**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"**

**ШИРОЧИН СЕМЕН СТАНІСЛАВОВИЧ**

**УДК 004.62 : 004.056.5: 621.391.7**

# МЕТОДИ КОМБІНОВАНОГО СТЕГАНОГРАФІЧНОГО ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ В ХМАРНИХ СХОВИЩАХ

Спеціальність 05.13.05 – комп'ютерні системи та компоненти

**АВТОРЕФЕРАТ**
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2015

Дисертацією є рукопис

Робота виконана на кафедрі програмного забезпечення комп'ютерних систем Національного технічного університету України "КПІ", Міністерства освіти і науки України

**Науковий керівник:** кандидат технічних наук, доцент
**Сулема Євгенія Станіславівна**
Національний технічний університет України
"Київський політехнічний інститут" МОН України,
доцент кафедри програмного забезпечення
комп'ютерних систем

**Офіційні опоненти:** доктор технічних наук, старший науковий співробітник
**Алішов Надір Ісмаіл-Огли**
Інститут кібернетики ім. В.М. Глушкова Національної академії наук України, провідний науковий співробітник,

доктор технічних наук, старший науковий співробітник
**Ланде Дмитро Володимирович**
Інститут проблем реєстрації інформації Національної академії наук України, завідувач відділом

Захист відбудеться 9 червня 2015 р. о 14:30 на засіданні спеціалізованої ради Д 26.002.02 у Національному Технічному Університеті України "Київський Політехнічний Інститут" (м. Київ, пр. Перемоги, 37, корп. 18, ауд. 516.)

Відгуки на автореферат у двох екземплярах, завірені печаткою установи, просимо надсилати на адресу: 03056, м. Київ, пр. Перемоги, 37, вченому секретарю Національного Технічного Університету України "Київський Політехнічний Інститут".

З дисертацією можна ознайомитись в бібліотеці Національного технічного університету України "Київський політехнічний інститут", м. Київ, пр. Перемоги, 37.

Автореферат розісланий "__"_____ 2015 р.

Вчений секретар
спеціалізованої ради, кандидат
технічних наук, доцент М.М. Орлова

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми.** Розширення сфери застосування хмарних технологій, в тому числі для задач, пов'язаних з реєстрацією, обробкою, передачею та збереженням мультимедійних даних, вимагає забезпечення захисту даних при їх передаванні через комп'ютерні мережі, віддаленій обробці та збережені у хмарних сховищах. Крім того, останнім часом спостерігається тенденція збільшення популярності хмарних сервісів, які надають широкому колу користувачів можливість зберігати віддалено особисті дані. Прикладами таких сервісів є Google Docs, Dropbox, ICloud, Яндекс.Диск. Фактично ця тенденція призводить до того, що переважна більшість фізичних та юридичних осіб мають певну долю власних даних, що зберігаються в хмарних сховищах.

Як показано в багатьох роботах, для захисту великих об'ємів даних в мобільних комп'ютерних системах з невизначеними чи обмеженими ресурсами іноді достатнім є сам факт непомітності передачі даних, що може бути досягнутий методами та засобами стеганографії, які за продуктивністю не поступаються методам та засобам легковагової (Light Weight) криптографії (LW-крипографії).

Комп'ютерна стеганографія також застосовується *для захисту авторського права, цілісності карт, знімків, конфіденційності текстів та зображень на медичних чи комерційних документах*.

Комп'ютерна стеганографія, як галузь науки, сформувалась лише на початку дев'яностих років, і за останні двадцять років стеганографія та стеганографічний аналіз відокремилися як самостійний напрямок з відомими науковими школами, наприклад, Державного університету штату Нью-Йорк (State University of New York), Дрезденського технічного університету (Dresden University of Technology), Бізнес-університету Гуандонга (Guangdong University of Business Studies), Оксфордського університету та інших. Такі наукові школи насамперед сформовані на базі відповідних кафедр комп'ютерних наук та інженерії. Серед відомих фахівців цих шкіл є Джессика Фридрих, Андреас Вестфельд, Рейнер Боме, Елке Франц, Юн Чжань, Ендрю Кер, Інгемар Кокс та інші. Дослідження в галузі стеганографії також проводяться східно-європейськими, в тому числі українськими, науковими школами. Зокрема, відомі роботи таких авторів, як: Олександр Балакін, Надір Алішов, Станіслав Кувшинов, Ян Кодовски, Валерій Задірака, Кирил Пономарьов, Олександр Алієв, Альберт Лейман та інші.

У зв'язку з розповсюдженням стеганографічного захисту та масовим використанням мультимедійної інформації актуальною стає науково-технічна задача захисту мультимедійних стегоданих додатковими методами та засобами, в тому числі – в комбінації з окремими функціями та компонентами LW-криптографії.

Значні витрати часу на криптографічні перетворення при масовому використанні мультимедійних даних значно впливають на продуктивність Cloud систем чи інших комп'ютерних систем з невизначеними чи обмеженими ресурсами.

Тема дисертаційної роботи, що присвячена розробленню швидких методів комбінованого стеганографічного захисту мультимедійних даних на основі принципів LSB (Least Significant Bit) стеганографії та LW-шифрування стегоданих блочними та потоковими ключами, ***є актуальною*** для створення та розвитку сучасних хмарних комп'ютерних систем та інтерактивних інформаційних технологій.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертаційне дослідження виконувалось на кафедрі програмного забезпечення комп'ютерних систем НТУУ "КПІ" в рамках науково-дослідної роботи "Методи та засоби обробки, захисту та пошуку мультимедійних даних у комп'ютерних системах та мережах" (реєстраційний номер 0114U003948).

**Мета і задачі дослідження.** Метою роботи є підвищення ефективності програмних сервісів захисту мультимедійних даних в розподілених комп'ютерних системах за рахунок розробки комбінованих крипто-стеганографічних методів захисту даних та застосування паралельних обчислень, що забезпечують надійність захисту та зручність доступу до конфіденційних даних, а також підвищення швидкодії при стрімко зростаючій кількості користувачів хмарних середовищ.

Відповідно до поставленої мети *основними задачами дослідження є*:

1. Аналіз надлишковості мультимедійних даних для створення швидких комбінованих методів та відповідних програмних сервісів захисту, орієнтованих на масову обробку, маскування та демаскування даних в процесах прозорої оперативної взаємодії в хмарних середовищах.
2. Розроблення нових комбінованих крипто-стеганографічних методів захисту мультимедійних даних, які враховують особливості мультимедійних даних і відрізняються вбудовуванням стегоданих з використанням мультимедійних даних контейнера в ролі ключа чи складених ключів з метою підвищення стійкості та скорочення часу вбудовування зображення в графічний контейнер, аудіо-даних в графічний контейнер та аудіо-даних в аудіо-контейнер.
3. Аналіз необхідних та достатніх умов використання графічних чи аудіо контейнерів для реалізації комбінованих стеганографічних методів захисту мультимедійних стегоданих та можливостей підвищення швидкодії програмних сервісів захисту стегоданих за рахунок використання паралельних обчислень.
4. Розробка експериментального зразка стегосистеми для реалізації та дослідження, як вищевказаних комбінованих стеганографічних методів, так і базових методів LSB-стеганографії та LSB-стеганографії з використанням шифрування AES, а також дослідження відповідних паралельних реалізацій програмних сервісів.

*Об'єкт дослідження:* процеси приховування конфіденційної інформації в стеганографічних контейнерах (зображеннях чи аудіо-файлах), які зберігаються в хмарних сховищах, а також процеси зчитування прихованої в мультимедійних контейнерах інформації.

*Предмет дослідження:* комбіновані методи захисту мультимедійних даних в хмарних сховищах із застосуванням LSB-стеганографії, криптографії та паралельної обробки даних, а також оцінки стійкості та швидкодії стеганографічних методів, заснованих на надлишковості, критерії повноти наявних характеристик зв'язаних множин контейнерів.

**Методи дослідження:** методи теорії інформаційної безпеки, теорії організації обчислювальних процесів, теорії інформації та кодування, теорії ймовірностей і математичної статистики.

**Наукова новизна одержаних результатів** полягає в теоретичному обґрунтуванні комплексного підходу до створення комбінованих стеганографічних та криптографічних

методів захисту мультимедійних даних з використанням оцінок швидкодії та стійкості до атак як критеріїв ефективності крипто-стеганографічного маскування мультимедійних даних в хмарних сховищах, зокрема:

1. Вдосконалено метод LSB-стеганографії з фрагментацією стегоданих за рахунок рандомізованої фрагментації та використання розділеного симетричного ключа змінної довжини, які забезпечують підвищення швидкодії та рівня стійкості приховування мультимедійних стегоданих у віддалених хмарних сховищах.
2. Вперше розроблено комбінований метод LSB-стеганографії на основі комплементарного образу, який відрізняється використанням частини даних контейнера в ролі відкритого ключа довільної довжини, а також секретного ключа, утвореного з латинського квадрату розміром 256x256, що дозволяє *підвищити швидкодію* за рахунок меншої кількості маскуючих перетворень – підстановок та перестановок у контейнері та *підвищити рівень захисту* великих об'ємів мультимедійних даних за рахунок значного збільшення довжини ключа.
3. Вперше розроблено комбінований метод стеганографічного захисту на основі шифрування палітри, який ґрунтується на заміні значень кольорів пікселів (або переходів між ними) зображення, що приховується, координатами відповідних пікселів або переходів кольорів у зображенні-ключі, що дозволяє забезпечити захист графічних даних шляхом кодування їх довільним відкритим зображенням-ключем або складеними ключами – групою зображень, які відповідають критерію повноти наявних байт або переходів.
4. Вперше теоретично обґрунтовані критерії повноти наявних байт контейнеру та повноти наявних переходів у зображені-ключі як необхідних та достатніх умов ефективного маскування комбінованим методом стеганографії на основі шифрування палітри.

