вбудови ДІ методом LSB з незначною ППС у випадку, коли в якості контейнера використовуються ЦВ або послідовність ЦЗ [5]; визначення порогових значень характеру змін кількості блоків з однаковими значеннями яскравості у ЦВ/послідовності ЦЗ, отриманих первинною вбудовою ДІ, у порівнянні з СП, отриманими в результаті повторної вбудови ДІ; розробка основних кроків САА та оцінка його ефективності шляхом визначення помилок першого та другого роду [6]; проведення обчислювальних експериментів [5-6].

Апробація результатів дисертації. Наукові результати і основні положення дисертаційної роботи доповідалися та обговорювалися на семінарах при Вченій раді НАН України «Технічні засоби захисту інформації» (Одеса, 2014) та 4 Міжнародних наукових конференціях [8-11].

Публікації. Матеріали дисертаційної роботи викладено в 11 публікаціях: 7 статей, 6 з яких опубліковано в журналах, які включені у Перелік фахових видань України; 6 статей – в журналах, включених до міжнародних наукометричних баз (Index Copernicus, РИНЦ, EBSCO, Google Scholar, Ulrich); 5 статей – без співавторів; 1 стаття – у зарубіжному періодичному виданні; 4 тези доповідей на міжнародних наукових конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, списку використаної літератури з 146 найменувань, 3 додатків на 5 сторінках, 13 рисунків і 18 таблиць – всього 162 сторінки. Основний текст дисерта-

ції складається з 130 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність напрямку дослідження, наведено зв'язок з науковими програмами, визначена мета й задачі роботи, показано наукову новизну та практичну цінність отриманих результатів, наведено інформацію про особистий внесок здобувача, апробацію наукових результатів роботи, публікації.

У **першому розділі** представлено огляд існуючих САМ для ЦВ та ЦЗ. На основі аналізу літературних джерел встановлено, що більшість сучасних САМ виконують аналіз ЦК в області перетворень, що є одною з причин їх недостатньої ефективності у випадку малої ППС завдяки накопиченню обчислювальної похибки при переході в область перетворень і назад. Стеганоаналіз просторової області ЦК найчастіше представлений аналізом пар кольорів, однак існуючі розробки мають значні обмеження і невисоку ефективність, якщо вбудова ДІ здійснюється з малою ППС.

Задача стеганоаналізу ЦВ до цього моменту є мало дослідженою, незважаючи на переваги використання ЦВ при стеганоперетворенні. Практично не розглядалося питання покадрового аналізу ЦВ у випадку, коли вбудова ДІ здійснюється лише у частину кадрів.

Таким чином, у розділі 1 показано, що задача підвищення ефективності стеганоаналізу ЦЗ і ЦВ, зокрема для малих значень ППС, залишається актуальною.

У **другому розділі** сформований теоретичний базис та на його основі розроблено САМ, направлені на виявлення вбудови ДІ у послідовності ЦЗ/ЦВ.

Обґрунтовано вибір області ЦК для здійснення процесу стеганоаналізу. Взагалі аналіз ЦЗ/ЦВ може бути проведеним як в області перетворень, так і в просторовій області. Але переведення ЦК в область перетворень призводить до додаткового накопичення обчислювальної похибки, що може значно ускладнити процес виявлення СП, сформованих, зокрема, при малих значеннях ППС. Тому найбільш перспективною для організації стеганоаналізу є просторова область ЦК, яка і використовується розробленими в роботі САМ.

В останній час для рішення задач стеганоаналізу добре зарекомендував себе ЗПАІС, у відповідності з яким зміна стану будь-якої інформаційної системи, зокрема стеганоперетворення ЦЗ, ЦВ формально може бути представлена у виді сукупності збурень повного набору параметрів: сингулярних чисел (СНЧ) та сингулярних векторів відповідних матриць.

ЦЗ (схема RGB) формалізується у вигляді сукупності трьох матриць R, G і B - колірних складових. При практичному аналізі з використанням ЗПАІС особливостей СНЧ $n \times n$-блоків матриць оригінальних ЦЗ, отриманих шляхом стандартного розбиття, практично в кожному ЦЗ було виявлено наявність блоків, що мають єдине ненульове СНЧ, яке належить множині натуральних чисел N та є кратним n. Така особливість є важливою для задачі, що розглядається: вона є чутливою до малих збурень, зокрема стеганоперетворення, і може бути використана у процесі стеганоаналізу, оскільки в загальному випадку СНЧ є невід'ємними дійсними числами. Однак аналіз ЦК з використанням інструментів ЗПАІС потребує переведення його в область перетворень – область сингулярного розкладання відповідних матриць, що є небажаним. У зв'язку з цим в роботі встановлюється відповідність між виявленими характерними особливостями СНЧ блоків (область перетворення) та особливостями значень яскравості пікселів (просторова область ЦЗ) цих блоків.

Теорема 1 (*необхідна умова належності ненульового СНЧ матриці одиничного рангу множині натуральних чисел*). Нехай A - $n \times n$-матриця, $\sigma_1, \sigma_2, ..., \sigma_n$ - СНЧ A, при

цьому $\sigma_1 > 0, \sigma_2 = ... = \sigma_n = 0$, $\sigma_1 \in \mathrm{N}$, $\sigma_1 \vdots n$, де N - множина натуральних чисел, тоді A має наступний вид:

$$A = \left(a_{ij}\right)_{i,j=1}^{n},\ a_{ij} = a,\ i,j = \overline{1,n}, a \neq 0. \quad (1)$$

Доведення. Побудуємо для A нормальне сингулярне розкладання: $A = U\Sigma V^T = \sum_{k=1}^{n} \sigma_k u_k v_k^T$, де U, V - $n \times n$ ортогональні матриці, стовпці яких $u_k, v_k, k = \overline{1,n}$, є лексикографічно додатними лівими та правими СНВ матриці A відповідно, $\Sigma = diag\left(\sigma_1, \sigma_2, ..., \sigma_n\right)$ - матриця СНЧ, в загальному випадку $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_n \geq 0$. З врахуванням умови $\sigma_1 > 0, \sigma_2 = ... = \sigma_n = 0$: $A = \sigma_1 u_1 v_1^T$. Оскільки для матриці (блоку матриці) ЦЗ розміру $n \times n$ СНВ u_1, v_1 мало відрізняються від n-оптимального вектора $n^O = \left(1/\sqrt{n}, ..., 1/\sqrt{n}\right)^T \in R^n$, тобто $u_1 \approx n^O$, $v_1 \approx n^O$, то:

$$A = \sigma_1 u_1 v_1^T = \sigma_1 n^O \left(n^O\right)^T = \sigma_1 \left(1/\sqrt{n}, ..., 1/\sqrt{n}\right)^T \left(1/\sqrt{n}, ..., 1/\sqrt{n}\right) = \begin{pmatrix} \sigma_1/n & ... & \sigma_1/n \\ ..... & & \\ \sigma_1/n & ... & \sigma_1/n \end{pmatrix},$$

звідки, з врахуванням, що σ_1 кратне n, безпосередньо витікає висновок теореми.

В ході обчислювального експерименту, проведеного з метою практичного підтвердження висновку теореми 1, було встановлено, що у просторовій області більше 99% $n \times n$-блоків з рангом 1 мають вид (1), де $a \in \{1,2,3,...,255\}$.

Теорема 2 (*достатня умова належності єдиного ненульового СНЧ матриці ЦЗ множині натуральних чисел*). Для $n \times n$-матриці A виду (1) максимальне СНЧ буде визначатися як $\sigma_1 = na \in \mathrm{N}$, а для інших СНЧ виконується умова $\sigma_2 = ... = \sigma_n = 0$.

Доведення. Умова $\sigma_2 = ... = \sigma_n = 0$ для матриці A витікає з її одиничного рангу. Енергії $En(A)$ сигналу, формальним представленням якого є A з елементами a_{ij}, $i,j = \overline{1,n}$, і СНЧ $\sigma_1 \geq ... \geq \sigma_n \geq 0$, може бути обчислена: $En(A) = \sum_{i,j=1}^{n} a_{ij}^2 = \sum_{i=1}^{n} \sigma_i^2$. З урахуванням умов теореми: $En(A) = n^2 a^2 = \sigma_1^2$, з чого витікає: $\sigma_1 = na \in \mathrm{N}$.

