НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КІНЗЕРЯВИЙ Олексій Миколайович

УДК 003.26:004.056.55

СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ДАНИХ У ВЕКТОРНІ ЗОБРАЖЕННЯ, СТІЙКІ ДО АКТИВНИХ АТАК НА ОСНОВІ АФІННИХ ПЕРЕТВОРЕНЬ

Спеціальність 05.13.21 – Системи захисту інформації

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Київ – 2015

Дисертацією є рукопис.

Робота виконана в Національному авіаційному університеті Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук
Ковтун Владислав Юрійович
Національний авіаційний університет,
доцент кафедри безпеки інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Кузнецов Олександр Олександрович,
Харківський національний університет ім. В.Н. Каразіна,
професор кафедри безпеки інформаційних систем і технологій

доктор технічних наук, професор
Смірнов Олексій Анатолійович,
Кіровоградський національний технічний університет,
завідувач кафедри програмного забезпечення

Захист відбудеться 01 жовтня 2015 р. о 14^{30} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий 31 серпня 2015 р.

Учений секретар
спеціалізованої вченої ради
к.т.н., доцент С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Розвиток глобальної мережі Інтернет та поширення її використання серед населення планети, сприяє збільшенню обсягів інформації, що передається, обробляється, зберігається та знищується. Використовуючи можливості і ресурси мережі Інтернет можна організувати резервний канал зв'язку, наприклад, з дипломатичними установами, що знаходяться на території іноземних держав. Скритність передачі інформації по такому каналу буде забезпечуватися стенографічними засобами захисту. Основна відміна стеганографії від інших методів захисту інформації, полягає саме у прихованні факту існування секретного повідомлення в іншому, не привертаючому уваги об'єкті – контейнері, використовуючи для цього структурні особливості побудови самого контейнера та властивості органів сприйняття людини.

Значний вклад в розвиток стеганографії в Україні й на пострадянському просторі внесли А.В. Аграновський, В.Г. Грибунін, В.К. Задірака, Є.А. Золотовкін, А.А. Кобозєва, Г.Ф. Конахович, О.О. Кузнецов, В.В. Лукічов, І.І. Маракова, О.А. Смірнов, В.О. Хорошко, М.Є. Шелест, Ю.Є. Яремчук та інші. Серед закордонних науковців варто згадати I. Cox, Y. Li, N. Nikolaidis, R. Ohbuchi, I. Pitas, V. Solachidis, M. Voigt та інших.

Більшість сучасних стеганографічних досліджень та методів присвячені приховуванню інформації в графічних зображеннях. Враховуючи той факт, що шлюзи доступу в мережу Інтернет знаходяться під контролем спецслужб розвинутих країн, то при передачі зображень можуть застосовуватися активні фільтри, які візуально непомітно модифікують їх і таким чином знищують приховане повідомлення. До таких атак слід віднести різного роду трансформації на основі афінних перетворень. Забезпечити стійкість до афінних перетворень можливо завдяки використанню в якості контейнерів векторних зображень, які за своїми властивостями і принципами побудови дозволяють будувати зображення з досить високою якістю.

Проведений аналіз сучасних стеганографічних методів приховування інформації у векторні зображення показав слабку стійкість їх до афінних перетворень. Крім того, існуючі методи базуються на просторових та частотних перетвореннях векторних зображень, що внаслідок зміни їх контурів чи положень координат точок призводять до погіршення якості самого зображення та утворення видимих відхилень ліній векторних об'єктів.

Таким чином, *актуальним* науковим завданням, що має теоретичне і практичне значення, є розробка нових та удосконалення існуючих стеганографічних методів приховування інформації у векторні зображення, з метою підвищення стійкості до активних атак на основі афінних перетворень.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження виконувалися в рамках «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009–2013 роки» (затверджених наказом МОН України та НАН України № 1066/609 від 26.11.2009), держбюджетної науково-дослідної роботи «Організація систем

захисту інформації від кібератак» (№ 0111U000171), «Методи та моделі стеганографічного захисту інформації від кібератак» (№ 101/14.01.06), «Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах» (№ 61/09.01.08), що проводились за планами НДР Національного авіаційного університету.

Мета і задачі дослідження. *Метою роботи* є підвищення стійкості стеганографічного захисту інформації на основі застосування нових методів приховування даних у векторні зображення, стійких до активних атак на основі афінних перетворень.

Для досягнення даної мети необхідно розв'язати такі *основні завдання*:

– провести аналіз сучасних стеганографічних методів приховування інформації у векторні зображення;

– формалізувати вимоги до вибору контейнера та визначити параметри приховування інформації у векторні зображення;

– розробити метод побітового приховування інформації у точково-задані криві векторних зображень, що забезпечує стійкість до активних атак на основі афінних перетворень;

– розробити метод шаблонного приховування інформації з визначеною таблицею співвідношень значень елементів шаблону різним крокам побудови точково-заданих кривих векторних зображень, що забезпечує стійкість до активних атак на основі афінних перетворень;

– розробити структурну модель процесу прихованої передачі інформації резервним каналом зв'язку;

– розробити алгоритми приховування інформації у криві Без'є третього ступеня векторних зображень;

– на основі запропонованих алгоритмів розробити програмне забезпечення (ПЗ) з метою їх верифікації.

Об'єктом дослідження є процес приховування інформації у векторні зображення.

Предметом дослідження є стеганографічні методи приховування інформації у точково-задані криві векторних зображень, що забезпечують стійкість до активних атак на основі афінних перетворень.