**Практичне значення одержаних результатів** полягає в створені теоретичних засад для розроблення нових та удосконалення вже існуючих сервісів захисту інформації в хмарних сховищах на основі комбінованих стеганографічних методів захисту конфіденційної мультимедійної інформації.

Серед практично значущих результатів слід визначити:

1) Організацію рандомізованої фрагментації стегоданих для захисту мультимедійних даних в графічних зображеннях та аудіо-файлах;
2) Формування рандомізованого ключа на основі латинського квадрату для шифрування даних в методі комплементарного образу;
3) Формування словника палітри для шифрування даних палітрою зображення-ключа або аудіо-файла-ключа;
4) Паралельну реалізацію обробки даних методів захисту мультимедійних даних.

Матеріали дисертації використовуються у міжнародному проекті «ParIS – Partnership in Information Security» (реєстраційний номер 2014-1-LU01-KA204-000034) програми Erasmus+, що виконується Університетом Люксембургу, Національним технічним університетом України «КПІ», Університетом Лісабону та Варшавським технологічним університетом.

Матеріали дисертації впроваджені на кафедрі програмного забезпечення комп'ютерних систем НТУУ «КПІ» для розроблення нових навчальних модулів.

**Особистий внесок здобувача.** Основні результати отримані автором самостійно. В роботі [1] автором виконано адаптацію метода стеганографії на основі комплементарного образу для аудіо-файлів; в роботі [2] автором реалізовано криптографічний метод захисту зображень з використанням довільного зображення в ролі ключа; в роботі [3] автором розроблено метод стеганографії з захистом стегоданих шляхом їх комплементарного перетворення; в роботі [4] автором розроблено алгоритм фрагментації стегоданих; в роботі [5] автором виконано біт-орієнтовану оцінку складності ряду криптографічних алгоритмів; в роботі [6] автором запропоновано довірений сервіс захисту мультимедійних даних користувача в хмарних сховищах; в роботі [7] автором проаналізовано часові показники послідовних та паралельних реалізацій стеганографічних алгоритмів; в роботі [8] автором виконано огляд існуючих засобів захисту мультимедійних даних; в роботі [9] автором запропоновано критерії стегопридатності для контейнеро-орієнтованої стегосистеми; в роботі [10] автором запропоновано алгоритм фрагментації стегоданих; в роботі [11] автором проаналізовано можливості подання захищених неграфічних даних в картографічних графічних даних в роботі [12] автором запропоновано критерії оцінки алгоритму фрагментації стегоданих в контейнері.

**Апробація результатів дисертації**. Основні результати дисертаційного дослідження доповідалися на міжнародних і національних наукових та науково-практичних конференціях:

1. 3rd IEEE Conference on Cloud Networking (CloudNet 2014), Luxemburg, 2014.
2. VIII Міжнародна науково-практична конференція «Актуальні проблеми комп'ютерних технологій (АПКТ-2014)», Хмельницький, 2014.
3. II Международная научно-практическая конференция «Информационные технологии. Проблемы и решения», Уфа, 2014.
4. VI Міжнародна науково-технічна конференція «Актуальні проблеми комп'ютерних технологій (АПКТ-2012)», Хмельницький, 2012.
5. IV Наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг (ПМК-2012)», Київ, 2012.
6. XIII Міжнародна конференція «Системний аналіз та інформаційні технології (САІТ-2011)», Київ, 2011.
7. V Міжнародна науково-практична конференція «Актуальні проблеми комп'ютерних технологій (АПКТ-2011)», Хмельницький, 2011.

**Публікації.** Основні результати дисертаційної роботи опубліковані в 12 наукових працях, серед яких 5 наукових статей у науково-технічних фахових виданнях, з них 2 статті опубліковано у журналах, що реферуються такими науко-метричними базами, як Directory of Open Access Journals (DOAJ), Російський індекс наукового цитування (РІНЦ), Google Scholar, «Наукова періодика України», UlrichsWeb Global Serials Directory; 7 публікацій в збірниках тез доповідей міжнародних та національних наукових та науково-практичних конференцій.

**Структура роботи**. Дисертаційна робота складається з вступу, чотирьох розділів, висновків, 4 додатків і списку літератури з 121 найменування. Загальний обсяг роботи становить 135 сторінок машинописного тексту, 39 рисунків, 10 таблиць.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

**У вступі** наведено загальну характеристику роботи, обґрунтовано актуальність теми, окреслено її джерельну базу, сформовано мету. Визначено основні задачі досліджень, наукову новизну та практичне значення основних результатів, наведено відомості про їхню апробацію та реалізацію.

**У першому розділі** розглянуто сучасний стан проблеми криптографічного та стеганографічного захисту конфіденційних мультимедійних даних, які зберігаються в хмарних сховищах і масово використовуються для вирішення оперативних задач дистанційного медичного діагностування, правоохоронної та митної служб, картографічних і аерокосмічних досліджень тощо.

Існують два основні варіанти реалізації стеганографічного захисту: у першому випадку спеціальна інформація розміщується у заголовках файлів різних форматів чи в текстових повідомленнях: вбудовування ідентифікаційних номерів (*fingerprinting*); вбудовування заголовків (*captioning*); вбудовування цифрових водяних знаків (*watermarking*), у другому випадку дані вбудовуються в цифрові дані, які мають аналогову природу – мова, зображення, аудіо та відео (мультимедійні дані). Другий варіант надає ширші можливості для розроблення нових ефективних методів захисту.

Сучасна *LSB*-стеганографія (*Least Significant Bits*) забезпечує приховання факту передачі даних за рахунок використання маскуючого алгоритму, який модифікує певну кількість молодших біт в кожному байті відкритих даних, додаючи до них конфіденційне повідомлення. Існує багато методів та способів стеганографії, різних за обчислювальною складністю, місткістю і орієнтованих на різні формати даних.

Концепція стеганографічного захисту забезпечує непомітність передачі вбудованих конфіденційних стегоданих при спробах з'ясувати відповідний зміст замаскованого повідомлення чи зображення. Це є важливою перевагою стеганографічного захисту порівняно з криптографічним захистом, оскільки зашифровані повідомлення автоматично перехоплюються у каналах зв'язку і зберігаються для подальшого криптоаналізу. Виявлення наявності стегоданих в зображеннях або аудіо-файлах потребує складного стегоаналізу на основі частотно-часових перетворень. Тільки у разі виникнення підозр стегодані можуть бути виявлені і стати доступними сторонньому спостерігачу. Отже, стеганографічний захист має низку переваг перед криптографічним. Тому використання саме стеганографічного підходу до захисту даних у хмарних сховищах є більш перспективним.

Хмарним сховищем даних (*cloud storage*) є сховище, в якому дані зберігаються на розподілених численних серверах, що утворюють для користувача один великий віртуальний сервер чи хмару.

Розглянуті наступні моделі організації хмарних сховищ: приватна модель, публічна модель, модель співтовариства, гібридна модель. Особливу увагу приділено хмарним сервісам загального доступу та обробки даних (DropBox, Google Docs та ін), оскільки саме тут присутні найбільші ризики даним користувача.

Мультімедійні дані (зображення та аудіо-файли) є особливим класом комп'ютерних даних, які характеризуються природною надлишковістю та великим обсягом даних. Розглянуто класифікацію мультимедійних даних в різних розрізах.

Проаналізовано різні формати зображень, такі як: JPEG, GIF, BMP, PNG. Виділено формати, які мають переваги для стеганографічного маскування даних. Розглянуто аудіо-формати RIFF, WAV, MP3, FLAC, що відрізняються якістю звуку та розмірами файлів, наявністю або відсутністю стиснення. Досліджено способи ущільнення з втратами, такі як вейвлетне та фрактальне ущільнення, а також ущільнення без втрат: RLE, LZ та код Хаффмана.

Розглянуто сучасні програмні засоби криптозахисту даних в хмарних сховищах, такі як TrueCrypt, Vormetric Cloud Encryption, CipherCloud та Cloudfogger. Було розглянуто характеристики стеганографічних систем EzStego, S-Tool, JSteg, Outguess та StegHide, та проаналізовані їх недоліки, зокрема відсутність захисту стегоданих в контейнері та відсутність підтримки різноманітних форматів.

В загальному випадку стегосистема розглядається як система захищеного зв'язку, відповідно до рис.1.