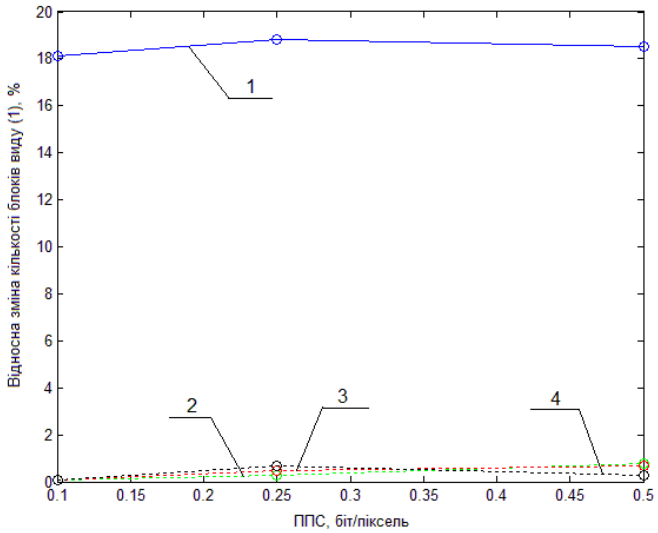
З теорем 1 і 2 отримано критерій належності єдиного ненульового СНЧ матриці (блоку матриці) ЦЗ множині натуральних чисел:

Твердження 1. Для того, щоб єдине ненульове СНЧ σ_1 $n \times n$-матриці (блоку матриці) A ЦЗ належало множині натуральних чисел, необхідно і достатньо, щоб A мала вид (1), при цьому $\sigma_1 = na \in \mathrm{N}$.

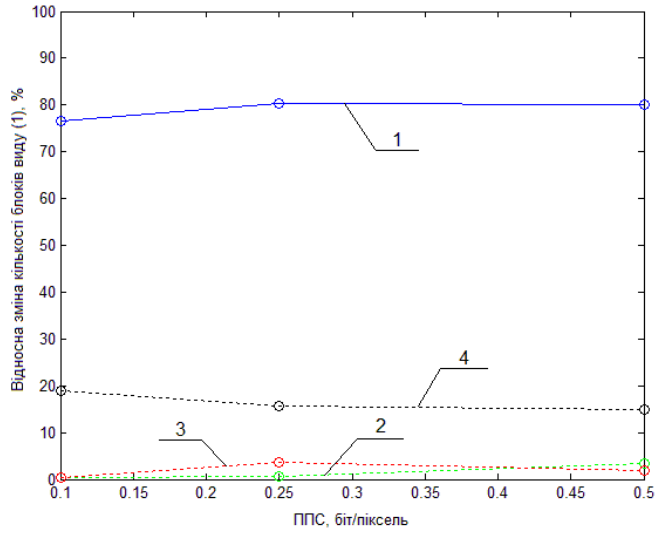
Зміна лише одного елементу матриці A, яка може виникнути в результаті стеганоперетворення, призведе до $\sigma_1 \notin \mathrm{N}$, що може служити показником порушення цілісності ЦК, зокрема показником стеганоперетворення.

З метою розробки САМ, використовуючих твердження 1, був проведений обчислювальний експеримент, направлений на отримання кількісної оцінки наявності блоків виду (1) різного розміру ($4 \times 4, 6 \times 6, 8 \times 8, 10 \times 10, 12 \times 12$) у ЦЗ. В експерименті були задіяні: множина I_1 - 200 ЦЗ у форматі TIFF з бази NRCS; множина I_2 - 200 ЦЗ у форматі TIFF, отриманих непрофесійними фотокамерами; I_3 - 203 ЦЗ у форматі JPG з бази NRCS; I_4 - 201 високоякісних ЦЗ у форматі JPG з WallpapersCraft; множина I_5 - 215 ЦЗ у форматі JPG, отриманих непрофесійними фотокамерами. Ці множини ЦЗ використовуються в роботі при проведенні обчислювальних експериментів.

По результатам експерименту встановлено, що кількість блоків (1) у R, G, B монотонно зменшується з ростом розміру блоку незалежно від конкретної множини ЦЗ. Кількісно найбільш вираженим факт наявності блоків виду (1) виявився при використанні 4×4-блоків. Відсутність 4×4-блоків виду (1) спостерігалася у 9% від загальної кількості колірних матриць ЦЗ в форматах без втрат (I_1 і I_2), та лише у 2.2% колірних матриць ЦЗ у форматах з втратами (I_3, I_4 і I_5). Така відмінність пояснюється стиском з втратами ЦЗ: округлення коефіцієнтів дискретного косинусного перетворення після квантування призводять до уніфікації сусідніх близьких по значеннях яскравостей до їх середнього значення.



а



б

Рисунок 1 – Залежність відносної зміни середнього значення кількості (%) 4×4-блоків виду (1) в матрицях ЦЗ від ППС: 1 – для СП отриманого в результаті первинної вбудови ДІ у порівнянні з оригінальним ЦЗ; 2 – для СП, отриманого шляхом повторної вбудови ДІ у СП з ППС 0.5 біт/піксель; 3 – для СП, отриманого повторною вбудовою ДІ у СП, сформоване з ППС 0.25 біт/піксель; 4 – для СП, отриманого повторною вбудовою ДІ у СП, сформоване з ППС 0.1 біт/піксель; а – ЦЗ з множини I_2; б – ЦЗ з множини I_5

З вищесказаного витікає гіпотеза: кількість 4×4-блоків виду (1) у СП буде незначною (можливо такі блоки будуть відсутні), що призведе до малих значень відносної кількості таких блоків після повторної вбудови ДІ у порівнянні з первинною вбудовою ДІ. Для оцінки відносної (по відношенню до загальної кількості блоків у матриці колірної складової ЦЗ) кількості 4×4-блоків виду (1) у СП, сформованих первинною вбудовою ДІ в контейнер, та СП, сформованих повторною вбудовою ДІ в ЦЗ-СП був проведений обчислювальний експеримент, результати якого знаходяться у повній відповідності з висунутою гіпотезою, а їх ілюстрація для одного ЦЗ представлена на рис.1: результати первинного та повторного стеганоперетворення кількісно відрізняються між собою настільки, що дають принципову можливість відокремити послідовність незаповнених ЦЗ від послідовності ЦЗ-СП.

Встановлено, що відносні зміни в результаті первинної вбудови ДІ у ЦЗ з множини I_2 (формат без втрат) порівняні з відносними змінами при повторній вбудові ДІ у ЦЗ з множини I_5 (формат з втратами). Таким чином при розробці САМ, заснованого на отриманих вище результатах, треба забезпечити можливість для визначення формату контейнера, що робиться за допомогою методу відокремлення ЦК, перезбережених з формату з втратами у формат без втрат, від ЦК, що початково зберігалися у форматі без втрат, який розроблено у розділі 3.

З врахуванням отриманих результатів розроблено САМ, який далі позначається

CAM1, для ЦВ/послідовності ЦЗ. Для послідовності з P кадрів ЦВ/ЦЗ $C_1, C_2, \ldots, C_P$ з колірними складовими $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ основні кроки CAM1 наступні:

Крок 1. Визначення формату оригінального контейнеру для вибору порогових значень, що використовуються на наступних кроках.

Крок 2. Вбудова ДІ (випадково сформованої бінарної послідовності). Для кожного C_i, $i = \overline{1, P}$: вбудувати у $Y_i^{(C)} \in \left\{R_i^{(C)}, G_i^{(C)}, B_i^{(C)}\right\}$ - колірні складові C_i методом LSB ДІ з ППС t біт/піксель, $t \in \{0.5, 0.25, 0.1\}$. Результат - S_i^t з колірними складовими $Y_i^{(t)} \in \left\{R_i^{(t)}, G_i^{(t)}, B_i^{(t)}\right\}$.

Крок 3. Для $i = \overline{1, P}$:

3.1. Визначити $ky_i^{(C)}$, $ky_i^{(C)} \in \left\{kr_i^{(C)}, kg_i^{(C)}, kb_i^{(C)}\right\}$ - кількість 4×4-блоків виду (1) у $Y_i^{(C)} \in \left\{R_i^{(C)}, G_i^{(C)}, B_i^{(C)}\right\}$ відповідно;

3.2. Визначити $ky_i^{(t)}$, $ky_i^{(t)} \in \left\{kr_i^{(t)}, kg_i^{(t)}, kb_i^{(t)}\right\}$, $t \in \{0.5, 0.25, 0.1\}$ - кількість 4×4-блоків виду (1) у $Y_i^{(t)} \in \left\{R_i^{(t)}, G_i^{(t)}, B_i^{(t)}\right\}$ відповідно.

Крок 4. Для $i = \overline{1, P}$:

4.1. Обчислити $ry_i^{(C)}$, $ry_i^{(C)} \in \left\{rr_i^{(C)}, rg_i^{(C)}, rb_i^{(C)}\right\}$ - відносну кількість 4×4-блоків у $Y_i^{(C)} \in \left\{R_i^{(C)}, G_i^{(C)}, B_i^{(C)}\right\}$ відповідно (у %);

4.2. Обчислити $ry_i^{(t)}$, $ry_i^{(t)} \in \left\{rr_i^{(C)}, rg_i^{(C)}, rb_i^{(C)}\right\}$, $t \in \{0.5, 0.25, 0.1\}$ - відносну кількість 4×4-блоків у $Y_i^{(t)} \in \left\{R_i^{(t)}, G_i^{(t)}, B_i^{(t)}\right\}$ відповідно (у %).