Методи дослідження. Проведені дослідження базуються на теоретико-множинному підході до розробки структурної моделі процесу прихованої передачі інформації резервним каналом зв'язку; для оцінки якісних показників методів приховування інформації у точково-задані криві векторних зображень використовуються чисельні методи, методи обчислювальної лінійної алгебри, матричного і статистичного аналізу; об'єктно-орієнтованого програмування (розробка ПЗ для експериментального дослідження) тощо.

Наукова новизна одержаних результатів полягає в такому:

– *вперше* визначено множину параметрів приховування даних у векторні зображення, які, за рахунок врахування особливостей побудови векторних зображень (ступеня точково-заданих кривих, їх допустимої довжини відносно опорних точок) та стеганографічних перетворень (точність координат опорних точок, допустимої похибки

округлення при вилученні даних та кількості інформації, що приховується в одну криву), дозволяють формалізувати вимоги до вибору контейнерів та впливати на процес приховування інформації у точково-задані криві;

– *вперше* розроблено метод побітового приховування інформації у точково-задані криві векторних зображень, який, за рахунок впливу послідовності даних на процес сегментації кривих з фіксованим кроком зміни параметра побудови заданих кривих (розбиття кривих на сегменти відбувається лише при вбудовуванні нульового/одиничного біта приховуваної послідовності даних), забезпечує високу швидкодію приховування, вилучення секретного повідомлення та підвищує стійкість до активних атак на основі афінних перетворень;

– *вперше* розроблено метод шаблонного приховування інформації у точково-задані криві векторних зображень, який, за рахунок впливу послідовності даних на процес сегментації кривих згідно визначеної таблиці співвідношень значень елементів шаблону різним крокам зміни параметра побудови заданих кривих (при розбитті кривої на два сегменти вбудовується блок даних), на відміну від побітового методу, дозволяє зменшити розміри стеганоконтейнерів, підвищити швидкість вбудовування та стійкість до активних атак на основі афінних перетворень.

Практичне значення одержаних результатів. Практична цінність роботи полягає в наступному:

– розробці структурної моделі процесу прихованої передачі інформації резервним каналом зв'язку, що дозволяє формувати множину стеганоконтейнерів, стійких до афінних перетворень.

– розробці двох нових стеганографічних алгоритмів приховування інформації у криві Без'є третього ступеня, що можуть бути використані для підвищення стійкості до активних атак на основі афінних перетворень;

– розробці методики проведення експериментального дослідження, що дозволяє оцінити ефективність приховування секретного повідомлення запропонованими методами;

– розробці програмних засобів для проведення експериментальних досліджень запропонованих рішень.

Результати дисертаційної роботи впроваджено у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету (від 30.06.2015 р.) та у науково-технічних розробках ТОВ «Сайфер ЛТД» (від 23.06.2015 р.), «Каскад Груп Україна» (від 19.02.2015 р.), що підтверджено відповідними актами впровадження.

Особистий внесок здобувача. Всі результати, які складають основний зміст дисертаційної роботи, отримано здобувачем самостійно. У роботах, написаних у співавторстві, автору належать: [1, 12] – розробка методу шаблонного приховування інформації з визначеною таблицею співвідношень значень елементів шаблону різним крокам побудови точково-заданих кривих; [3, 11] – розробка методу побітового приховування інформації у точково-задані криві векторних зображень; [2, 4, 13, 14] – експериментальне дослідження стійкості побітового та шаблонного методу до атак на основі афінних перетворень, визначення вимоги до вибору контейнера, основних

етапів та параметрів приховування інформації у векторні зображення; [5] – аналіз сучасних стеганографічних методів захисту інформації; [6, 7] – розробка принципів побудови нових блокових шифрів для їх використання в процесі вбудовування інформації.

Апробація результатів дисертації. Результати дисертаційної роботи доповідались та обговорювались більш ніж на 15 науково-технічних конференціях, серед яких: науково-технічна конференція «Безпека інформаційних технологій (ITSEC)» (Київ, 2012-2014 р); міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК)» (Київ, 2012-2014 р.); міжнародна науково-практична конференція «Інфокомунікації - сучасність та майбутнє» (Одеса, 2013 р., 2014 р.); науково-практична конференція «Механізми управління безпекою підприємств в сучасних умовах господарювання» (Київ, 2013 р.); міжнародна науково-практична конференція «Захист інформації і безпека інформаційних систем» (Львів, 2014 р); міжнародний форум «Радиоэлектроника и молодежь в XXI веке» (Харків, 2014 р.); всесвітній конгрес «Безпека в авіації та космічні технології» (Київ, 2014 р.); науково-практична конференція «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Київ, 2015 р.); міжнародна науково-практична конференція «Політ. Сучасні проблеми науки» (Київ, 2015 р.); міжнародна науково-технічна конференція «Авіа-2015» (Київ, 2015 р.); міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2015 р.); науково-методичні семінари кафедри безпеки інформаційних технологій Національного авіаційного університету.

Публікації. Основні положення дисертації опубліковано у 14 наукових працях, у тому числі – 7 статтях у фахових виданнях України (6 з яких входять до міжнародних наукометричних баз даних), а також 7 тезах доповідей на конференціях.

Структура роботи та її обсяг. Дисертація складається із вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел, і має 140 сторінок основного тексту, 74 рисунків, 29 таблиць, 87 сторінок додатків. Список використаних джерел містить 109 найменувань і займає 12 сторінок. Загальний обсяг роботи − 239 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** дисертаційної роботи обґрунтовано актуальність теми, вказано зв'язок роботи з науковими програмами, сформульовано мету та задачі досліджень. Наведено основні наукові, практичні результати та дані про їх апробацію і впровадження.