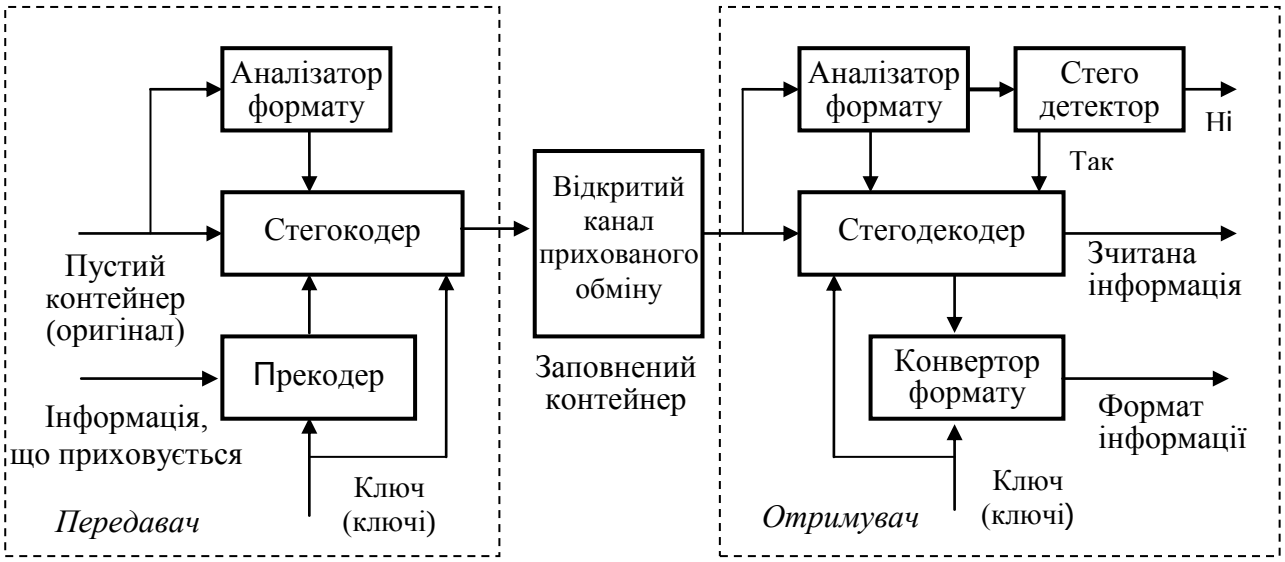


Рис. 1. Загальна структура стегосистеми, що приховує текстові дані

Порівняльний аналіз існуючих засобів стеганографії, що представлений в таблиці 1, враховує важливі для даного дослідження властивості.

Таблиця 1

Порівняння функцій існуючих стеганографічних систем

| Стегосистема: | EzStego | S-Tool | JSteg | OutGuess | StegHide |
|---|---|---|---|---|---|
| Захист від стегоаналізу | + | - | + | + | + |
| Криптозахист стегоданих | - | DES, IDEA | - | - | AES |
| Підтримувані формати | GIF | BMP, GIF | JPEG | JPEG | JPEG, BMP, WAV, AU |
| паралельні обчислення | - | - | - | - | - |

**<u>У другому розділі</u>** наведено результати розробки методів комбінованого стеганографічного захисту. Серед них – метод LSB-стеганографії з фрагментацією стегоданих та перестановкою фрагментів до їх вбудовування в контейнер.

На вході стегосистеми з фрагментацією стегоданих є порожній контейнер (рис. 2) і конфіденційне зображення (графічний або аудіо-файл). На виході – ущільнений

заповнений контейнер і розділений ключ 1,2. Захист стегоданих в контейнері відбувається при його модифікації згідно зі схемою розподілу фрагментів конфіденційного зображення або звукового повідомлення.

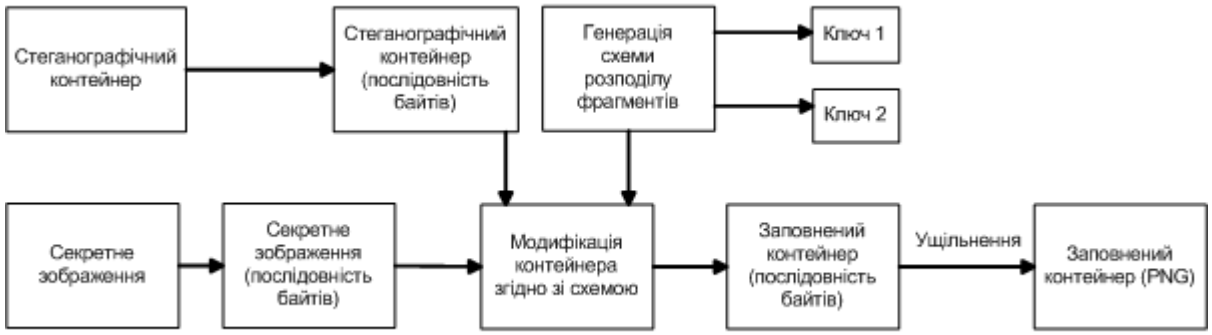


Рис. 2. Структура передавача стегосистеми з фрагментацією стегоданих

*Метод LSB-стеганографії з фрагментацією блоків* контейнера включає 5 етапів та передбачає наступні дії.

*Етап 1.* Для кожного блоку *i* генерується випадкове значення адреси

$$B_i = \gamma(C), \tag{1}$$

де $C$ – максимальне значення адреси, що дорівнює об'єму контейнера.

При цьому має виконуватись умова незайнятості даної адреси:

$$\begin{cases} B_i > B_k + S_k \\ B_i < B_j \end{cases}, \tag{2}$$

де: $B_i$ - початкова адреса $i$ -го блоку даних;

$B_j$ - початкова адреса найближчого наступного блоку;

$B_k$ - початкова адреса найближчого попереднього блоку;

$S_k$ - довжина найближчого попереднього блокую.

*Етап 2.* У випадку невідповідності умові 2, відбувається повторне обчислення значення $B_i$ за формулою 1.

Після обчислення адреси початку блоку даних обчислюється випадкове значення розміру даного блоку *i*:

$$S_i = \gamma(D), \tag{3}$$

де D – максимальне значення довжини блоку.

При цьому має виконуватись вимога можливості розмістити блок такої довжини за такою адресою:

$$B_i + S_i < B_j, \tag{4}$$

де: $B_i$ - початкова адреса $i$ -го блоку даних;

$S_i$ - довжина $i$ -го блоку даних;

$B_j$ - початкова адреса найближчого наступного блоку даних.

*Етап 3.* Об'єднавши правила 3 і 4, генерується випадкова довжина $i$ -го блоку:

$$S_i = \gamma(\min(D, B_j - B_i)) \tag{5}$$

Таким чином, випадкова довжина блоку водночас обмежена об'ємом нефрагментованих даних і початковою адресою найближчого наступного блоку.

*Етап 4.* Створення нових блоків припиняється, коли не залишається нефрагментованих даних (рис. 2). Таким чином, гарантовано як випадковий розподіл адрес і довжин, так і випадкову кількість блоків.

*Етап 5.* Формується ключ, який складається з двох векторів: вектору $\bar{a}[n]$ адрес та вектору $\bar{l}[n]$ довжин фрагментів, де *n* – кількість фрагментів.

Об'єм отриманого ключа для *n* фрагментів буде визначатись за формулою:

$$S(\bar{a}) = S(\bar{l}) = 4n \text{ байт.} \quad (6)$$

Час $T_з$ запису стегоданих визначається за формулою

$$T_з = T_{чф} + T_{чп} + T_г + T_м + T_{зф} + T_{зк}\ , \quad (7)$$

де $T_{чф}$ – час зчитування файлу контейнера;

$T_{чп}$ – час зчитування повідомлення;

$T_г$ – час генерування ключа;

$T_м$ – час модифікації контейнера;

$T_{зф}$ – час зберігання заповненого файлу контейнера;

$T_{зк}$ – час зберігання ключа (ключів).

На боці *отримувача* первинного конфіденційного повідомлення потрібен контейнер з вбудованими стегоданими, а також розділений стеганографічний ключ, що складається з вектору $\bar{a}$ початкових адрес та вектору $\bar{l}$ довжин фрагментів.

Процес відновлення на боці отримувача складається з наступних дій:

1. Зчитування векторів $\bar{a}$ та $\bar{l}$ та перевірка ідентичності їх довжин.
2. Перехід до наступного елементу вектора $\bar{a}$ та зчитування $\bar{l}$ байт.
3. Конкатенація результуючого вектору $\bar{X}$ і зчитаного фрагменту.
4. Якщо вектори $\bar{a}$ та $\bar{l}$ ще не закінчились, перехід до п. 2.
5. Збереження вектору $\bar{X}$ у вихідний файл.

Операції відновлення вихідного конфіденційного повідомлення для блоку $i$ визначаються формулою (8):

$$X[i] = C\big[a[i]\big] \cdot C[a[i]+1] \cdot \ldots \cdot C\big[a[i]+l[i]\big], \quad (8)$$

де: $l[i]$ – *i*-й елемент вектору $\bar{l}$;

$a[i]$ – *i*-й елемент вектору $\bar{a}$;

*C* – масив байтів контейнера;

" · " – конкатенація масиву байтів блоку стегоданих.

Час $T_ч$ зчитування стегоданих визначається за формулою

$$T_ч = T_{чк} + T_{чф} + T_в + T_{зп}, \quad (9)$$

де: $T_{чк}$ – час зчитування ключа;

$T_{чф}$ – час зчитування контейнера;

$T_в$ – час відновлення стегоданих;

$T_{зп}$ – час зберігання відновленого повідомлення.

*В запропонованому комбінованому методі LSB-стеганографії зображень на основі комплементарного образу* (КО) захист стегоданих забезпечується за рахунок їх попереднього маскування за допомогою комплементарного перетворення.