Крок 5. Визначити: $\overline{ry}^{(C)} = \frac{1}{P}\sum_{i=1}^{P} ry_i^{(C)}$; $\overline{ry}^{(t)} = \frac{1}{P}\sum_{i=1}^{P} ry_i^{(t)}$, де $\overline{ry}^{(C)}, \overline{ry}^{(t)}$ - середні значення кількості (%) 4×4-блоків виду (1) по всім ЦЗ/кадрам ЦВ відповідно для C_i та S_i^t, $\overline{ry}^{(C)} \in \left\{\overline{rr}^{(C)}, \overline{rg}^{(C)}, \overline{rb}^{(C)}\right\}$, $\overline{ry}^{(t)} \in \left\{\overline{rr}^{(t)}, \overline{rg}^{(t)}, \overline{rb}^{(t)}\right\}$, $t \in \{0.5, 0.25, 0.1\}$.

Крок 6. Обчислити $\overline{Y}_t = \left(\left|\overline{ry}^{(C)} - \overline{ry}^{(t)}\right| \Big/ \overline{ry}^{(C)}\right) \cdot 100\%$, де $\overline{Y}_t$ - зміни середнього значення кількості 4×4-блоків виду (1) відповідних колірних складових C_i у порівнянні з S_i^t, $\overline{Y}_t \in \left\{\overline{R}_t, \overline{G}_t, \overline{B}_t\right\}$, $t \in \{0.5, 0.25, 0.1\}$.

Крок7. *Детектування наявності ДІ.*

Якщо $\left(\overline{Y}_{t_1} < T_Y \text{ AND } \overline{Y}_{t_2} < T_Y\right) \text{OR } \left(\overline{Y}_{t_1} < T_Y \text{ AND } \overline{T}_{t_3} < T_Y\right) \text{OR} \left(\overline{Y}_{t_2} < T_Y \text{ AND } \overline{Y}_{t_3} < T_Y\right)$ $\text{OR } \left(\overline{Y}_{t_1} < T_Y \text{ AND } \overline{Y}_{t_2} < T_Y \text{ AND } \overline{Y}_{t_3} < T_Y\right)$, де $\overline{Y}_t \in \left\{\overline{R}_t, \overline{G}_t, \overline{B}_t\right\}$, $t_j \in t \in \{0.5, 0.25, 0.1\}$, $T_Y \in \left\{T_R, T_G, T_B\right\}$, *то* $C_1, C_2, ..., C_P$ містять вбудовану ДІ у Y-ій колірній складовій, $Y \in \left\{R, G, B\right\}$, *інакше* ДІ відсутня у Y-ій колірній складовій $C_1, C_2, ..., C_P$,

де $T_Y \in \left\{T_R, T_G, T_B\right\}$ – порогові значення для кожної колірної складової, які визначаються на основі результатів обчислювального експерименту окремо для форматів з втратами та форматів без втрат. Порогові значення рекомендується приймати однаковими для різних значень ППС, оскільки при стеганоаналізі невідомо, з яким значенням ППС здійснювалась вбудова ДІ.

Основним недоліком CAM1 є залежність кількості блоків (1) від виду ЦК. Для ЦК, навіть у випадку великого розміру, який містить дуже багато дрібних деталей, кількість блоків виду (1) буде незначною (аж до 0), що значно ускладнює процес стеганоаналізу. Для ЦВ з малим розміром кадрів метод може виявитися недостатньо ефективним, зважаючи на початково невелику загальну кількість блоків у кадрі. З метою забезпечення

можливості ефективного стеганоаналізу ЦВ з малим розміром кадрів було визначено параметр, що якісно характеризує зміни кількості блоків виду (1) (зменшення, збільшення або незмінність) в результаті первинної та повторної вбудови ДІ. Таку якісну характеристику будемо називати характером зміни кількості блоків виду (1).

На основі ЦЗ з множин $I_1,...,I_5$ було проведено обчислювальний експеримент, який показав, що в результаті первинної вбудови ДІ у більшості матриць колірних складових ЦЗ (не залежно від формату контейнеру) спостерігається зменшення кількості 4×4-блоків виду (1): у ЦК в форматах з втратами зменшення спостерігається у 80-90% матриць, у ЦК в форматах без втрат – у 34-46% матриць. Якщо вбудова ДІ здійснюється повторно у ЦЗ-СП, то зменшення блоків з однаковими значеннями яскравості майже не спостерігається (аж до 0, особливо, якщо ППС при первинній вбудові ДІ складала 0.25-0.5 біт/піксель).

Таким чином, на основі характеру змін кількості 4×4-блоків виду (1) більшості елементів (ЦЗ, кадрів ЦВ) послідовності можна зробити висновок про наявність/відсутність ДІ у ЦК. З врахуванням проведених досліджень основні кроки CAM CAM2 наступні:

Кроки 1, 2 відповідають крокам 2, 3 відповідно методу CAM1.

Крок 3. Визначення характеру змін кількості 4×4-блоків виду (1) у кожній колірній складовій. Для $i=\overline{1,P}$: $dY_i^{(t)}=ky_i^{(C)}-ky_i^{(t)}$, де $dY_i^{(t)}\in\{dR_i^{(t)},dG_i^{(t)},dB_i^{(t)}\}$, $t\in\{0.5,0.25,0.1\}$, $ky_i^{(C)}\in\{kr_i^{(C)},kg_i^{(C)},kb_i^{(C)}\}$, $ky_i^{(t)}\in\{kr_i^{(t)},kg_i^{(t)},kb_i^{(t)}\}$.

Крок 4. Визначити загальну кількість матриць ЦЗ/кадрів ЦВ, у яких спостерігається зменшення кількості 4×4-блоків з однаковими значеннями яскравості у кожній колірній складовій. Для $i=\overline{1,P}$:

Якщо $dY_i^{(t)}>0$, *то* $kY^{(t)}=kY^{(t)}+1$ ($kY^{(t)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4-блоків виду (1)), де $t\in\{0.5,0.25,0.1\}$, $dY_i^{(t)}\in\{dR_i^{(t)},dG_i^{(t)},dB_i^{(t)}\}$, при цьому відповідно $kY^{(t)}\in\{kR^{(t)},kG^{(t)},kB^{(t)}\}$, початкові значення $kY^{(t)}=0$.

Крок 5. Обчислити: $pY^{(t)}=\left(kY^{(t)}/P\right)\cdot100\%$, де $pY^{(t)}\in\{pR^{(t)},pG^{(t)},pB^{(t)}\}$, $kY^{(t)}\in\{kR^{(t)},kG^{(t)},kB^{(t)}\}$, $t\in\{0.5,0.25,0.1\}$.

Крок 6. *Детектування вбудови ДІ.*

Якщо

$$\left(pY^{(t_1)}\le T\text{ AND }pY^{(t_2)}\le T\right)\text{OR}\left(pY^{(t_1)}\le T\text{ AND }pY^{(t_3)}\le T\right)\text{OR}\left(pY^{(t_2)}\le T\text{ AND }pY^{(t_3)}\le T\right)$$
$$\text{OR}\left(pY^{(t_1)}\le T\text{ AND }pY^{(t_2)}\le T\text{ AND }pY^{(t_3)}\le T\right),$$

де $pY^{(t)}\in\{pR^{(t)},pG^{(t)},pB^{(t)}\}$, $t_j\in\{t_1=0.5,t_2=0.25,t_3=0.1\}$, *то* $C_1,C_2,...,C_P$ містять вбудовану ДІ у Y-ій колірній складовій, $Y\in\{R,G,B\}$; *інакше* ДІ відсутня у Y-ій колірній складовій $C_1,C_2,...,C_P$, де T – порогове значення, яке характеризує максимальну кількість кадрів у ЦВ (зображень у послідовності ЦЗ), у яких спостерігалося зменшення кількості 4×4-блоків виду (1) при повторній вбудові ДІ.

Розроблений CAM2 може використовуватися для стеганоаналізу як кольорових ЦВ, так і ЦВ у градаціях сірого, у тому числі ЦВ з малим розміром кадрів.

У **третьому розділі** розроблено CAM, направлений на виявлення вбудови ДІ в окремих ЦЗ/кадрах ЦВ; проведена адаптація розроблено CAM для ЦВ.

Кожний колір $M\times N$-ЦЗ визначається триплетом значень $(r_{i,j},g_{i,j},b_{i,j})$ пікселя $pc(i,j)$, $i=\overline{1,M}$, $j=\overline{1,N}$, який представлений значеннями яскравості червоної, зеленої

та синьої колірної складових у діапазоні [0, 255].