У **першому розділі** проведено аналіз вітчизняної та зарубіжної літератури за темою дисертаційного дослідження. Розглянуто спосіб організації резервного каналу зв'язку через загальнодоступну мережу Інтернет, який, наприклад, може бути застосований дипломатичними установами, що знаходяться на території іноземних держав.

Скритність передачі інформації по такому каналу здійснюється стенографічними засобами захисту, за якими секретне повідомлення

вбудовується в не привертаючий увагу об’єкт – контейнер, який потім відкрито транспортується адресату. Одним із найпоширеніших та використовуваних контейнерів є зображення. Це пов’язано з тим, що вони здатні приховувати досить великі обсяги даних.

Однак, враховуючи той факт, що шлюзи доступу в мережу Інтернет знаходяться під контролем спецслужб розвинутих країн, то можуть бути застосовані активні фільтри при передачі контейнерів-зображень. Такі атаки можуть візуально непомітно модифікувати саме зображення і безповоротно знищити приховане повідомлення. До таких атак відносяться накладання різного роду трансформацій, серед яких найбільш поширеними є афінні перетворення.

Проведені дослідження, показують, що стеганографічні методи, які використовують растрові та фрактальні зображення в якості контейнерів, не забезпечують стійкість до афінних перетворень. У той час, як методи приховування у векторні зображення, завдяки властивостям побудови векторної графіки, можуть успішно протистояти їм.

Відомими стеганографічними методами, що використовують векторні зображення є методи Канга, Обуші, Шульца-Войта, Карпінцева-Яремчука та інші. Проведений аналіз стійкості заданих методів показав слабку здатність протидії їх до афінних перетворень. Крім того, дані методи базуються на просторових та частотних перетвореннях векторних зображень, які при зміні контурів векторних об’єктів погіршують якість самого зображення та утворюють видимі відхилення ліній даних об’єктів, що не дозволяє їх в повній мірі використовувати для передачі секретної інформації резервним каналом зв’язку.

Зважаючи на це, існує необхідність у проведенні досліджень та розробки стеганографічних методів приховування даних у векторні зображення, стійких до афінних перетворень, характер змін яких не призводитиме до помітних відхилень об’єктів в контейнері, що дасть можливість підвищити ефективність стеганографічного захисту інформації.

Другий розділ присвячений формалізації вимог до вибору контейнера, визначенню параметрів приховування інформації у векторні зображення та розробці методів вбудовування даних у точково-задані криві.

Векторні зображення використовуються при побудові повнокольорових ілюстрацій, складних креслень, емблем тощо, де потрібне виконання афінних перетворень без втрати якості. Основним елементом в векторній графіці є лінія, якій притаманні деякі властивості: форма, колір, товщина та інші. Задається кожна лінія за допомогою аналітичної формули з певним числом параметрів необхідних для її представлення. Будь-який об’єкт (прямокутник, еліпс, пряма лінія тощо) сприймається і подається як криві лінії. Досить великий клас кривих, які відрізняються різним ступенем гладкості, можна побудувати за сукупністю точок, заданих за допомогою проективних координат. Такий клас кривих називається точково-заданими, а до їх складу відносяться ламана лінія та різноманітні сплайнові криві.

Будуються дані криві за допомогою множини точок (вершин) $\mathbf{P} = \{P_i\}$, $i = \overline{0,n}$, n – ступінь кривої, та параметра побудови кривих t, $t \in [a,b]$, що при послідовному з'єднані утворюють ламану, яку називають опорною, а її вершини – опорними.

Кожне значення параметра побудови кривих t строго визначає положення точок на кривій. Зафіксувавши певний крок Δt зміни параметра t буде здійснюватися перехід між його значеннями $t_{i+1} = t_i + \Delta t$ під час побудови кривої в межах визначеного проміжку $[a,b]$. Використовуючи значення t_i можна здійснювати приховування інформації у точково-задані криві шляхом їх розбиття на сукупності сегментів в даних точках. За допомогою властивості афінно-інваріантності, якою володіє ряд кривих даного класу, буде забезпечуватися стійкість до атак на основі афінних перетворень.

Для підвищення ефективності вбудовування інформації у криві векторного зображення введено множину параметрів $\mathbf{V} = \{V_j\}$, $j \in \overline{1,5}$, що впливатимуть на вибір допустимих контейнерів та на процес вбудовування/вилучення інформації.

1. Точково-задані криві визначаються ступенем порядку, а саме кількістю опорних точок необхідних для їх представлення. Кількість таких точок для представлення кривої може бути довільною. Тому, введено параметр V_1, що визначає ступінь кривих в які буде вбудовуватися інформація.

2. Розбиття досить малих кривих призводить до отримання опорних точок сформованих сегментів з координатами, що практично не відрізняються одна від одної. Використання таких кривих ускладнює процес приховування/вилучення інформації. Тому, введено параметр V_2, що визначає мінімальну допустиму відстань між опорними точками кривої.

3. Приховування всього повідомлення в одну криву векторного зображення призведе до отримання великої кількості сегментів та координат опорних точок необхідних для їх представлення. Таке вбудовування може бути помітним при аналізі контейнера, тому введено параметр V_3, що визначає максимальну кількість вбудовуваної інформації в одну криву.

4. Векторні зображення задаються координатами точок, які можуть мати довільну кількість розрядів дробової частини. Відкидання певної кількості розрядів до певної точності не вплине суттєво на якість самого зображення і тим самим зменшить розміри контейнера/стеганоконтейнера. Тому, введено параметр V_4, що визначатиме точність координат опорних точок в кривих.

5. При розбитті/відтворенні початкових кривих буде присутня похибка округлення, яка стосуватиметься останніх розрядів дробової частини координат опорних точок. Тому, введено параметр V_5, що визначатиме максимально допустиму похибку, яка враховуватиметься при вилученні прихованого повідомлення.