**Визначення 1.** Комплементарним образом стегоданих називаються зашифровані стегодані (зображення чи аудіо-файли), що утворюються за допомогою

комплементарного перетворення, яке задає відображення множини стегоданих на множину даних відкритого зображення у комплементарному каналі (потокового ключа К довільної довжини). Комплементарне перетворення задається таблицею (ключем Т), що зберігає відповідність між байтами комплементарного каналу (ключа К) та байтами стегоданих.

**Твердження 1.** Комплементарне перетворення має задовольняти вимогам:

- для будь-якої пари значень даних у комплементарному каналі та стегоданих, що знаходяться в певному діапазоні значень, має існувати одне та лише одне значення підстановки ключа Т, що знаходиться у тому ж діапазоні;
- має існувати однозначне зворотне перетворення $T^{-1}$, що дозволяє отримати стегодані з даних комплементарного образу, комплементарного каналу і ключа Т .

Цим вимогам задовольняє комплементарне перетворення, що ґрунтується на застосуванні латинського квадрату з випадковими підстановками у рядках. Структурна схема передавача даних запропонованим методом зображена на рис. 3.

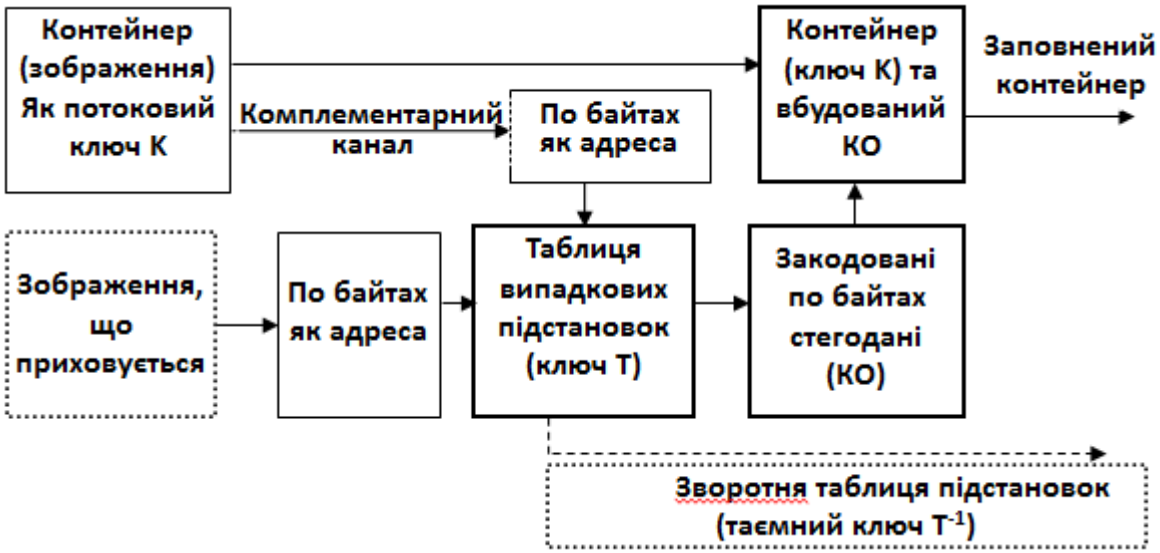


Рис. 3. Структура передавача, що реалізує метод LSB-стеганографії на основі комплементарного образу

Розмір комплементарної зони дорівнює розміру стегозображення, а розмір комплементарного образу залежить від кількості використаних стегобіт, що може бути від 1 до 8. Отже, розміщення стегоданих об'ємом $I$ в контейнері об'ємом $C$ при кількості стегобіт $b$ є можливим за виконання наступної умови:

$$C \geq 8 \cdot I/b \qquad (10)$$

Процес створення комплементарного образу полягає у заміні значень $< S_i, C_j >$, де $S_i$ – $i$-й байт стегоданих, $C_j$ – $j$-й байт контейнера, значенням $X_k$, що є $i$-м байтом комплементарного образу, відповідно до ключа Т. При цьому $S_i$ та $C_j$ використовуються в ролі координат комірки зі значенням $X_k$ у ключі (таблиці) Т.

Для збереження заповненого контейнеру можуть бути використані графічні формати з ущільненням без втрат, такі як PNG та lossless JPEG. Ключ передається окремо від основних даних за звичайними правилами передачі секретного ключа.

Декодування складається з двох етапів. Першим етапом є зчитування комплементарного образу. Другим етапом є відновлення прихованого зображення.

*Стійкість методу.* Ключ комплементарного образу є унікальним і генерується наново для кожного кодування, отже при повторному кодуванні того самого стегозображення в той самий контейнер буде отриманий інший комплементарний образ. Виходячи з цього, поєднання пари значень $< S_i, C_j >$ і ключа є унікальним, отже при наявності іншого ключа повне відновлення стегоданих неможливо.

Нехай $Q$ – об'єм стегозображення, а $K$ – довжина ключа. Значення $K$ постійне і дорівнює 65535, а $Q$ залежить від стегозображення, отже можливі випадки $Q \geq K$ і $Q < K$. Максимальну теоретично можливу кількість використаних байт ключа $\lambda$ можна обчислити за формулою

$$\lambda = \min(Q, K). \tag{11}$$

Оскільки реальна кількість використаних байт $\omega$ є псевдовипадковою величиною, заздалегідь невідомою, можна лише стверджувати, що

$$\omega(\lambda) \leq \lambda \tag{12}$$

Тобто реальна кількість використаних байт не може перевищити максимально теоретичну. Складність підбору використаної частини ключа виражається параметрично, а відповідна біт-орієнтована оцінка стійкості методу комплементарного образу становить $2^{<\omega,\lambda>}$.

На базі методу стеганографії на основі комплементарного образу розроблено аналогічний метод, що використовує в ролі контейнера аудіо-файли.

З орієнтацією на фонові зображення запропоновано та обґрунтовано новий метод LSB-стеганографії на основі ***шифрування палітри.***

Даний метод ґрунтується на шифруванні кодів відтінків кольорів пікселів зображення шляхом їх заміни координатами пікселів відповідних відтінків кольорів у зображенні-ключі, що використовується як ***палітра***, в якій представлені всі відтінки кольорів, наявні у зображені, що шифрується.

В ролі ключа виступає звичайне зображення, яке в процесі шифрування не зазнає жодних змін. Оскільки для шифрування і дешифрування використовується один і той самий ключ, криптосистема є симетричною, але ключ є відкритим.

**Твердження 2.** Необхідною і достатньою вимогою до зображення, яке використовується в ролі ключа для шифрування палітри, є наявність в його графічних даних *повного діапазону всіх можливих значень байт від 0 до 255.*

Назвемо цей критерій ***повнотою наявних байт***. В процесі перевірки на критерій повноти наявних байт відбувається процес створення словника координат байт, що мають відповідне значення. У випадку, якщо в словнику не залишається порожніх комірок, зображення може бути використано в ролі ключа.

В результаті формується масив списків:

$$\begin{gathered} C_0 = \{C_{0,0}, C_{0,1}, \dots C_{0,n}\}, \\ C_1 = \{C_{1,0}, C_{1,1}, \dots C_{1,m}\}, \\ \dots \\ C_{255} = \{C_{255,0}, C_{255,1}, \dots C_{255,k}\}, \end{gathered} \tag{13}$$

де: $C_i$ – список координат пікселів зображення-ключа зі значенням кольору *i*;

*n, m, k* – кількість пікселів зображення-ключа, що мають відповідне значення.

Формування словника припиняється, коли у ньому немає жодного порожнього рядка. На момент виконання даної умови всі інші рядки будуть у більшості випадків містити декілька варіантів значень пари координат. Іншим варіантом завершення формування словника є умова перевищення у всіх рядках порогової кількості $\varphi$ пар, що визначається пріоритетом швидкодії або захищеності, в залежності від ситуації.

Під час шифрування замість кожного байту графічних даних зображення, що підлягає захисту, записується значення координат деякого псевдовипадкового пікселя того ж відтінку кольору у зображені-ключі:

$$X_i = C_{S_i,R}, \quad R \in [1,n], \tag{14}$$

де: $X_i$ – $i$ -й байт даних зашифрованого зображення;

$C_{S_i}$ – список координат пікселів зображення-ключа зі значенням кольору $S_i$;

$S_i$ – $i$-й байт зображення, що шифрується;

$R$ – випадкове число у діапазоні від 1 до $n$;

$n$ – кількість елементів у рядку $C_{S_i}$.

Для відновлення даних із зашифрованого зображення необхідно мати зображення-ключ. На відміну від процесу шифрування, при розшифруванні не відбувається розкладання палітри зображення-ключа. В процесі відновлення даних відбувається зчитування графічних даних зображення-ключа $K$, а також масиву значень зашифрованого зображення $X$. В результаті розшифрування отримується масив графічних даних вихідного зображення $S$, що може бути збережене у будь-якому форматі.

**Твердження 3.** Для кодування переходів кольорів вимогою до зображення є наявність повного набору всіх можливих послідовних пар байт від {0;0} до {255;255}. Назвемо цей критерій ***повнотою наявних переходів***. Цей критерій вимагає від ключа, що може бути аудіо-файлом або зображенням, наявності всіх 255*255 можливих переходів.