Визначення 1. Усі різні триплети значень $(r_{i,j}, g_{i,j}, b_{i,j})$, $i = \overline{1,M}$, $j = \overline{1,N}$, в межах ЦЗ будемо називати унікальними кольорами. Їх кількість позначимо U.

Визначення 2. Матрицею унікальних кольорів UCT будемо називати матрицю розміром $U \times 3$, рядки якої містять унікальні кольори $(\breve{r}_k, \breve{g}_k, \breve{b}_k)$, $k = \overline{1,U}$.

Матриця UCT не враховує частоту появи триплету $(\breve{r}_k, \breve{g}_k, \breve{b}_k) \in UCT$ у ЦЗ. При вбудові ДІ в одну довільну колірну складову триплету $(\breve{r}_k, \breve{g}_k, \breve{b}_k)$ модифікується лише один його елемент. Якщо триплет зустрічається у ЦЗ не одноразово, то при вбудові ДІ методом LSB зростає ймовірність того, що він може бути змінений трьома способами: значення яскравості колірної складової може збільшитися/зменшитися на 1, залишитися незмінним. Таким чином, можна припустити, що матриця UCT СП буде містити більше послідовностей триплетів, що відрізняються між собою лише на одиницю у той колірній складовій, в яку здійснювалась вбудова ДІ, ніж UCT контейнера, що може сигналізувати про модифікації яскравості колірних складових ЦЗ.

Визначення 3. Послідовними Red-, Green-, Blue-тріадами триплетів у матриці унікальних кольорів будемо називати тріади:

$$(\breve{r}_k, \breve{g}_k, \breve{b}_k) \in UCT \;\&\; (\breve{r}_k - 1, \breve{g}_k, \breve{b}_k) \in UCT \;\&\; (\breve{r}_k + 1, \breve{g}_k, \breve{b}_k) \in UCT, k = \overline{1,U}; \quad (2)$$

$$(\breve{r}_k, \breve{g}_k, \breve{b}_k) \in UCT \;\&\; (\breve{r}_k, \breve{g}_k - 1, \breve{b}_k) \in UCT \;\&\; (\breve{r}_k, \breve{g}_k + 1, \breve{b}_k) \in UCT, k = \overline{1,U}; \quad (3)$$

$$(\breve{r}_k, \breve{g}_k, \breve{b}_k) \in UCT \;\&\; (\breve{r}_k, \breve{g}_k, \breve{b}_k - 1) \in UCT \;\&\; (\breve{r}_k, \breve{g}_k, \breve{b}_k + 1) \in UCT, k = \overline{1,U}; \quad (4)$$

відповідно. При підрахуванні кількості послідовних тріад триплетів будемо асоціювати послідовну тріаду з $(\breve{r}_k, \breve{g}_k, \breve{b}_k) \in UCT$, для якого виконуються умови (2), (3) або (4) в залежності від виду тріади. Триплет $(\breve{r}_k, \breve{g}_k, \breve{b}_k) \in UCT$ будемо називати середнім, якщо для нього існує послідовна тріада.

Визначення 4. Основними тріадами триплетів будемо називати послідовні тріади, що відповідають тій колірній складовій контейнера, у яку здійснюється вбудова ДІ. Супутніми тріадами триплетів будемо називати такі послідовні тріади, які відповідають незаповненим ДІ колірним складовим контейнера.

На основі ЦЗ з множин $I_1, ..., I_5$ було проведено обчислювальний експеримент, направлений на підрахунок кількості послідовних тріад у незаповнених контейнерах та СП, сформованих вбудовою ДІ методом LSB-Matching в одну довільну колірну складову, який показав, що ЦЗ в форматах з втратами (контейнери) містять у середньому не більше 3% середніх триплетів по відношенню до загальної кількості унікальних кольорів U, при цьому максимальний вміст середніх триплетів не перевищує 12%. Інша ситуація спостерігається для ЦЗ в форматах без втрат, де вміст середніх триплетів початково високий (у середньому 40-60%), крім того, різниця між кількістю Red-, Green- та Blue-тріад одного ЦЗ складає не більше 1-1.5%. Це пояснюється відсутністю стиску та, як наслідок, більшою різноманітністю унікальних кольорів.

В результаті вбудови ДІ у матриці унікальних кольорів СП, сформованих на основі ЦЗ в форматах з втратами, характерно значне відносне зростання кількості послідовних тріад триплетів, особливо сильним є зростання основних тріад триплетів, які перевищують кількість супутніх тріад у 1.5-2 рази (зростання супутніх тріад триплетів пов'язано зі зростанням кількості унікальних кольорів при вбудові ДІ). У випадку СП, сформованих на основі ЦЗ в форматах без втрат, зміни у кількості послідовних тріад незначні.

Враховуючи отримані результати, основні кроки САМ САМЗ виявлення наявності ДІ, вбудованої в одну колірну складову ЦЗ/кадр ЦВ I розміром $M \times N$, що зберігається

в форматі з втратами, з колірними складовими R, G, B наступні:

Крок 1. Формування матриці UCT розміром $U \times 3$ унікальних триплетів кольорів $\left(\breve{r}_k, \breve{g}_k, \breve{b}_k\right), k = \overline{1,U}$ для ЦЗ I.

Крок 2. Підрахування кількості послідовних тріад триплетів для кожної колірної складової.

2.1. *Якщо* для поточного триплету $\left(\breve{r}_k, \breve{g}_k, \breve{b}_k\right), k = \overline{1,U}$ в UCT одночасно існують триплети $\left(\breve{r}_k + 1, \breve{g}_k, \breve{b}_k\right)$ і $\left(\breve{r}_k - 1, \breve{g}_k, \breve{b}_k\right)$, *то* $countR = countR + 1$, $countR$ – кількість Red-тріад в UCT;

2.2. *Якщо* для поточного триплету $\left(\breve{r}_k, \breve{g}_k, \breve{b}_k\right), k = \overline{1,U}$ в UCT одночасно існують триплети $\left(\breve{r}_k, \breve{g}_k + 1, \breve{b}_k\right)$ і $\left(\breve{r}_k, \breve{g}_k - 1, \breve{b}_k\right)$, *то* $countG = countG + 1$, $countG$ – кількість Green-тріад в UCT;

2.3. *Якщо* для поточного триплету $\left(\breve{r}_k, \breve{g}_k, \breve{b}_k\right), k = \overline{1,U}$ в UCT одночасно існують триплети $\left(\breve{r}_k, \breve{g}_k, \breve{b}_k + 1\right)$ і $\left(\breve{r}_k, \breve{g}_k, \breve{b}_k - 1\right)$, *то* $countB = countB + 1$, $countB$ – кількість Blue-тріад в UCT.

Крок 3. Обчислити кількість середніх триплетів послідовних тріад відносно загальної кількості унікальних кольорів (%):

$$pR = \frac{countR}{U} \cdot 100,\ pG = \frac{countG}{U} \cdot 100,\ pB = \frac{countB}{U} \cdot 100;\ p_{\max} = \max(pR, pG, pB),$$

де $p_{\max}$ – максимальне значення серед pR, pG, pB.

Крок 4. *Детектування наявності/відсутності ДІ.*

4.1. *Якщо* $\left(pR = p_{\max}\right) \text{AND} \left(pR > T_{up}\right)$, *то* I містить вбудовану ДІ у червоній колірній складовій; *інакше якщо*

$$\left(\left(pR > T_{low}\right) \text{OR} \left(pG > T_{low}\right) \text{OR} \left(pB > T_{low}\right)\right) \text{AND} \left(\left(pR > 1.5 \cdot pG\right) \text{AND} \left(pR > 1.5 \cdot pB\right)\right)$$

то I містить вбудовану ДІ у червоній колірній складовій;

інакше ДІ відсутня у червоній колірній складовій;

4.2. *Якщо* $\left(pG = p_{\max}\right) \text{AND} \left(pG > T_{up}\right)$, *то* I містить вбудовану ДІ у зеленій колірній складовій, *інакше якщо*

$$\left(\left(pR > T_{low}\right) \text{OR} \left(pG > T_{low}\right) \text{OR} \left(pB > T_{low}\right)\right) \text{AND} \left(\left(pG > 1.5 \cdot pR\right) \text{AND} \left(pG > 1.5 \cdot pB\right)\right)$$

то I містить вбудовану ДІ у зеленій колірній складовій;

інакше ДІ відсутня у зеленій колірній складовій;

4.3. *Якщо* $\left(pB = p_{\max}\right) \text{AND} \left(pB > T_{up}\right)$, *то* I містить вбудовану ДІ у синій колірній складовій, *інакше якщо*

$$\left(\left(pR > T_{low}\right) \text{OR} \left(pG > T_{low}\right) \text{OR} \left(pB > T_{low}\right)\right) \text{AND} \left(\left(pB > 1.5 \cdot pR\right) \text{AND} \left(pB > 1.5 \cdot pG\right)\right)$$

то I містить вбудовану ДІ у синій колірній складовій,

інакше ДІ відсутня у синій колірній складовій;

де T_{low} і T_{up} – порогові значення. Порогове значення T_{low} характеризує максимальну кількість середніх триплетів послідовних тріад (%) у незаповнених контейнерах, неперевищення T_{low} усіма послідовними тріадами триплетів свідчить про оригінальне ЦЗ. Поріг T_{up} характеризує мінімальну кількість середніх триплетів послідовних тріад (%) в СП, перевищення T_{up} усіма послідовними тріадами свідчить про СП.