На основі вищесказаного розроблено стеганографічний *метод побітового приховування інформації* у векторні зображення. За яким приховування інформації відбувається наступним чином:

Крок 1. Секретне повідомлення $a=\{a_i\}$, $a_i \in \{0,1\}$, $i=\overline{1,h}$, a_i – біт секретного повідомлення, h – кількість біт повідомлення a, ділиться на частини $a=\left\{a_1^1,...,a_{V_3}^1,a_1^2,...,a_{V_3}^2,...,a_1^j,...,a_{V_3}^j\right\}$, $a^j=\left\{a_1^j,...,a_{V_3}^j\right\}$, $a_i^j \in \{0,1\}$, $i=\overline{1,V_3}$, $j=\overline{1,m}$, $m=h/V_3$, де m – кількість кривих ступеня V_1 з мінімальною допустиму відстанню між опорними точками V_2 із сукупності векторних зображень в які приховуються частини повідомлення.

Крок 2. Для кожної послідовності a^j визначається стеганоключ Δt^j, $j=\overline{1,m}$ кроку зміни параметра t, де кожний $\Delta t^j < 1/V_3$.

Крок 3. Приховування кожної послідовності a_i^j, $i=\overline{1,V_3}$ в криву D_j, $j=\overline{1,m}$ виконується шляхом розбиття її на послідовність сегментів $D_j^* = D_{V_1}^0 \cup D_{V_1}^1 \cup ... \cup D_{V_1}^w$, де w – індекс послідовності сегментів кривої D_j^*, $w \in N$ (перед приховуванням $w=0$ і $D_{V_1}^0 = D_j$). Розбиття виконується при заданому параметрі t_i ($t_i = t_{i-1} + \Delta t^j$, де t_0 – довільне початкове значення, $0 \le t_0 < 1 - V_3 \cdot \Delta t^j$):

3.1 При приховуванні біта $a_i^j = 0$ ($a_i^j = 1$ – в залежності від вибору значення біта при якому відбувається поділ кривих) в заданій точці розбиття t_i крива не ділиться, а відбувається перехід до наступного біта a_{i+1}^j.

3.2 При приховуванні біта $a_i^j = 1$ ($a_i^j = 0$ – в залежності від вибору значення біта при якому відбувається поділ кривих) в заданій точці розбиття t_i виконується поділ кривої $D_{V_1}^w$ на два сегмента $D_{V_1}^w$ і $D_{V_1}^{w+1}$. Координати опорних точок отриманих сегментів розраховуються із обраною точністю V_4. Подальше внесення наступного біта a_{i+1}^j відбувається при наступному значенні t_{i+1} в отриманий сегмент $D_{V_1}^{w+1}$. Кожний поділ кривої призводить до збільшення кількості послідовності сегментів на один ($w = w+1$).

3.3. Після приховування послідовності a^j у D_j криву, отримана послідовність сегментів D_j^* записується до стеганоконтейнера замість D_j кривої.

Також, розроблено стеганографічний метод шаблонного приховування інформації у векторні зображення, який оперуватиме вже не бітами даних, а цілими блоками біт. Основною відмінністю шаблонного методу від побітового є можливість визначати наперед різні кроки зміни параметра t відповідно кожному значенню елемента шаблону. В свою, чергу це дозволить

приховувати цілий блок бітів лише за одне розбиття кривої. Таблиця значень шаблону буде відігравати роль стеганоключа, необхідного для приховування/відтворення інформації.

Значення елементів шаблону, де кожному її елементу ставитиметься у відповідність свій крок зміни параметра t, задаватимуться наступним співвідношенням:

$$TV_l^k \to T\Delta t^k,$$

де k – індекс значень елементів шаблону, $k = \overline{1, 2^l}$, TV_l^k – значення одного елементу шаблону, l – кількість біт одного значення елементу шаблону, $T\Delta t^k$ – відповідний крок зміни параметра t для приховування блоку TV_l^k.

Приховування інформації за шаблонним методом відбувається наступним чином:

Крок 1. Секретне повідомлення $a = \{a_i\}$, $a_i \in \{0,1\}$, $i = \overline{1,h}$, a_i – біт секретного повідомлення, h – кількість біт повідомлення a, ділиться на частини $a = \left\{a_1^1,...,a_{V_3}^1, a_1^2,...,a_{V_3}^2,...,a_1^j,...,a_{V_3}^j\right\}$, $a^j = \left\{a_1^j,...,a_{V_3}^j\right\}$, $a_i^j \in \{0,1\}$, $i = \overline{1,V_3}$, $j = \overline{1,m}$, $m = h/V_3$, де m – кількість допустимих кривих ступеня V_1 з мінімальною допустиму відстанню між опорними точками V_2 із сукупності векторних зображень в які приховуються частини повідомлення. Після чого, кожна a^j послідовність ділиться на блоки $a^j = \left\{a_1^l, a_2^l,..., a_i^l ..., a_z^l\right\}$, $z = V_3 / l$, де a_i^l – i-та частина блоку a^j довжиною l біт, $i = \overline{1,z}$. Кожному a_i^l відповідатиме свій елемент з таблиці шаблонів TV_l^k, $k = \overline{1, 2^l}$.

Крок 2. Визначається максимально допустиме значення $\max \Delta t = l / V_3$ та встановлюється кожному елементу TV_l^k шаблону власний крок $T\Delta t^k$, $k = \overline{1, 2^l}$, зміни параметра побудови кривої t, де кроки $T\Delta t^k$ не повторюються та $T\Delta t^k \le \max \Delta t$.