Ця модифікація методу спричиняє низку відмінностей в алгоритмі побудови списків координат. Замість вектору списків формується матриця списків:

$$\begin{aligned} C_{0,0} &= \{C_{0,0,0}, C_{0,0,1}, \dots C_{0,0,n}\}, \\ C_{0,1} &= \{C_{0,1,0}, C_{0,1,1}, \dots C_{0,1,m}\}, \end{aligned} \tag{15}$$

...

$$C_{255,255} = \{C_{255,255,0}, C_{255,255,1}, \dots C_{255,255,k}\},$$

де: $C_{i,j}$ – матриця координат пікселів зображення-ключа зі значенням коду відтінку кольору $i,j$;

$n, m, k$ – кількість пікселів зображення-ключа, що мають відповідне значення.

Статистичні дослідження виявили, що більшість зображень (99,2%) не задовольняє критерію наявних переходів. Аналіз відсутніх у різних зображеннях переходів дозволяє стверджувати, що в різних зображеннях відсутні неоднакові набори переходів.

Всі розроблені методи використовують стеганографічний принцип прихованої передачі даних, при чому метод фрагментації і метод на основі комплементарного образу базуються на LSB й використовують генерацію секретного симетричного ключа.

Функції та особливості розроблених крипто-стеганографічних методів наведені у таблиці 2.

Таблиця 2

Порівняння характеристик розроблених методів

| | Метод фрагментації | Метод комплементарного образу | Метод шифрування палітри |
|---|---|---|---|
| Тип крипто функції | симетрична | симетрична | симетрична |
| Тип ключа | Секретний, складений | Секретний та відкритий | Відкритий |
| Розмір ключа | Випадковий | 64 кбайт та довільної довжини (потоковий) | не менше від 256 байт до 64 кбайт |
| Фіксованість розміру ключа | Ні | Так і Ні | Ні |
| Складність підбору ключа | $2^{<i,j>}$ | $2^{<\omega,\lambda>}$ | $\frac{n!}{(n-m)! \times m!} \times \frac{m!}{(m-z)! \times z!}$ |
| Обмеження застосування | Розмір контейнера визначається як: $C \geq 8 \cdot I/b$ | Розмір контейнера визначається як: $C \geq 8 \cdot I/b$ | Ключ має відповідати критеріям повноти наявних байт або переходів |
| Збільшення об'єму даних у захищеному вигляді | Від 1 до 8 разів в залежності від кількості стегобіт. | Від 2 до 9 разів в залежності від кількості стегобіт. | в 2 або 4 рази |
| Підтримка аудіо та зображень | є | є | є |

**<u>У третьому розділі</u>** досліджуються питання попереднього розпаралелювання алгоритмів реалізації запропонованих методів. Відомо, що захист сповільнює роботу з даними, отже для оперативної обробки даних виникає необхідність пришвидшення роботи методів захисту.

Найбільш тривалою процедурою для методів є модифікація контейнеру. Визначення часових складових роботи методу фрагментації описані формулою (7). Ті складові, що відповідають за зчитування та запис файлів на носій пам'яті, а саме $T_{чф}, T_{чп}, T_{зф}, T_{зк}$, залежать в першу чергу від особливостей апаратного забезпечення конкретного комп'ютера. Паралельне генерування ключа може спричинити колізії, оскільки алгоритм фрагментації працює як розподільних пам'яті - алокатор.

Алгоритм модифікації контейнера реалізовано у вигляді подвійного циклу, де в зовнішньому циклі відбувається зсув байт повідомлення, у внутрішньому – зсув байт контейнера відповідно до кількості використовуваних стегобіт. Паралельно відбувається контроль довжин блоку, перевіряється, чи дійшло значення потокового байта контейнера *k* до суми значень *i*-го елемента ключа *blockaddresses*, що містить адреси блоків, та відповідного значення в ключі *blocksizes*, що містить їх довжини.

Розпаралелювання застосовується до зовнішнього циклу, оскільки внутрішній цикл обмежений кількістю стегобіт, що, як правило, дорівнює 1. Використання більше одного стегобіту порушує непомітність модифікації і не вважається доцільним, хоча передбачена можливість варіювання значень від 1 до 8 стегобіт.

При розпаралелюванні між *n* ядрами багатоядерного процесора відбувається паралельна обробка *n* байт контейнера. При цьому контроль меж кожного фрагменту

відбувається окремо у кожному потоці, що дозволяє уникнути виходу за межі фрагментів. В кожний потік одразу передається необхідна адреса стегоданих в контейнері, всі подальші перевірки відбуваються вже всередині даного потоку. Таким чином, кожен потік використовує лише свої внутрішні змінні і звертається назовні лише при отриманні вихідної інформації та при видачі результату. Така організація забезпечує відносну незалежність паралельних потоків, отже, дає можливість зменшення часу роботи, незважаючи на зростання часу, що витрачається на передачу управління між потоками та надлишкове використання пам'яті для створення окремих змінних в кожному потоці. Така організація дозволяє обробляти кожний потік незалежно як при запису, так і при зчитуванні. Паралельний код є незалежним від кількості ядер і адаптується до конфігурації комп'ютера.

В алгоритмах реалізації всіх стеганографічних методів захисту мультимедійних даних запропоновано розпаралелювання алгоритмів модифікації та шифрування. Зчитування та запис повідомлень, контейнерів та ключів займає відносно небагато часу у всіх методах і виконується стандартними низькорівневими методами. Запропоновані алгоритми є адаптивними до кількості ядер процесору.

**Четвертий розділ** присвячений розробці програмного комплексу MultiHide та проведенню на ньому експериментальних досліджень запропонованих комбінованих стеганографічних методів захисту мультимедійних даних. Розроблений експериментальний комплекс містить модулі виконання алгоритмів незахищеного та захищеного LSB-стеганографічного захисту, а також LSB з шифруванням AES в реалізації RijndaelManaged. Для розробки обрано середовище Microsoft Visual Studio 2010 на платформі .NET Framework 4.0 та мову програмування C#. Вибір пов'язаний з тим, що платформа .NET містить велику кількість вже реалізованих класів для багатьох задач програмування. Комплекс має вбудований замір часу роботи алгоритмів та інструменти їх тестування зі змінюваними параметрами.

В комплексі реалізовано деякі аналітичні функції:

- регулювання кількості використовуваних стегобіт;
- аналіз місткості контейнера для кожного методу;
- можливість візуалізації даних без наявності ключа у захищеному вигляді;
- аналіз відповідності критеріям повноти наявних байт та повноти наявних переходів для методу шифрування палітри;
- модифікація ключа для використання в методі шифрування палітри.

Оскільки Windows є багатозадачною операційною системою, проведення експериментів вимагало мінімізувати кількість сторонніх процесів, що могли вплинути на час роботи методів. В експериментах з вимірюванням часу роботи методів захисту в графічних контейнерах було використано декілька пар «контейнер» - «стегодані» та різні налаштування кількості стегобіт для спостерігання незалежності тенденцій від умов. Дослідження проводились на 8-ядерному процесорі Intel Core i7. Для оцінки ефективності розпаралелювання методу КО були виконані виміри часу при різних обмеженнях на максимальну кількість використовуваних ядер процесора.

Як видно з рис. 4, збільшення кількості паралельних ядер не завжди зменшує час роботи. Для 1 та 2 стегобіт розпаралелювання є ефективним для будь-якої кількості ядер, але найшвидшим є метод КО з розпаралелюванням на 8 ядрах. Для всіх випадків при 8

ядрах метод працює швидше, ніж на 2. При 8 стегобітах найшвидшим є як послідовний метод КО, так і розпаралелений на 4 ядрах.

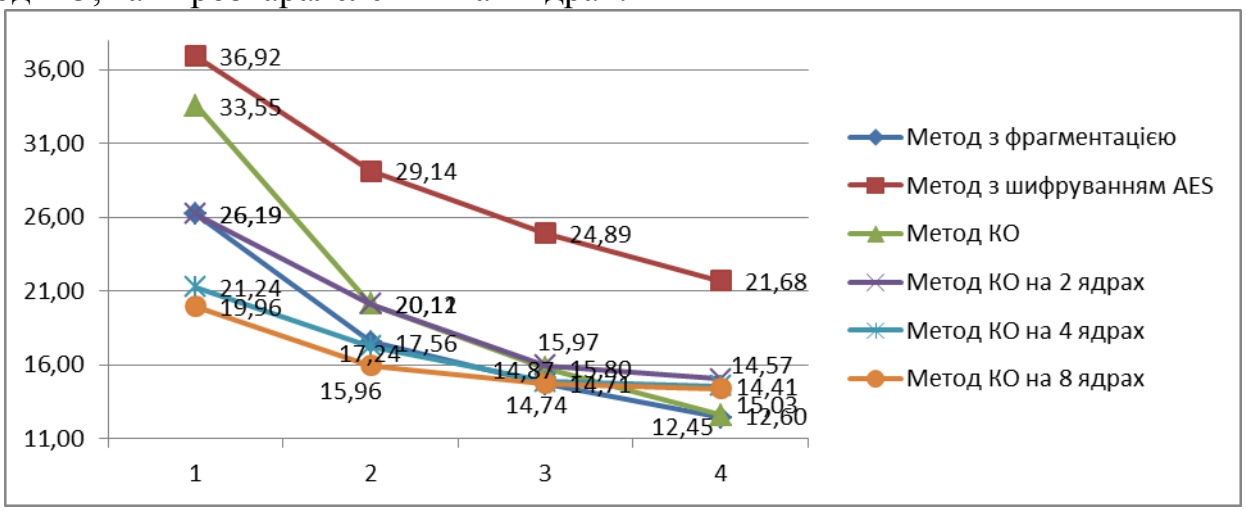


Рис. 4. Час роботи методів при вбудовуванні графічних даних в графічний контейнер (мс), 1 – 1 біт, 2 – 2 біта, 3 – 4 біта, 4 – 8 біт

Аналіз рис. 5 вказує про дещо інші тенденції, що виникають при вбудовуванні аудіо-даних в графічний контейнер. Для всіх випадків розпаралелювання зменшує час роботи методу. Найбільш ефективним є розпаралелювання на 4 ядра. Розпаралелювання на 2 ядра є більш ефективним, ніж розпаралелювання на 8 ядер.