Для забезпечення можливості застосування розробленого методу для ЦВ за умови повного заповнення кадрів (вбудова ДІ здійснюється в усі кадри ЦВ) в роботі проведено його адаптацію для ЦВ – метод CAM3v:

Крок 1. Для кожного кадру ЦВ F_z, $z=\overline{1,P}$, здійснюється детектування в ньому ДІ згідно кроків 1-4 методу САМ3. Результатом детектування є матриця розміром $P\times 3$, яка містить значення 0 і 1: 0 – якщо ДІ відсутня у відповідній колірній складовій, 1 – якщо виявлено наявність ДІ у відповідній колірній складовій.

Крок 2. Підрахування кількості позитивних (значення 1) та негативних (значення 0) результатів детектування у кадрах ЦВ окремо для кожного виду послідовних тріад триплетів, що відповідають червоної, зеленої та синьої колірним складовим.

Крок 3. *Детектування наявності ДІ у ЦВ.*

Якщо кількість позитивних результатів детектування послідовних Red- (Green-, Blue-) тріад перевищує кількість негативних результатів, *то* ДІ міститься у червоній (зеленій, синій) колірній складовій, *інакше* ДІ відсутня у червоній (зеленій, синій) колірній складовій.

В процесі стеганоперетворення в якості контейнерів можуть виступати як ЦК в форматі з втратами, так і в форматі без втрат. Після вбудови ДІ у просторову область контейнера методом LSB СП зберігаються в форматі без втрат, тобто при стеганоаналізі маємо, як правило, ЦК в форматі без втрат (при відсутності оригінального контейнера). Можливість відокремлення ЦЗ, збереженого в форматі без втрат початково, від ЦЗ, перезбереженого в формат без втрат із формату з втратами, може підвищити ефективність стеганоаналізу, указавши на проведену з ЦЗ дію. Задача визначення формату оригінального контейнера є суттєвою в роботі: для розробленого методу САМ1 потрібний вибір порогових значень T_R, T_G, T_B в залежності від формату контейнера, розроблені методи САМ3 та САМ3v розраховані на контейнери в форматах з втратами.

Вище була виявлена характерна відмінність між ЦК у форматах з втратами та форматами без втрат, яка полягає у різниці між вмістом в відповідних матрицях послідовних тріад триплетів, на основі якої в роботі розроблений метод виявлення формату контейнера (МВФКА) для кольорового ЦЗ/кадру ЦВ:

Кроки 1-3. Кроки відповідають крокам 1-3 метода САМ3.

Крок 4. Визначення формату ЦК.

Якщо $\left(\left(pR>T_{\lim}\right)\&\left(pG>T_{\lim}\right)\&\left(pB>T_{\lim}\right)\right)$ при $pR\approx pG\approx pB$, *то* оригінальним форматом I є формат без втрат, *інакше* оригінальним форматом I є формат з втратами, де $T_{\lim}$ – порогове значення, що відокремлює ЦК, перезбережені з формату з втратами в формат без втрат, від ЦК, що початково зберігалися в форматі без втрат.

У **четвертому розділі** проводиться оцінка ефективності та порівняльний аналіз з сучасними аналогами САА, що реалізують розроблені САМ, розробляються практичні рекомендації для використання розроблених САМ і відповідних САА, на основі яких розробляється комплексний метод виявлення наявності ДІ у ЦВ/послідовності ЦЗ. Використовуються позначення: САА1, САА2, САА3, САА3v - алгоритми, які реалізують методи САМ1, САМ2, САМ3, САМ3v відповідно.

Для оцінки ефективності розроблених алгоритмів проводяться обчислювальні експерименти для ЦЗ з множин I_3, I_4, I_5, а також наступних ЦВ в форматах з втратами: 200 ЦВ розміром кадрів 320×240, отриманих камерами мобільних пристроїв (множина V_1); 167 ЦВ розміром кадрів 320×240, отриманих відеокамерою (множина V_2); 49 ЦВ розміром кадрів 176×144, отриманих камерою застарілої моделі мобільного телефону (множина V_3). У кожному ЦВ по 250 кадрів, після вбудови ДІ відео зберігаються без втрат в форматі *.avi.

Вбудова ДІ у ЦВ здійснюється в одну постійну колірну складову, обрану довільно для кожного ЦВ, з різними значеннями ППС, постійність обраної колірної складової

обумовлено особливостями зберігання оригінальних ЦВ в форматах з втратами, коли при стисненні відеоданих використовується метод кодування за відмінностями, який передбачає посилання на сусідні кадри, якщо відповідні пікселі сусідніх кадрів не відрізняються (наприклад, фонові ділянки). Вбудова ДІ у ЦЗ здійснюється в одну довільну колірну складову з різними значеннями ППС.

ЦВ-СП аналізуються алгоритмами САА1 з пороговими значеннями $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$, САА2 з пороговим значенням $T = 3$, САА3v з пороговими значеннями $T_{low} = 2.5$ и $T_{up} = 8$; ЦЗ-СП аналізуються алгоритмом САА3 з пороговими значеннями $T_{low} = 2.5$ и $T_{up} = 8$. Усі порогові значення були отримані в результаті обчислювальних експериментів. По результатам стеганоаналізу визначені помилки першого та другого роду, які для ЦВ наведені у табл.1. Для САА3 помилки 2-го роду виявлені не були, ненульові помилки 1-го роду були зафіксовані: для ЦЗ з I_3, I_5 лише при ППС 0.05 біт/піксель (1.97 і 2.32% відповідно), для ЦЗ з I_4 - для ППС ≤ 0.167 біт/піксель (від 0.5 до 7.96%), тобто алгоритм САА3 є ефективним при стеганоаналізі СП, сформованих вбудовою ДІ у ЦЗ навіть з ППС 0.05-0.1 біт/піксель.

Таблиця 1 –

Ефективність детектування наявності/відсутності ДІ у ЦВ алгоритмами САА1, САА2, САА3v, %

Алгоритм	Помилки	ППС, біт/піксель					
		0.5	0.25	0.167	0.125	0.1	0.05
ЦВ з множини V_1							
САА1	1-го роду	0	0	2.19	11.68	51.09	90.88
	2-го роду	0.36	0.36	0.36	0.36	0.73	6.14
САА2	1-го роду	0	0	0	64.23	97.08	100
	2-го роду	0	0	0	0	0	0
САА3v	1-го роду	0	0	0	0.73	2.19	32.12
	2-го роду	0	0	0	0	0	0
ЦВ з множини V_2							
САА1	1-го роду	0	0	19.56	98.26	100	100
	2-го роду	0	0	0	0	0	0
САА2	1-го роду	0	0	0	80	100	100
	2-го роду	0	0	0	0	0	0
САА3v	1-го роду	0	0	0	0	0	10
	2-го роду	0	0	0	0	0	0
ЦВ з множини V_3							
САА1	1-го роду	0	0	0	0	0	0
	2-го роду	94.90	94.90	94.90	91.84	91.84	91.84
САА2	1-го роду	0	0	0	6.12	40.82	90.82
	2-го роду	5.10	5.10	5.10	5.10	5.10	5.10
САА3v	1-го роду	79.59	83.67	85.71	95.92	93.88	85.71
	2-го роду	1.02	7.14	5.10	13.27	12.24	6.12

З табл.1 видно, що найкращі результати детектування досягаються методом САА3v, однак цей метод ефективний лише у випадках кольорових контейнерів, в які ДІ вбудовується лише в одну колірну складову. Алгоритми САА1 та САА2 мають гіршу ефективність детектування, ніж САА3v (особливо при малих значеннях ППС), але вони можуть використовуватися як для кольорових ЦВ, так і ЦВ в градаціях сірого, крім того ці методи спроможні виявляти наявність ДІ, вбудованої у дві або три колірні складові, на відміну від САА3v. Як і передбачалось, алгоритм САА1 є неефективним при детектуванні ЦВ з малим розміром кадрів (множина V_3), але він дає кращі результати детектування (у порівнянні з САА2) для ЦВ з множини V_1, при значеннях ППС не нижче 0.125 біт/піксель. Найефективнішим для виявлення вбудови ДІ у ЦВ з малим розміром кадрів (множина V_3) є алгоритм САА2.