Крок 3. Виконується приховування кожного a^j секретного повідомлення в криву D_j, $j = \overline{1,m}$, шляхом розбиття її на послідовність сегментів $D_j^* = D_{V_1}^0 \cup D_{V_1}^1 \cup ... \cup D_{V_1}^w$, де w – індекс послідовності створених сегментів кривої D_j^*, $w \in N$ (перед приховуванням $w = 0$ і $D_{V_1}^0 = D_j$), при різних значеннях параметра t:

3.1. Приховування кожного елементу a_i^l ($a^j = \left\{a_1^l, a_2^l,..., a_i^l ..., a_z^l\right\}$, $i = \overline{1,z}$) послідовності a^j при певному значенні t_i ($t_i = t_{i-1} + T\Delta t^k$, де t_0 – довільне початкове значення, $0 \le t_0 < 1 - z \cdot \max \Delta t$, $T\Delta t^k$ відповідає кроку зміни параметра t для приховування a_i^l) відбувається шляхом розбиття кривої $D_{V_1}^w$

на два сегмента $D_{V_1}^w$ і $D_{V_1}^{w+1}$ в точці t_i. Координати опорних точок отриманих сегментів розраховуються із обраною точністю V_4. Подальше внесення наступних елементів a_{i+1}^l шаблону з послідовності a^j буде відбуватися при наступному значенні точки розбиття t_{i+1} в отриманий другий сегмент $D_{V_1}^{w+1}$ Кожне розбиття кривої збільшує кількості кривих в послідовності сегментів на один ($w = w+1$).

3.2. Після приховування послідовності a^j у D_j криву, отримана послідовність сегментів $D_j^* = D_{V_1}^0 \cup D_{V_1}^1 \cup ... \cup D_{V_1}^w$ записується до стеганоконтейнера замість D_j кривої.

На основі визначених параметрів приховування та розроблених методів вбудовування даних розроблено структурну модель процесу прихованої передачі інформації резервним каналом зв'язку, що дозволяє формувати множину стеганоконтейнерів, стійких до афінних перетворень.

Третій розділ присвячений розробці алгоритмів приховування інформації у криві Без'є векторних зображень.

Для роботи з векторними зображеннями використовуються спеціальні графічні пакети: Adobe Illustrator, CorelDRAW, AutoCAD, KOMPAS-3D, Autodesk 3ds Max, Inkscape. Вони підтримують велику кількість форматів представлення даних: AI, CDR, CDW, CDT, DWG, DXF, WMF, FLA, FH, SVG, SWF, 3DM та інші. В структурі кожного векторного формату використовуються різні типи точково-заданих кривих. Для приховування інформації у векторні зображення слід використовувати найпоширеніші криві, що підтримуються більшістю графічними пакетами, а саме криві Без'є.

Крива Без'є – це параметрична крива, яка задається наступним рівнянням:

$$B(t) = \sum_{i=0}^{n} b_{i,n}(t) P_i \ , \ t = t + \Delta t \ , \ t \in [0,1],$$

де P_i – опорні точки, $i \in \overline{0,n}$, i – індекс опорних точок, n – ступінь поліноміальної кривої і кількості її сегментів, $n+1$ – кількість опорних точок, t – параметр побудови кривої, Δt – крок зміни параметра t, $b_{i,n}(t)$ – поліноми Бернштейна. Криві Без'є володіють необхідними властивостями для приховування інформації: будь-яка крива Без'є є афінно-інваріанта відносно афінних перетворень; будь-яку криву Без'є можна розбити та подати у вигляді довільної сукупності сегментів.

На основі методів побітового та шаблонного приховування інформації і властивостей кривих Без'є реалізовано алгоритми StegoBIT та StegoTEMPL, що дозволяють вбудовувати дані у криві Без'є третього ступеня. Псевдокоди процедури вбудовування інформації за даними алгоритмами представлено на рис. 1 та 2 відповідно.

Під операцією $SplitMessage(x, y)$ мається на увазі побітове розбиття вхідного повідомлення x на частини розмірністю y біт. Операція

$SelectImage(x, y, z)$ виконує відбір допустимих контейнерів з множини x необхідних для вбудовування y частин прихованого повідомлення, в структурі яких містяться криві Без'є ступеня z. Операція $SelectCurves(x, y, z, h)$ визначає з множини зображень x кількість кривих Без'є ступеня z необхідних для вбудовування y частин прихованого повідомлення, що відповідають мінімальній допустимій відстані h між опорними точками.

Input: Секретне повідомлення $a = \{a_i\}$, $a_i \in \{0,1\}$, $i = \overline{1,h}$, $h \in N$;

множина векторних зображень (контейнерів) $I = \{I_b\}$, $b \in N$;

множина стеганоключів $T = \{\Delta t^u\}$, $\Delta t^u \in (0,1)$, $u \in N$;

множина параметрів $V = \{V_i\}$, $i = \overline{1,4}$, $V_i \in N$, $V_1 = 3$;

значення біту при якому буде відбуватись поділ кривих Без'є Q, $Q \in \{0,1\}$.

Output: множина стеганоконтейнерів $S = \{S_x\}$, $x \in N$.