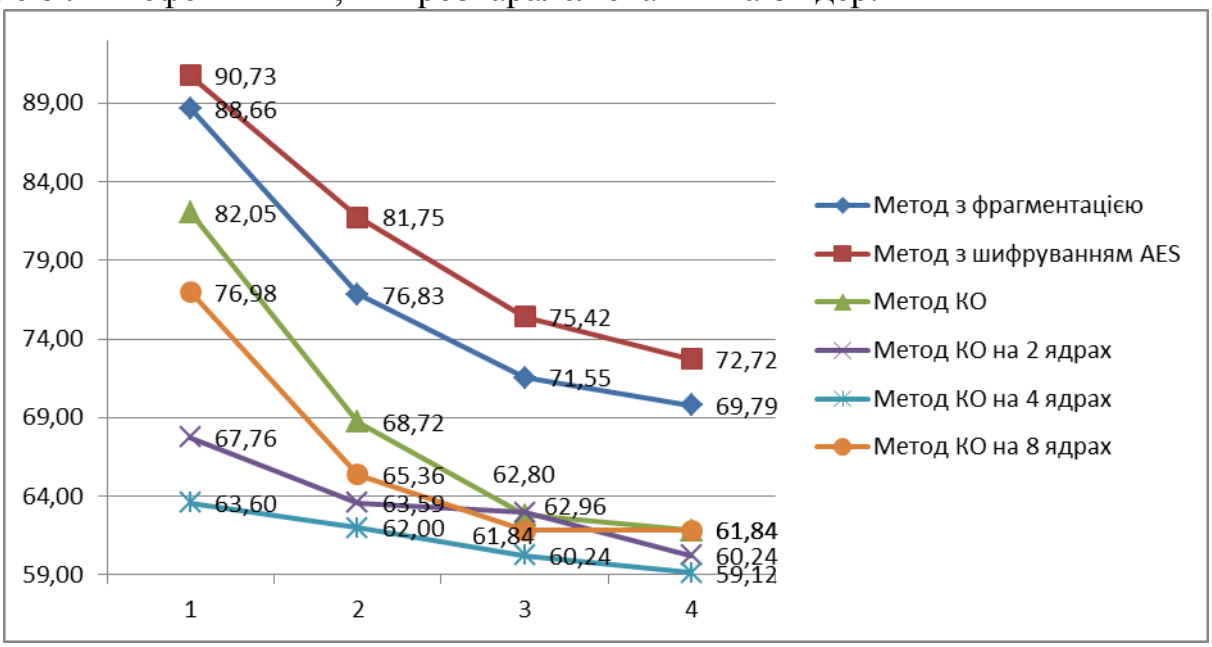


Рис. 5. Час роботи методів при вбудовуванні аудіо-даних в графічний контейнер (мс), 1 – 1 біт, 2 – 2 біта, 3 – 4 біта, 4 – 8 біт

При вбудовуванні аудіо-даних в аудіо-контейнер (рис. 6) для 1 та 2 стегобіт найбільш ефективним є розпаралелювання на 8 ядер. При 2 та 4 стегобіт – на 4 ядра. Розпаралелювання на 4 та 8 ядер є значно ефективнішим, ніж розпаралелювання на 2 ядра. При 8 стегобітах розпаралелювання є неефективним.

Висновки з серії експериментів полягають у наступному.

1) Запропоновані стеганографічні методи (КО та з фрагментацією) є швидшими за криптографічний захист на основі AES в усіх розглянутих випадках.
2) Найменший час роботи не завжди досягається при найбільшій кількості ядер.

3) При обробці різних типів даних ефективність запропонованих методів, а також варіантів розпаралелювання методу КО на різну кількість ядер, є неоднаковою.
4) Для найбільш практично використовуваних налаштувань (1 та 2 стегобіти) розпаралелювання є найбільш ефективним при 4 та 8 ядрах.

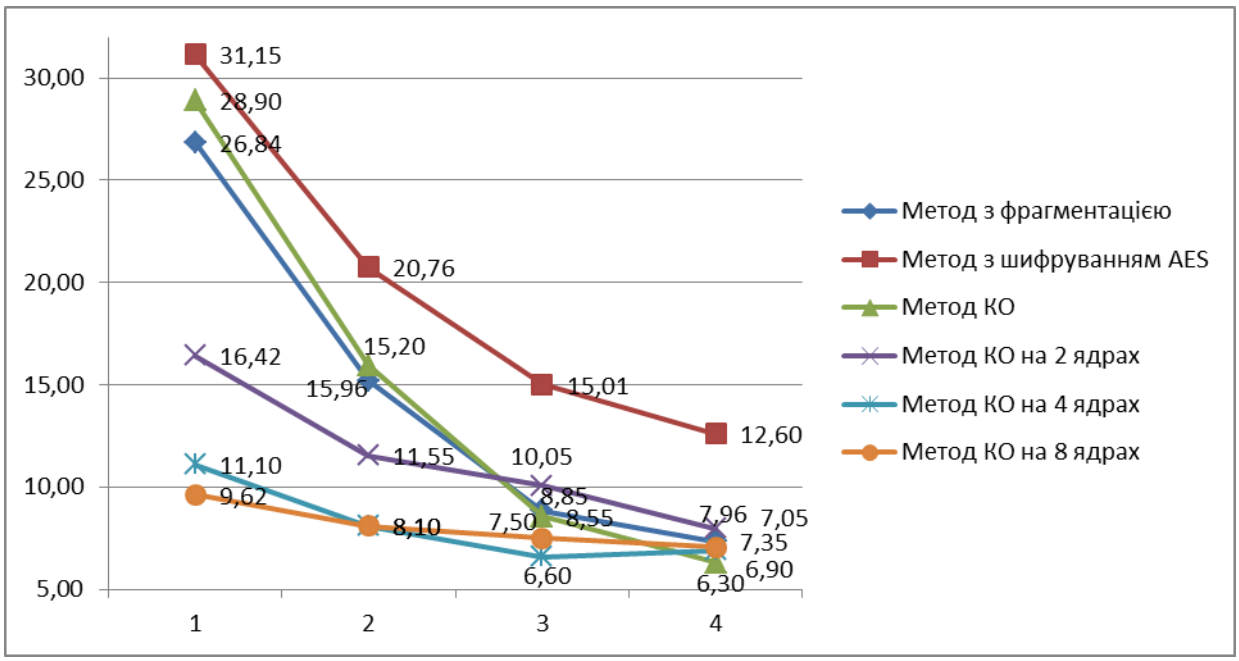


Рис. 6. Час роботи методів при вбудовуванні аудіо-даних в аудіо-контейнер (мс), 1 – 1 біт, 2 – 2 біта, 3 – 4 біта, 4 – 8 біт

Оскільки в попередніх дослідженнях виявлено, що кількість стегобіт є одним з визначальних чинників, що впливають на час роботи методів, в роботі введено новий показник ***R – коефіцієнт прискорення***, який відображає характеристику впливу кількості стегобіт на ефективність роботи методів (таблиця 3).

Найбільш ефективним при запису даних є LSB без захисту (6,22), а при зчитуванні - метод фрагментації (5,91); найменше прискорюється метод з шифруванням AES (2,66 при запису та 2,36 при зчитуванні).

Таблиця 3

Коефіцієнти прискорення при збільшенні кількості стегобіт

| Метод | Запис | | | Зчитування | | |
|---|---|---|---|---|---|---|
| | 2 біти | 4 біти | **8 біт** | 2 біти | 4 біти | **8 біт** |
| Базовий спосіб | 1,91 | 3,56 | **6,22** | 1,92 | 3,29 | **6,02** |
| LSB з фрагментацією | 1,89 | 3,43 | **5,91** | 1,97 | 3,89 | **7,24** |
| LSB з шифруванням AES | 1,54 | 2,13 | **2,66** | 1,48 | 1,97 | **2,36** |
| Метод на основі Комплементарного образу | 1,84 | 3,19 | **5,00** | 1,66 | 2,46 | **3,29** |

Для оцінки ефективності паралельної реалізації методу шифрування палітри (ШП) були проведені виміри часу шифрування для п’яти різних зображень. Як видно з таблиці 4, паралельна реалізація дає економію часу від 5,5% до 12%, що є меншим, ніж очікуваний приріст за рахунок розпаралелювання обчислень на два ядра. Цей результат пояснюється тим, що розпаралелений алгоритм шифрування палітри порівнювався з оптимізованим алгоритмом послідовного обчислення.