При оцінці ефективності алгоритмічної реалізації методу виявлення формату контейнеру було отримано: помилки 1-го роду (пропуск факту стиску за його наявності) - 3%, помилки 2-го роду (визначення нестиснутого ЦК як стиснутого) – 4.5%, що дозволяє говорити про високу ефективність розробленого методу.

Обчислювальна складність алгоритмів САА1 і САА2 визначається як $P \cdot \underline{O}(M^2)$, де $M \times M$ – розмір матриці ЦЗ/кадру ЦВ, P – кількість кадрів ЦВ; для алгоритмів, що реалізують методи САМ3 і МВФКА, – $\underline{O}(M^4)$, для алгоритму САА3v – $P \cdot \underline{O}(M^4)$.

Порівняння ефективності усіх САА, здійснюється за допомогою точності виявлення $AD : AD = (TP + TN)/(TP + FN + TN + FP)$, де FN - помилки першого роду (%), FP - помилки другого роду (%), TP - відсоток правильно виявлених СП, TN - відсоток правильно виявлених незаповнених контейнерів.

Оцінка ефективності САА3, направленого на стеганоаналіз окремих ЦЗ, додатково здійснюється за допомогою інтегрального параметру ρ.

Для проведення порівняльного аналізу САА САА1, САА2, САА3v, використовувалися сучасні аналоги: V1(2005), V2(2005), V3(2007), V4(2013), V5(2015).

Для проведення порівняльного аналізу розробленого алгоритму САА3 використовувалися сучасні аналоги, що позначаються далі З1(2008), З2(2008), З3(2009), З4(2010), З5(2015), З6(2015) – за допомогою точності виявлення AD; Зі1(2005), Зі2(2008), Зі3(2011), Зі4(2011), Зі5(2011), Зі6(2011), Зі7(2011), Зі8(2012), Зі9(2016) – за допомогою параметру ρ.

Результати порівняння ефективності розроблених САА з сучасними аналогами представлені у таблиці 2 – для ЦВ за умови заповнення усіх кадрів ЦВ, таблиці 3 – для ЦЗ за умови часткового заповнення кадрів ЦВ, таблиці 4 – для порівняння точності виявлення AD ЦЗ, рис. 2 – для порівняння інтегральних параметрів ρ ЦЗ.

Таблиця 2 –

Порівняння AD для розроблених САА, направлених на детектування ЦВ, з сучасними аналогами

ППС, біт/піксель	V1 2005 (10)	V2 2005 (10)	V3 2007 (10)	V4 2013 (9)	V5 2015 (26)	САА1 (367)	САА2 (367)	САА3v (367)
0.5	0.925	0.955	0.98	1	0.9991	0.9991	**1**	**1**
0.4	0.885	0.94	0.97	-	-	0.9991	**1**	**1**
0.3	0.825	0.92	0.945	-	-	0.9991	**1**	**1**
0.25	-	-	-	0.996	0.9988	0.9991	**1**	**1**
0.2	0.68	0.875	0.925	-	-	0.9691	**1**	**1**
0.167	-	-	-	-	-	0.9537	**1**	**1**
0.125	-	-	-	0.928	-	0.7757	0.7530	**0.9991**
0.1	0.555	0.755	0.89	-	0.9744	0.7139	0.6703	**0.9973**
0.0625	-	-	-	0.794	-	0.5157	0.5	**0.9433**
0.05	-	-	-	-	-	0.5074	0.5	**0.9391**

Таблиця 3 –

Порівняння AD для розробленого САА3 та сучасного аналога за умови часткового заповнення кадрів ЦВ

ППС окремих кадрів ЦВ, біт/піксель	Кількість заповнених кадрів							
	80%		60%		40%		20%	
	V5 2015	САА3	V5 2015	САА3	V5 2015	САА3	V5 2015	САА3
0.5	1	1	0.9978	**1**	1	1	0.9932	**1**
0.25	1	1	1	1	0.9926	**1**	0.9843	**0.9999**
0.167	-	0.9998	-	0.9998	-	0.9998	-	0.9999
0.125	-	0.9959	-	0.9948	-	0.9948	-	0.9991
0.1	0.9381	**0.9897**	0.9276	**0.9867**	0.7974	**0.9867**	0.6688	**0.9974**
0.05	-	0.9232	-	0.9048	-	0.9048	-	0.9811

Таблиця 4 – Порівняння *AD* для розробленого САА3, направленого на детектування ЦЗ, з сучасними аналогами

ППС, біт/піксель	31 2008	32 2008	33 2009	34 2010	35 2015	36 2015	САА3
0.5	0.9975	-	-	-	-	-	**1**
0.4	0.995	-	-	-	-	-	**1**
0.3	0.982	-	-	-	-	-	**1**
0.25	-	-	-	-	-	-	**1**
0.2	0.98	0.9985	0.9993	0.9992	0.9999	-	**1**
0.167	-	-	-	-	-	-	**0.9995**
0.125	-	-	-	-	-	-	**1**
0.1	0.922	0.9943	0.9937	0.9924	**0.9971**	0.95	0.9968
0.05	-	0.9283	0.9319	0.9404	0.9770	0.93	**0.9865**

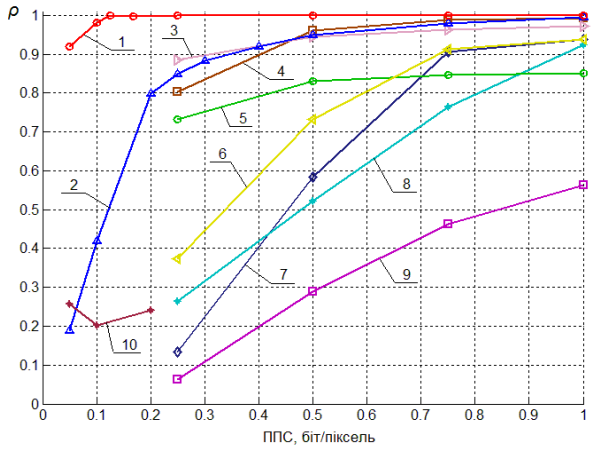


Рисунок 2 – Результати порівняння інтегрального параметру ρ алгоритму САА3 з сучасними аналогами: 1 – САА3, 2 – Зі8, 3 – Зі7, 4 – Зі2, 5 – Зі5, 6 – Зі6, 7 – Зі1, 8 – Зі4, 9 – Зі3, 10 – Зі9

Наведені результати говорять про високу абсолютну ефективність алгоритмів, що реалізують розроблені методи, а також про підвищення ефективності стеганоаналізу в порівнянні з існуючими аналогами. Алгоритми САА1 та САА2, направлені на виявлення наявності ДІ у ЦВ (табл. 2), по ефективності максимально перевищують сучасні аналоги при ППС, більшій за 0.125 біт/піксель, крім того для САА2 і САА3v досягнуто абсолютний результат для ППС 0.167-0.5 біт/піксель. Алгоритм САА2 є ефективним при виявленні СП у ЦВ з малим розміром кадрів: при ППС 0.167-0.5 біт/піксель помилки першого роду відсутні, при ППС вони складають 6.12%, помилки другого роду складають 5.1% (табл. 1), дані сучасних аналогів для порівняння ефективності детектування ЦВ з малим розміром кадрів відсутні. У випадку малих значень ППС найефективнішим є САА3v (табл. 2) – результати детектування перевищують кращий аналог на 2.3% для ППС 0.1 біт/піксель. Найбільше підвищення ефективності стеганоаналізу досягається при виявленні ДІ, вбудованої з ППС, меншої за 0.1 біт/піксель – точність детектування САА3v для ППС 0.0625 біт/піксель на 14.93% перевищує сучасний аналог, у випадку ППС 0.05 біт/піксель для сучасних аналогів відсутні дані для порівняння ефективності. В умовах заповнення лише частини кадрів ЦВ (табл. 3) для ППС 0.1 біт/піксель результати детектування за допомогою САА3 окремих кадрів ЦВ на 5.5% перевищують аналог при степені заповнення кадрів 60-80% та на 32/18% при степені заповнення кадрів 20-40% відповідно. Алгоритм САА3, направлений на аналіз ЦЗ, перевищує сучасні аналоги, найбільш показовим є порівняння САА3 з Зі8 та Зі9 (рис. 2), які аналізували ЦЗ з малою ППС, значення інтегрального параметру ρ перевищує указані аналоги у 5/3.7 разів відповідно при ППС 0.05 біт/піксель, у 2.3/4.8 разів відповідно при ППС 0.1 біт/піксель. Порівнюючи точність детектування *AD* для ЦЗ алгоритмом САА3 (табл. 4), досягнуто абсолютний результат виявлення СП, сформованих вбудовою ДІ з ППС не нижче 0.2 біт/піксель, при ППС 0.1 біт/піксель результати детектування є зіставними, при ППС 0.05 біт/піксель САА3 перевищує кращий аналог на 1%.