1. $\{a^j\} = SplitMessage(a, V_3)$, $a^j = \{a_1^j, ..., a_{V_3}^j\}$, $a_i^j \in \{0,1\}$, $i = \overline{1,V_3}$, $j = \overline{1,m}$, $m = \lceil h/V_3 \rceil$;
2. $S = SelectImage(I, m, V_1)$, $S = \{S_x\}$, $x \in N$, $x \le m$, $m = \lceil h/V_3 \rceil$;
3. $D = SelectCurves(S, m, V_1, V_2)$, $D = \{D_j\}$, $j = \overline{1,m}$, $m = \lceil h/V_3 \rceil$;
2. $For\ (j = 1; j \le m; j++)$
2.1. $\Delta t^j = SelectKey(T, V_3)$, $\Delta t^j < 1/V_3$;
2.2. $w = 0$; $t = 0$; $D_{V_1}^w = D_j$;
2.3. $For\ (i = 1; i \le V_3; i++)$
2.3.1. $t = t + \Delta t^j$;
2.3.2. $if\ (a_i^j == Q)$
2.3.2.1. $\{P_e\} = GetPoints(D_{V_1}^w)$, $e = \overline{0,3}$;
2.3.2.2. $P_0^1 = (1-t) \cdot P_0 + t \cdot P_1$;
2.3.2.3. $P_1^1 = (1-t) \cdot P_1 + t \cdot P_2$;
2.3.2.4. $P_2^1 = (1-t) \cdot P_2 + t \cdot P_3$;
2.3.2.5. $P_0^2 = (1-t) \cdot P_0^1 + t \cdot P_1^1$;
2.3.2.6. $P_1^2 = (1-t) \cdot P_1^1 + t \cdot P_2^1$;
2.3.2.7. $P_0^3 = (1-t) \cdot P_0^2 + t \cdot P_1^2$;
2.3.2.8. $D_{V_1}^w = CreateCurve(P_0, P_0^1, P_0^2, P_0^3)$;
2.3.2.9. $D_{V_1}^{w+1} = CreateCurve(P_0^3, P_1^2, P_2^1, P_3)$;
2.3.2.10. $w = w + 1$;
2.4. $D_j = ReplaceCurve(S, D_j, \{D_{V_1}^i\})$, $i = \overline{0,w}$;
3. $Return\ S$;

Рис. 1. Псевдокод процедури приховування інформації алгоритму StegoBIT

Операція $SelectKey(x, y)$ використовується для визначення з множини x допустимих стеганоключів Δt^j, необхідних для вбудовування частин приховуваної інформації розмірності y. Операція $GetPoints(x)$ використовується для одержання координат опорних точок кривої x. Операція $CreateCurve(x, y, z, h)$ використовується для побудови кривої Без'є за координатами опорних точок x, y, z та h. Операція $ReplaceCurve(x, y, z)$ виконує заміну в зображеннях x початкових кривих y на сукупності сегментів z, що містять приховану інформацію.

Input: Секретне повідомлення $a = \{a_i\}$, $a_i \in \{0,1\}$, $i = \overline{1,h}$, $h \in N$;

множина векторних зображень (контейнерів) $I = \{I_b\}$, $b \in N$;

множина параметрів $V = \{V_i\}$, $i = \overline{1,4}$, $V_i \in N$, $V_1 = 3$;

таблиця шаблону $TV_l[i]$, що виступатиме стеганоключем, $i = \overline{0, 2^l - 1}$, $TV_l[i] \in (0,\ l/V_3)$, $l \in N$, $c = V_3 / l$.

Output: множина стеганоконтейнерів $S = \{S_x\}$, $x \in N$.

1. $\{a^j\} = SplitMessage(a, V_3)$, $a^j = \{a_1^j, ..., a_{V_3}^j\}$, $a_i^j \in \{0,1\}$, $i = \overline{1,V_3}$, $j = \overline{1,m}$, $m = \lceil h/V_3 \rceil$;
2. $S = SelectImage(I, m, V_1)$, $S = \{S_x\}$, $x \in N$, $x \le m$, $m = \lceil h/V_3 \rceil$;
3. $D = SelectCurves(S, m, V_1, V_2)$, $D = \{D_j\}$, $j = \overline{1,m}$, $m = \lceil h/V_3 \rceil$;
2. $For\ (j = 1;\ j \le m;\ j++)$
2.1. $\{A_1^j\} = SplitMessage(a^j, l)$, $A_1^j \in \{0,1\}^l$, $i = \overline{1,c}$;
2.2. $w = 0$; $t = 0$; $D_{V_1}^w = D_j$;
2.3. $For\ (i = 1; i \le c; i++)$
2.3.1. $t = t + TV_l[A_1^j]$;
2.3.2. $\{P_e\} = GetPoints(D_{V_1}^w)$, $e = \overline{0,3}$;
2.3.3. $P_0^1 = (1-t) \cdot P_0 + t \cdot P_1$;
2.3.4. $P_1^1 = (1-t) \cdot P_1 + t \cdot P_2$;
2.3.5. $P_2^1 = (1-t) \cdot P_2 + t \cdot P_3$;
2.3.6. $P_0^2 = (1-t) \cdot P_0^1 + t \cdot P_1^1$;
2.3.7. $P_1^2 = (1-t) \cdot P_1^1 + t \cdot P_2^1$;
2.3.8.. $P_0^3 = (1-t) \cdot P_0^2 + t \cdot P_1^2$;
2.3.9. $D_{V_1}^w = CreateCurve(P_0, P_0^1, P_0^2, P_0^3)$;
2.3.10. $D_{V_1}^{w+1} = CreateCurve(P_0^3, P_1^2, P_2^1, P_3)$;
2.3.11. $w = w + 1$;
2.4. $D_j = ReplaceCurve(S, D_j, \{D_{V_1}^i\})$, $i = \overline{0,w}$;
3. $Return\ S$;

Рис. 2. Псевдокод процедури приховування інформації алгоритму StegoTEMPL

Вилучення даних виконується при відтворені початкових кривих D_j з сукупностей сегментів D_j^*, $j=\overline{1,m}$. Відтворення кривої D_j відбувається при поступовому об'єднанні двох останніх кривих $D_{V_1}^{w-1}$ та $D_{V_1}^{w}$ з послідовності сегментів D_j^* при певному значенні параметра t ($0<t\le 1$), що зменшується за StegoBIT на визначений стеганоключ Δt^j, $j=\overline{1,m}$ та за StegoTEMPL на певний крок TV_l^k з таблиці шаблонів, $k=\overline{1,2^l}$. Об'єднання двох кривих призводить до зменшення кількості сегментів послідовності D_j^* на один ($w=w-1$).