Таблиця 4.

Час шифрування палітри при паралельній і послідовній реалізаціях алгоритму

| Об’єм файлу зображення | Розміри зображення | Середній час шифрування (послідовна реалізація), мс | Середній час шифрування (паралельна реалізація), мс | Економія часу (%) |
|---|---|---|---|---|
| 59 815 | 320 × 213 | 11,1 | 10,5 | 5,7 |
| 376 459 | 1024 × 765 | 110,5 | 103,1 | 7,1 |
| 109 699 | 800 × 1204 | 147,5 | 139,8 | 5,5 |
| **608 290** | **1324 × 2048** | **432,3** | **385,8** | **12,0** |
| 6 529 035 | 3888 × 2592 | 1600,9 | 1451,9 | 10,2 |

Розроблений програмний комплекс MultiHide дозволяє детально аналізувати властивості контейнерів (ліве вікно), в які записуються закодовані стегодані (праве вікно). Комплекс підтримує інтерактивний інтерфейс, який дозволяє контролювати виконання етапів реалізації методів захисту. На рис. 7 подано приклад успішного запису конфіденційних графічних даних (праворуч) в аудіо-контейнер (ліворуч), при необхідних та достатніх співвідношеннях об’ємів стегоданих та контейнеру.

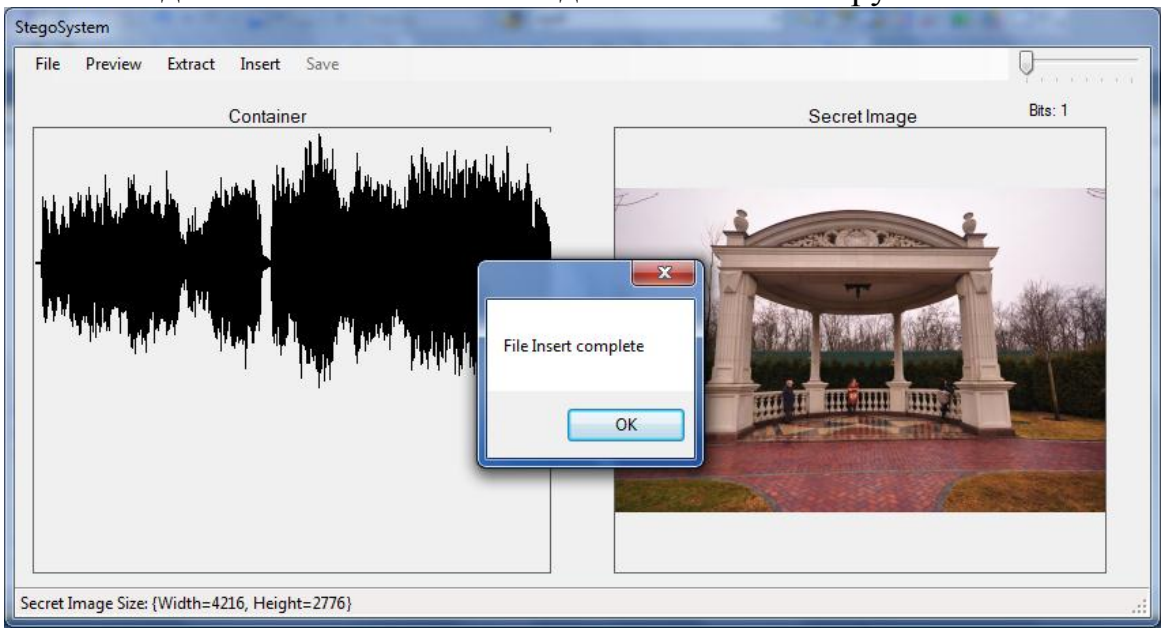


Рис. 7. Вікно інтерфейсу програмного комплексу MultiHide

## ВИСНОВКИ

В роботі вирішена актуальна науково-технічна задача створення комбінованих крипто-стеганографічних методів масового захисту мультимедійних даних на основі поєднання елементів криптографічного захисту зі стеганографічним принципом приховування мультимедійних даних, що забезпечує підвищення ефективності захисту та продуктивності при масовій обробці стрімко зростаючих об’ємів конфіденційних мультимедійних даних в розподілених комп’ютерних системах.

Отримані наступні наукові результати.

1. Запропоновано новий підхід до масового захисту мультимедійних даних в хмарних сховищах на основі створення швидких комбінованих методів та відповідних

програмних сервісів захисту, орієнтованих на масову обробку, маскування та демаскування даних в процесах прозорої оперативної взаємодії в хмарних середовищах.

2. Розроблено модифікований метод LSB-стеганографії на основі рандомізованої фрагментації стегоданих та складеного симетричного ключа, що забезпечує підвищення рівня стійкості приховування мультимедійних стегоданих за рахунок розбиття зображень чи аудіо-даних на певну кількість фрагментів, що захищає контейнер від можливості аналітичного передбачення схеми фрагментації, а також зменшує час маскування стегоданих (в 2,14 рази) порівняно з шифруванням на основі алгоритму AES.

3. Запропоновано комбінований метод LSB-стеганографії на основі комплементарного образу, що ґрунтується на формуванні блочного ключа за допомогою модифікованого латинського квадрату і відрізняється комбінованим вбудовуванням стегоданих з використанням частини даних контейнера в ролі змінного потокового ключа, що дозволяє використати наявні об'єми контейнеру та скоротити час маскування аудіо-даних в аудіо-контейнері (в 1,83 рази), зображення в графічному контейнері (в 1,66 рази), аудіо-даних в графічному контейнері (в 1,8 рази) порівняно з шифруванням на основі алгоритму AES.

4. Розроблено комбінований метод стеганографічного захисту на основі шифрування палітри шляхом заміни кодів переходів кольорів піксель первинного зображення координатами відповідних переходів кольорів у зображенні-ключі, що дозволяє за рахунок розпаралелювання зменшити час (від 5,5% до 12%) маскування мультимедійних даних довільним зображенням-ключем чи аудіо-файлом-ключем або складеними ключами – групою зображень чи групою аудіо-файлів, які відповідають критерію повноти наявних переходів.

5. Визначені оцінки критеріїв повноти наявних байт контейнеру та повноти наявних переходів у зображені-ключі як необхідні та достатні умови ефективного маскування комбінованим методом стеганографії на основі шифрування палітри.

6. Розроблені структурно-алгоритмічні засади створення засобів стеганографічного захисту мультимедійних даних, зокрема: рандомізованої фрагментації стегоданих для захисту мультимедійних даних в графічних зображеннях та аудіо-файлах; формування блочного рандомізованого ключа на основі модифікованого латинського квадрату в методі комплементарного образу; формування словника палітри для шифрування даних палітрою зображення-ключа або аудіо-файлу-ключа; паралельна реалізація методів стеганографічного захисту мультимедійних даних, яка дозволила на 4-х ядрах багатоядерного процесора додатково скоротити час маскування зображення в графічний контейнер (в 1,91 рази), аудіо-даних в аудіо-контейнер (в 3,76 рази) в порівнянні з послідовною реалізацією відповідних алгоритмів.

7. Розроблено експериментальний зразок стеганографічної системи MultiHide для реалізації та дослідження, як вищевказаних комбінованих стеганографічних методів, так і базових методів LSB-стеганографії та LSB-стеганографії з шифруванням на основі алгоритму AES, а також дослідження відповідних сервісів.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Широчин, С.С. Спосіб стеганографічного захисту даних в аудіо-файлах на основі комплементарного образу / Є.С. Сулема, С.С. Широчин // Вісник КПІ. Інформатика,

управління та обчислювальна техніка. – 2014. – Вип. 61. – С. 80-87. – *(Входить до наукометричних баз Directory of Open Access Journals (DOAJ), Російський індекс наукового цитування (РІНЦ), Google Scholar).*

*Здобувачем виконано адаптацію метода стеганографії на основі комплементарного образу для аудіо-файлів.*

2. Широчин, С.С. Метод захисту зображень на основі шифрування палітри / Є.С. Сулема, С.С. Широчин // Вісник Хмельницького національного університету. – 2014. – №3. – С. 114-119.

*Дисертантом реалізовано криптографічний метод захисту зображень з використанням довільного зображення в ролі ключа.*

3. Широчин, С.С. Спосіб стеганографії зображень на основі комплементарного образу / Є.С. Сулема, С.С. Широчин // Захист інформації. – 2013. – Вип. 4. – С. 345-353.

*Автором розроблено метод стеганографії з захистом стегоданих шляхом їх комплементарного перетворення.*

4. Широчин, С.С. Спосіб стеганографії зображень з фрагментацією стегоданих та розділенням закритого ключа / Є.С. Сулема, С.С. Широчин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Вип. 1 (22). – С. 64-68. – *(Входить до наукометричних баз: Directory of Open Access Journais, «Наукова періодика України», UlrichsWeb Global Serials Directory)*.

*Дисертантом розроблено алгоритм фрагментації стегоданих.*

5. Широчин, С.С. Біт-орієнтовані оцінки стійкості криптографічних алгоритмів / В.П. Широчин, В.Є. Мухін, С.С. Широчин // Сучасна спеціальна техніка. – 2010. – № 1. – С. 54-59.