Оскільки при стеганоаналізі невідомо, скільки колірних складових ЦК було заповнено в результаті стеганоперетворення, рекомендується проводити двохетапну перевірку наявності ДІ у ЦК, у відповідності з якою в роботі розроблені рекомендації щодо засто-

сування розроблених методів, з урахуванням яких розроблено комплексний метод для виявлення ДІ у ЦВ/послідовності ЦЗ:

Крок 1. Визначення кількості кадрів, розміру кадрів ЦВ (M, N), обчислення загальної кількості 4×4-блоків в кадрі $cb = \lfloor M/4 \rfloor \cdot \lfloor N/4 \rfloor$.

Крок 2. (*Детектування ЦВ з малим розміром кадрів*)

Якщо $cb < T_{cb}$, $T_{cb} = 4800$, *то* CAM2, перехід на крок 6, *інакше* крок 3.

Крок 3. (*Детектування ЦВ в градаціях сірого*).

Якщо ЦВ має лише одну колірну складову, *то*:

3.1. Визначення формату оригінального контейнеру за допомогою МВФКБ.

3.2. Вибір порогових значень T_R, T_G, T_B в залежності від визначеного формату контейнера;

3.3. Стеганоаналіз ЦВ за допомогою методів CAM1 та CAM2.

3.4. Прийняття рішення щодо наявності/відсутності ДІ у ЦВ (за умови протилежних результатів детектування перевага надається методу, найефективнішому для ймовірного джерела ЦВ – для ЦВ, отриманих камерами мобільних пристроїв перевага надається методу CAM1), перехід на крок 6.

Інакше крок 4.

Крок 4. (*Детектування кольорових ЦВ*).

4.1. Визначення формату оригінального контейнеру за допомогою МВФКА.

4.2. Вибір порогових значень T_R, T_G, T_B в залежності від визначеного формату контейнера;

4.3. Стеганоаналіз ЦВ за допомогою методу CAM1.

4.4. *Якщо* ДІ виявлена у двох або трьох колірних складових ЦВ або визначений у кроці 4.1 формат контейнера без втрат, *то* додаткова перевірка здійснюється методом CAM2, *інакше* додаткова перевірка здійснюється методом CAM3v.

4.5. Прийняття рішення щодо наявності/відсутності ДІ у ЦВ (за умови порівняння результатів CAM1 та CAM3v перевага надається останньому; при порівнянні результатів CAM1 і CAM2 перевага надається методу, найефективнішому для ймовірного джерела ЦВ), перехід на крок 6.

Крок 5 (необов'язковий). (*Покадровий аналіз ЦВ*).

Якщо в п. 4.1 виявлено формат з втратами та в п. 4.3 ДІ виявлена в одній колірній складовій або не виявлена, *то* для кожного кадру ЦВ здійснюється аналіз за допомогою методу CAM3.

Крок 6. Виведення кінцевого результату.

Оцінки ефективності комплексного методу виявлення наявності ДІ в ЦВ співпадають для конкретних випадків з отриманими вище оцінками для його складових.

ВИСНОВКИ

В роботі вирішена важлива науково-практична задача, що полягає у підвищенні ефективності стеганоаналізу для ЦЗ і ЦВ шляхом розробки методів, що детектують в них вкладення конфіденційної інформації LSB-методом, ефективних, у тому числі, при малих (не більше 0.25 біт/піксель) значеннях ППС.

У роботі одержані наступні результати:

1. *Отримав подальший розвиток* загальний підхід до аналізу стану і технології функціонування інформаційних систем шляхом встановлення відповідності між властивостями параметрів $n \times n$ – блоку ЦЗ у просторовій області і області сингулярного розкладання відповідної матриці. Доведено, що необхідною і достатньою умовою належності єдиного ненульового сингулярного числа блоку множині натураль-

них чисел та його кратності n є співпадіння значень яскравості пікселів, що належать блоку. Показано, що виявлена властивість є чутливою до будь-яких збурних дій, а тому використовується як основа теоретичного базису розроблених стеганоаналітичних методів CAM1 і CAM2 для аналізу ЦВ, який проводиться у просторовій області контенту, що забезпечує їх високу ефективність, у тому числі в умовах ППС, меншій за 0.25 біт/піксель.

2. *Вперше* на основі аналізу змін кількості блоків з однаковими значеннями яскравості в матрицях ЦК в результаті стеганоперетворення LSB-методом послідовності ЦЗ/кадрів ЦВ розроблені стеганоаналітичні методи CAM1 і CAM2, ефективні, у тому числі, для малої ППС, кадрів малого розміру, незалежно від пристрою, за допомогою якого отримане ЦВ, його формату зберігання (з/без втрат) та кількості колірних складових, що були задіяні при стеганоперетворенні. Метод CAM1 дозволив підвищити ефективність стеганоаналізу для ЦВ, отриманих камерами мобільних пристроїв в умовах ППС 0.125 біт/піксель на 1.2%. При стеганоаналізі з використанням CAM2 ЦВ з малим розміром кадрів в умовах ППС 0.167-0.5 біт/піксель помилки першого роду відсутні, при ППС 0.125 біт/піксель вони складають 6.12%; помилки другого роду – 5.1%. Методом CAM2 досягнутий абсолютний результат детектування наявності ДІ у ЦВ з середнім і великим розміром кадрів – AD=1 при ППС 0.167-0.5 біт/піксель, що не досягалось аналогами та дозволило підвищити ефективність стеганоаналізу ЦВ максимально на 7.5% (при ППС 0.2 біт/піксель).

3. *Вперше* на основі аналізу кількості послідовних тріад колірних триплетів у матриці унікальних кольорів ЦЗ/кадрів ЦВ в результаті вбудови ДІ методом LSB в одну довільну колірну складову ЦК, які початково зберігалися в форматах з втратами, розроблено метод CAM3, ефективний, в тому числі, для малої ППС, ефективність якого перевищує сучасні аналоги: для ППС 0.05/0.1 біт/піксель точність детектування підвищена на 4.5/2.19% відповідно, інтегральний параметр у 3.7/2.3 рази відповідно. Метод CAM3v, що є результатом адаптації CAM3 для ЦВ, дозволив підвищити ефективність стеганоаналізу для малих значень ППС максимально на 14.93% (ППС 0.0625 біт/піксель), та забезпечив високу ефективність стеганоаналізу ЦВ ($AD = 0.9391$) в умовах, де сучасні аналоги є недієздатними (ППС 0.05 біт/піксель).

4. *Вперше* на основі отриманих практичних рекомендацій застосування розроблених стеганоаналітичних методів, які забезпечують вибір конкретного методу в залежності від характеристик ЦВ, що аналізується, і ефективного удосконалення стеганоаналітичного методу CAM3 з метою використання його для визначення формату (з/без втрат) оригінального контейнеру, для якого помилки першого роду склали 3%, другого роду – 4.5%, розроблено комплексний метод виявлення вкладень ДІ в ЦВ, ефективний, у тому числі при малих значеннях ППС, при різній кількості заповнених колірних складових контейнерів, в якості яких можуть виступати як кольорові ЦВ, так і відео в градаціях сірого, незалежно від формату (з/без втрат), різній степені заповненості кадрів цифрового відео.

5. Алгоритмічні реалізації всіх розроблених методів мають поліноміальну обчислювальну складність: для CAA1 і CAA2 обчислювальна складність визначається як $P \cdot \underline{O}\left(M^2\right)$, де $M \times M$ – розмір матриці ЦЗ/кадру ЦВ, P – кількість зображень/кадрів у послідовності ЦЗ/ЦВ; для алгоритмічних реалізацій методів CAM3, МВФКА – $\underline{O}\left(M^4\right)$; для алгоритму CAA3v – $P \cdot \underline{O}\left(M^4\right)$, що дає можливість для їх практичного використання для стеганоаналізу ЦЗ/ЦВ будь-якого, у тому числі значного, розміру.