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням розроблених алгоритмів. Розроблено методику проведення експериментального дослідження, визначено його мету, завдання, вхідні параметри та послідовність необхідних дій.

Для проведення експерименту запропоновані алгоритми StegoBIT та StegoTEMPL були програмно реалізовані (розроблено ПЗ StegoInSVG-Bitwise і StegoInSVG-Template).

В 30 контейнерів формату SVG вбудовувалась інформація розміром 2^{10} біт при використанні різних стеганоключах та параметрах приховування: $V_1=3$ (кубічні криві), $V_2\ge 1$, $V_3\in\{40,60,80\}$ біт, $V_4=\{5,6\}$, $V_5\in\{2\cdot 10^{-5},4\cdot 10^{-5}\}$ (для StegoBIT та StegoTEMPL), $l=4$, $k=16$ (для StegoTEMPL). Всього проведено 36 експериментів, в кожному з яких визначено коефіцієнт візуального спотворення, зміну розмірів стеганоконтейнерів, швидкісні характеристики та стійкість розроблених алгоритмів до афінних перетворень. Середні результати одержаних результатів представлені в табл. 1, 2.

Таблиця 1

Середні швидкісні характеристики розроблених алгоритмів

Алгоритм приховування	Процесор	Розмір прихованої інформації, біт	Час вбудов., с	Швидкість вбудов., біт/с	Час вилуч., с	Швидкість вилуч., біт/с
StegoBIT	1	1024	0,1758	5824,80	1,4983	683,44
	2		0,1318	7769,35	1,3127	780,07
	3		0,3189	3211,04	1,3843	739,72
StegoTEMPL	1		0,1259	8133,44	0,8154	1255,83
	2		0,2899	3532,25	1,2149	842,87
	3		0,1781	5749,58	1,4035	729,60
1 – AMD A10-4600M, 2.3 GHz; 2 – AMD Phenom(tm) II X4 945 Processor, 3.00 GHz; 3 – Intel® Pentium® quad core processon N3540, up to 2.66 GHz.						

Таблиця 2

Порівняння середніх значень розмірів одержаних стеганоконтейнерів

Алгоритм приховування	Розмір прихованої інформації, біт	Розмір контейнера «до», Кб	Розмір контейнера «після», Кб	Збільшення розміру конт. «після» відносно конт. «до», раз
StegoBIT	1024	26,81	55,81	2,08
StegoTEMPL			43,13	1,61

Середній коефіцієнт візуального спотворення одержаних стеганоконтейнерів відносно контейнерів-оригіналів склав за StegoBIT – 0,11%, а за StegoTEMPL – 0,1%.

За наступною формулою наведено загальний принцип проведення експериментального дослідження, щодо перевірки стійкості запропонованих алгоритмів до афінних та майже афінних перетворень:

$$S_k = F\left(S_{k-1}, \alpha_{1,1}^k, \alpha_{1,2}^k, \alpha_{2,1}^k, \alpha_{2,2}^k, \beta_1^k, \beta_2^k, \varepsilon_1^k, \varepsilon_2^k, \varepsilon_3^k, \varepsilon_4^k, \varepsilon_5^k, \varepsilon_6^k\right),\ k = k+1, \quad (1)$$

де F – афінне перетворення, S_0 – початковий стеганоконтейнер, $\alpha_{1,1}^k, \alpha_{1,2}^k, \alpha_{2,1}^k, \alpha_{2,2}^k, \beta_1^k, \beta_2^k, \varepsilon_1^k, \varepsilon_2^k, \varepsilon_3^k, \varepsilon_4^k, \varepsilon_5^k, \varepsilon_6^k \in R$, $k \in N$. В залежності від підібраних коефіцієнтів $\alpha_{1,1}^k$, $\alpha_{1,2}^k$, $\alpha_{2,1}^k$, $\alpha_{2,2}^k$, β_1^k, β_2^k, ε_1^k, ε_2^k, ε_3^k, ε_4^k, ε_5^k, ε_6^k виконувалось перетворення перенесення, повороту, майже повороту, зсуву і масштабування. Для кожного S_k, $k > 0$ виконувалося вилучення прихованих даних з обробленого стеганоконтейнера для його аналізу.

Накладання перетворення *перенесення* згідно (1) виконувалось до кожного стеганоконтейнера за наступними коефіцієнтами: $\alpha_{1,1}^k = \alpha_{1,2}^k = \alpha_{2,1}^k = \alpha_{2,2}^k = 0$, $\beta_1^k \in [-500, 500]$, $\beta_2^k \in [-500, 500]$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,100}$. Середні результати з кількості втраченої інформації при накладанні даного перетворення наведені на рис. 3.