*Автором виконано біт-орієнтовану оцінку складності ряду криптографічних алгоритмів.*

6. Shyrochyn Semen. Methods for user's personal multimedia data protection in clouds / Semen Shyrochyn, Yevgeniya Sulema // Proc. 3rd IEEE Conference on Cloud Networking. – Luxemburg. – 2014.

*Здобувачем запропоновано довірений сервіс захисту мультимедійних даних користувача в хмарних сховищах.*

7. Широчин, С.С. Аналіз ефективності паралельної реалізації алгоритмів захисту зображень / Є.С. Сулема, С.С. Широчин // Збірник праць міжнародної науково-практичної конференції "Актуальні проблеми комп'ютерних технологій". – Хмельницький. – 2014. – С. 64-68.

*Дисертантом проаналізовано часові показники послідовних та паралельних реалізацій стеганографічних алгоритмів.*

8. Широчин С.С., Сулема Е.С., Защита персональных графических данных пользователя при передаче по компьютерным сетям // Материалы I Международной научно-практической конференции "Информационные технологии. Проблемы и решения". – Уфа. – 2014. – С. 7-10.

*Автором виконано огляд існуючих засобів захисту мультимедійних даних.*

9. Широчин, С.С. Підвищення стійкості LSB-стегосистем шляхом аналізу і корекції характеристик контейнера / Сулема Є.С., Широчин С.С. // Збірник наукових праць

шостої міжнародної науково-технічної конференції "Актуальні проблеми комп'ютерних технологій (АПКТ-2012)". – Хмельницький. – 2012. – С. 319-327.

*Дисертантом запропоновано критерії стегопридатності для контейнеро-орієнтованої стегосистеми.*

10. Широчин, С.С. Алгоритм фрагментації стегоданих у стеганографії зображень / С.С. Широчин, Є.С. Сулема // Збірник тез доповідей четвертої наукової конференції магістрантів та аспірантів "Прикладна математика та комп'ютинг (ПМК-2012)". – Київ. – 2012. – С. 299-303.

*Дисертантом запропоновано алгоритм фрагментації стегоданих.*

11. Широчин, С.С. Засоби подання інформації з обмеженим доступом в картографічних зображеннях / С.С. Широчин, Є.С. Сулема // Збірник праць міжнародної науково-практичної конференції "Актуальні проблеми комп'ютерних технологій". – Хмельницький. – 2011. – С. 207-213.

*Здобувачем проаналізовано можливості подання захищених неграфічних даних в картографічних графічних даних.*

12. Широчин, С.С. Критерії пошуку оптимального розташування блоків стеганографічних даних в контейнері / Є.С. Сулема, С.С. Широчин // Матеріали міжнародної конференції "Системний аналіз та інформаційні технології". – Київ. – 2011. – С. 516.

*Дисертантом запропоновано критерії оцінки алгоритму фрагментації стегоданих в контейнері.*

## АНОТАЦІЯ

**Широчин С.С. Методи комбінованого стеганографічного захисту мультимедійних даних в хмарних сховищах. – Рукопис.**

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти. – Національний технічний університет України "Київський політехнічний інститут", Київ, 2015.

Робота присвячена вирішенню актуальної науково-технічної задачі захисту конфіденційних мультимедійних даних в хмарних сховищах шляхом розроблення нових і модифікації існуючих методів захисту на основі LSB-стеганографії та LW-криптографії, масового захисту мультимедійних даних в зображеннях-контейнерах чи аудіо-файлах-контейнерах з використанням приватних та публічних ключів.

Розроблено нові методи захисту мультимедійних даних в хмарних сховищах, що забезпечують захищену передачу даних при зменшенні часових витрат, зокрема запропоновано метод стеганографії з фрагментацією стегоданих в контейнері, метод стеганографії на основі комплементарного образу, а також метод шифрування палітри. В запропонованих методах передбачається використання як складених блочних ключів, так і змінних потокових ключів довільної довжини.

Запропоновано зменшення часової складності методів захисту мультимедійних даних за рахунок розпаралелювання обчислень на ядрах багатоядерного процесора та спрощення маскуючих перетворень для захисту стегоданих в контейнері.

Розроблено експериментальний зразок стеганографічної системи MultiHide для реалізації та дослідження, як вищевказаних комбінованих стеганографічних методів, так

і базових методів LSB-стеганографії та LSB-стеганографії з шифруванням на основі алгоритму AES, а також для дослідження програмної реалізації відповідних хмарних сервісів захисту.

**Ключові слова:** LSB-стеганографія, LW-криптографія, хмарні сховища, захист мультимедійних даних, стегодані, розпаралелювання обчислень.

## АННОТАЦИЯ

**Широчин С.С. Методы комбинированной стеганографической защиты мультимедийных данных в облачных хранилищах. - Рукопись.**

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – Компьютерные системы и компоненты. – Национальный технический университет Украины "Киевский политехнический институт", 2015.

Работа посвящена решению актуальной научно-технической задачи защиты конфиденциальных мультимедийных данных в облачных хранилищах путем разработки новых и модификации существующих методов защиты на базе LSB-стеганографии и LW-криптографии, массовой защиты мультимедийных данных в изображениях-контейнерах или аудио-файлах-контейнерах с использованием открытых и закрытых ключей. Разрабатываемые методы комбинируют стеганографический принцип сокрытия факта передачи данных с криптографическим принципом шифрования, что повышает защиту данных даже в случае обнаружения факта их наличия.

Предложен метод стеганографии, использующий фрагментацию стегоданных при записи в контейнер. Метод использует новое рандомизированное разделение исходного сообщения на фрагменты произвольной длины, также выполняющий функцию аллокатора и гарантирующий размещение фрагментов в пространстве контейнера без коллизий. Составной секретный ключ содержит адреса и длины фрагментов в последовательности, необходимой для восстановления исходного сообщения.

Разработан и исследован комбинированный метод LSB-стеганографии на основе комплементарного образа, основанный на формировании блочного ключа с помощью модифицированного латинского квадрата, и отличается комбинированным встраиванием стегоданных с использованием части данных контейнера в роли переменного потокового ключа, позволяет использовать имеющиеся объемы контейнера и сократить время маскировки аудио-данных в аудио-контейнере (в 1,83 раза), изображение в графическом контейнере (в 1,66 раза), аудио-данных в графическом контейнере (в 1,8 раза) по сравнению с шифрованием на основе алгоритма AES.

Разработан и теоретически обоснован метод шифрования палитры, заменяющий значение байт сообщения соответствующими координатами изображения-ключа или аудио-файла-ключа. В качестве ключа предполагается произвольное изображение или аудио-файл, соответствующий одному из критериев полноты имеющихся характеристик – полноты имеющихся байт или полноты имеющихся переходов. Также в качестве ключа могут выступать группы изображений или аудио-файлов, суммарно соответствующие критериям полноты. В процессе кодирования ключ (группа ключей) не подвергается изменениям и может быть передан открытыми каналами связи.

Исследованы параллельные реализации методов защиты мультимедийных данных путём распараллеливания вычислений на ядрах многоядерного процессора, что

позволило обосновать возможности организации параллельных каналов маскирующих преобразований для защиты графических и аудио-стегоданных в графическом и аудио-контейнере.

Разработан экспериментальный образец стеганографической системы MultiHide для реализации и исследования как вышеуказанных комбинированных стеганографических методов, так и базовых методов LSB-стеганографии и LSB-стеганографии с использованием шифрования на основе алгоритма AES, а также для исследования программной реализации соответствующих облачных сервисов защиты.

Полученные экспериментальным образом данные замеров временных затрат свидетельствуют о применимости предложенных методов и их повышенному быстродействию в сравнении с защитой с использованием шифрования на основе алгоритма AES, особенно при использовании параллельных вычислений. Исследована параллельная реализация предложенных методов стеганографической защиты мультимедийных данных, которая позволила на 4-х ядрах многоядерного процессора дополнительно сократить время маскировки изображения в графический контейнер (в 1,91 раза), аудио-данных в аудио-контейнер (в 3,76 раза) по сравнению с последовательной реализацией соответствующих методов.

**Ключевые слова**: LSB-стеганография, LW-криптография, облачные хранилища, защита мультимедийных данных, стегоданные, распараллеливание вычислений.

## ABSTRACT

**Shyrochyn S.S. Methods combined steganographic protection of multimedia data in cloud storages. - Manuscript.**

Thesis for the degree of candidate of technical sciences, specialty 05.13.05 – Computer Systems and Components. – National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, 2015.

The work is devoted to solving actual scientific and technical problem of protection of sensitive multimedia in cloud storages by developing new and modifying existing protection methods based on LSB-steganography and LW-cryptography protection of multimedia data in image containers and audio containers using private and public keys.

New methods of protection of multimedia data in cloud storage have been developed, providing secure data transmission while reducing time expenses, in particular – the stegodata fragmentation method, steganography method based on complementary image and palette encryption method. Proposed methods use composite block keys and stream keys of random length.

A reduction of time complexity of multimedia data protection methods hs been proposed by parallelizing computations on cores of multicore processor and simplifying masking transformations to protect stegodata in the container.

The experimental model of steganography system MultiHide has been developed to implement and analyze both the above mentioned methods and basic methods of LSB-steganography and LSB-steganography using AES-cryptography, and also for research of program implementation of appropriate cloud security services.

**Keywords**: LSB-steganography, LW-cryptography, cloud storage, protection of multimedia data, stegodata, parallelizing computations.