СПИСОК РОБІТ АВТОРА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ахмаметьева, А.В. Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров / А.В. Ахмаметьева // Інформатика та математичні методи в моделюванні. – 2015. – Т.5. – № 4. – С. 367-375. (Ulrich, EBSCO, РИНЦ, Index Copernicus)
2. Ахмаметьева, А.В. Стеганоанализ цифровых изображений, хранящихся в формате с потерями / А.В. Ахмаметьева // Захист інформації. – 2016. – Випуск 23. – С. 135-145. (Ulrich, РИНЦ)
3. Ахмаметьєва, Г.В. Стеганоаналітичний алгоритм для цифрових контейнерів, збережених в форматах з втратами / Г.В. Ахмаметьєва // Сучасна спеціальна техніка. – 2016. – № 3. – С. 31-38. (Google Scholar)
4. Method of detection the fact of compression in digital images as an integral part of steganalysis / A. Akhmametieva // Інформатика та математичні методи в моделюванні. – 2016. – Т.6. – №4. – С. 357-364. (Ulrich, EBSCO, РИНЦ, Index Copernicus)
5. Кобозева, А.А. Стеганоаналитеческий метод для цифровых контейнеров, хранящихся в формате без потерь / А.А. Кобозева, А.В. Ахмаметьева, А.А. Ефименко // Інформаційна безпека. – 2014. – №1(13). – С. 31-42.
6. Маєвський, Д.А. Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів / Д.А. Маєвський, Г.В. Ахмаметьєва // Інформатика та математичні методи в моделюванні. – 2016. – Т.6. – №1. – С. 52-60. (Ulrich, EBSCO, РИНЦ, Index Copernicus)
7. Ахмаметьева, А.В. Выявление области применения стеганоаналитического подхода, основанного на анализе пространственной области цифровых контентов / А.В. Ахмаметьева // Problemele energeticii regionale [Проблемы региональной энергетики]. Электронный журнал Академии наук Республики Молдова. – 2016. – № 2 (31). – С.104-111. (Google Scholar)
8. Ахмаметьева, А.В. Стеганоаналитический метод, основанный на анализе пространственной области цифровых контентов / А.В. Ахмаметьева // Международная научно-техническая конференция «Современные информационно-телекоммуникационные технологии», Киев, 17-20 ноября 2015 г. – Т. II. – С. 83-84.
9. Ахмаметьєва, Г.В. Детектування стеганоповідомлень, вбудованих методом LSB Matching у цифрові контейнери в форматах з втратами / Г.В. Ахмаметьєва // V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», Львів, 2-3 червня 2016 р. – С. 106-107.
10. Ахмаметьєва, Г.В. Виявлення області застосування стеганоаналітичного алгоритму, що аналізує просторову область цифрових зображень / Г.В. Ахмаметьєва // V Міжнародна науково-технічна конференція «Інформаційні системи та технології» (ІСТ-2016), Харків-Коблево, 12-17 вересня 2016 р. – С. 287-288.
11. Ахмаметьева, А.В. Стеганоанализ цифровых видео, основанный на анализе пространственной области / А.В. Ахмаметьева // V Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології» (ІУСТ-Одеса - 2016), Одеса, 20-22 вересня 2016 р. – С. 161-163.

АНОТАЦІЯ

Ахмаметьєва Г.В. Підвищення ефективності стеганоаналізу для цифрових зображень та відео. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації – Одеський національний політехнічний університет, Одеса, 2017.

В роботі вирішено важливу науково-технічну задачу, що полягає в підвищенні ефективності стеганоаналізу цифрових зображень та цифрових відео шляхом розробки ефективних стеганоаналітичних методів виявлення наявності додаткової інформації, вбудованої методом LSB у цифрові зображення та відео, у тому числі при малих значеннях пропускної спроможності прихованого каналу зв'язку (ППС).

Стеганоаналіз цифрових контентів реалізований без наявності оригінального контейнеру у просторовій області контентів, що дозволило уникнути додаткового накопичення обчислювальної похибки. Досягнуто високу ефективність виявлення стеганоповідомлень, сформованих вбудовою додаткової інформації в одну довільну колірну складову цифрових зображень (при ППС 0.05 біт/піксель помилки I роду максимально склали 7.96% при відсутності помилок II роду). Для цифрових відео досягнуто абсолютний результат детектування при ППС не нижче 0.167 біт/піксель, у тому числі при малих розмірах кадрів.

Ключові слова: стеганоаналітичний метод, цифрове зображення, цифрове відео, просторова область контентів, метод модифікації найменшого значущого біту

АННОТАЦИЯ

Ахмаметьева А.В. Повышение эффективности стеганоанализа для цифровых изображений и видео. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации – Одесский национальный политехнический университет, Одесса, 2017.

В работе решена важная научно-техническая задача, которая заключается в повышении эффективности стеганоанализа цифровых изображений (ЦИ) и видео (ЦВ) путем разработки эффективных стеганоаналитических методов выявления вложений дополнительной информации, погруженной методом LSB в ЦИ и ЦВ, в том числе при малых значениях пропускной способности скрытого канала связи (СПС).

Объект исследования – процессы организации и обнаружения стеганографического канала связи.

Предмет исследования – стеганоаналитические методы для цифровых изображений и видео.

Для организации стеганоанализа обоснован выбор пространственной области цифровых контентов благодаря возможности избежать накопления вычислительной погрешности, что в значительной степени влияет на эффективность стеганоанализа при условии малых значений СПС.

Получил дальнейшее развитие общий подход к анализу состояния и технологии функционирования информационных систем путем получения критерия принадлежности ненулевого сингулярного числа матрицы единичного ранга множеству натуральных чисел, что позволило установить соответствие между пространственной областью и областью преобразования цифровых контентов.

На основе полученного критерия разработан теоретический базис и на его основе разработаны стеганоаналитические методы выявления вложений дополнительной информации в цифровых видео, основанные на учете различий в количестве блоков с одинаковыми значениями яркости в результате первичного и вторичного погружений дополнительной информации. Для цифровых видео достигнут абсолютный результат детектирования при СПС не ниже 0.167 бит/пиксель, что позволило повысить эффективность стеганоанализа максимально на 7.5%. Разработанный метод, основанный на учете характера изменения количества блоков с одинаковыми значениями яркости, обеспечивает высокую эффективность выявления вложений дополнительной информации, по-

груженной в цифровые видео с малым размером кадров: при СПС 0.167-0.5 бит/пиксель ошибки I рода отсутствуют, при СПС 0.125 бит/пиксель ошибки I рода составляют 6.12% при ошибках II рода 5.1%.

На основе анализа последовательных триад цветовых триплетов в матрице уникальных цветов цифровых изображений разработан метод выявления дополнительной информации, погруженной в одну произвольную цветовую составляющую цифровых изображений (отдельных кадров цифровых видео), что позволило с высокой эффективностью выявлять стеганосообщения, сформированные при малой СПС: при СПС 0.05 бит/пиксель ошибки I рода максимально составили 7.96% при отсутствии ошибок II рода. Разработанный метод адаптирован для выявления вложений дополнительной информации в цифровых видео, что позволило повысить эффективность стеганоанализа максимально на 14.93% (при СПС 0.0625 бит/пиксель).

Исходя из различий в количестве последовательных триад триплетов в матрице уникальных цветов цифровых изображений в форматах с/без потерь, разработан метод выявления формата оригинального контейнера, используемый как составная часть стеганоанализа, что, с учетом полученных оценок эффективности разработанных стеганоаналитических методов, позволило увеличить эффективность видеостеганоанализа путем разработки комплексного метода выявления стеганосообщений, сформированных при различных условиях погружения дополнительной информации (СПС, количество цветовых составляющих), а также использовании в качестве контейнеров цветных и полутоновых цифровых видео в формате с/без потерь.

Разработанные стеганоаналитические алгоритмы, основанные на учете изменений в количестве блоков с одинаковыми значениями яркости, являются полиномиальными степени 2, алгоритмы, основанные на анализе последовательных триад триплетов в матрице уникальных цветов ЦК, являются полиномиальными степени 4.

Ключевые слова: стеганоаналитический метод, цифровое изображение, цифровое видео, пространственная область контентов, метод модификации наименьшего значащего бита, LSB

ABSTRACT

Akhmametieva A. Improving the efficiency of steganalysis for digital images and video. – Manuscript.

Thesis for a candidate's degree by specialty 05.13.21 – Information security system – Odessa National Polytechnic University, Odessa, Ukraine, 2017.

The paper is devoted the development of complex steganalytic method, aimed to detect the fact of presence of additional information, embedded by LSB method in digital images and video with different values of hidden capacity including small values. This methods led to improving the efficiency of steganalysis.

Steganalysis of digital contents is realized without presence of original container in spatial domain of content, that allows avoid additional accumulation of a computing error. It was reached high efficiency of detection stego, formed by embedding of additional information into one random color component of digital images, by analyzing of sequential triads of triplets in the matrix of unique colors. To provide steganalysis of digital video it was developed methods, based on the accounting of differences in the change of the number of blocks with the equal color brightness values of matrices of frames of a video sequence as a result of primary and repeated embedding of additional information. It was developed the method of detection the fact of compression in color digital images, which can be used as an integral part of steganalysis.

Key words: steganalytic method, digital image, digital video, spatial domain of contents, least significant bit method, LSB