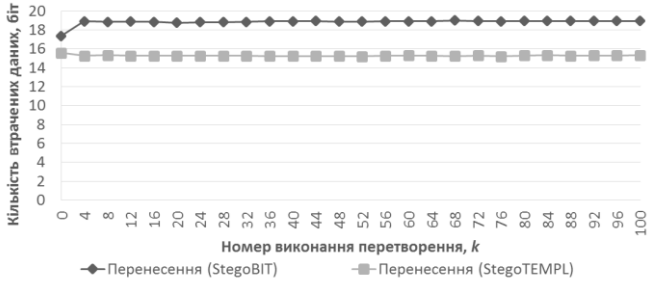

Рис. 3. Результати вилучення інформації з стеганоконтейнерів після виконання перетворень перенесення

Накладання перетворення *повороту* (а) та *майже повороту* (б) навколо точки $(0,0,1)$ згідно (1) виконувалось до кожного стеганоконтейнера за наступними коефіцієнтами: а) $\alpha_{1,1}^k = \cos\theta$, $\alpha_{1,2}^k = -\sin\theta$, $\alpha_{2,1}^k = \sin\theta$, $\alpha_{2,2}^k = -\cos\theta$, $\theta = 1$, $\beta_1^k = \beta_2^k = 0$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,360}$; б) $\alpha_{1,1}^k = \cos\theta$, $\alpha_{1,2}^k = -\sin\theta$, $\alpha_{2,1}^k = \sin\theta$, $\alpha_{2,2}^k = -\cos\theta$, $\theta = 1$, $\beta_1^k = \beta_2^k = 0$, $\varepsilon_1^k = \varepsilon_4^k = \varepsilon_6^k = -0,0001$, $\varepsilon_2^k = \varepsilon_3^k = \varepsilon_5^k = 0,0001$, $k = \overline{1,360}$.

Середні результати з кількості втраченої інформації при накладанні даних перетворень наведені на рис. 4.

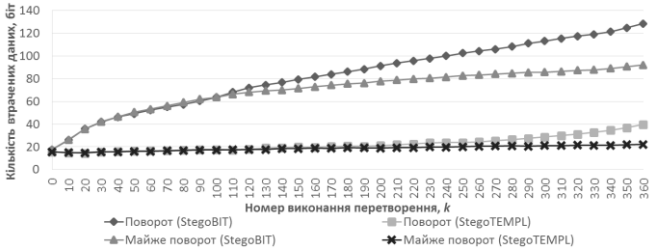

Рис. 4. Результати вилучення інформації з стеганоконтейнерів після виконання перетворень повороту та майже повороту

Накладання перетворення *зсуву за віссю абсцис* (а) та *ординат* (б) згідно (1) виконувалось до кожного стеганоконтейнера за наступними коефіцієнтами: а) $\alpha_{1,1}^k = \alpha_{2,2}^k = 1$, $\alpha_{1,2}^k = 0,01$, $\alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,100}$; б) $\alpha_{1,1}^k = \alpha_{2,2}^k = 1$, $\alpha_{1,2}^k = \beta_1^k = \beta_2^k = 0$, $\alpha_{2,1}^k = 0,01$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = 0$, $\varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,100}$. Середні результати з кількості втраченої інформації при накладанні даних перетворень наведені на рис. 5.

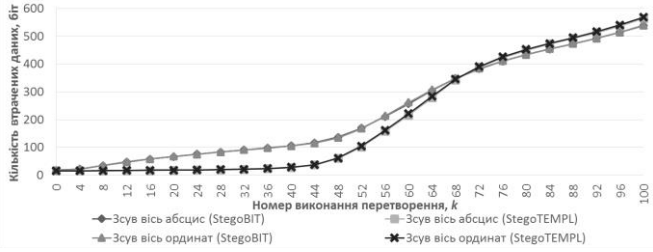

Рис. 5. Результати вилучення інформації з стеганоконтейнерів після виконання перетворень зсуву

Накладання перетворень *пропорційного* (а) та *непропорційного масштабування за віссю абсцис* (б) і *ординат* (в) згідно (1) виконувалось шляхом стискання/розтягування кожного стеганоконтейнера за наступними коефіцієнтами: а) стиснення – $\alpha_{1,1}^k = \alpha_{2,2}^k = 0,99$, $\alpha_{1,2}^k = \alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,99}$; розширення – $\alpha_{1,1}^k = \alpha_{2,2}^k = 1,01$, $\alpha_{1,2}^k = \alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,100}$; б) стиснення – $\alpha_{1,1}^k = 0,99$, $\alpha_{1,2}^k = \alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\alpha_{2,2}^k = 1$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,99}$; розширення – $\alpha_{1,1}^k = 1,01$, $\alpha_{1,2}^k = \alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\alpha_{2,2}^k = 1$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,100}$; в) стиснення – $\alpha_{1,1}^k = 1$, $\alpha_{1,2}^k = \alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\alpha_{2,2}^k = 0,99$, $\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,99}$; розширення – $\alpha_{1,1}^k = 1$, $\alpha_{1,2}^k = \alpha_{2,1}^k = \beta_1^k = \beta_2^k = 0$, $\alpha_{2,2}^k = 1,01$,

$\varepsilon_1^k = \varepsilon_2^k = \varepsilon_3^k = \varepsilon_4^k = \varepsilon_5^k = \varepsilon_6^k = 0$, $k = \overline{1,100}$. Середні результати з кількості втраченої інформації при стисненні та розширенні векторних зображень наведені на рис. 6, 7 відповідно.

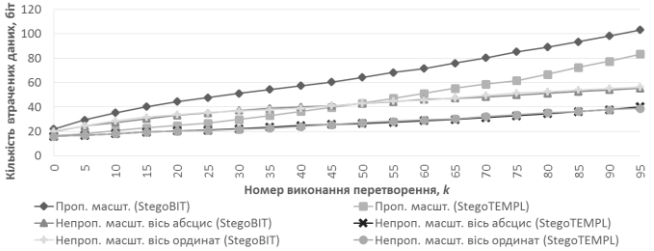

Рис. 6. Результати вилучення інформації з стиснутих стеганоконтейнерів після виконання перетворень масштабування

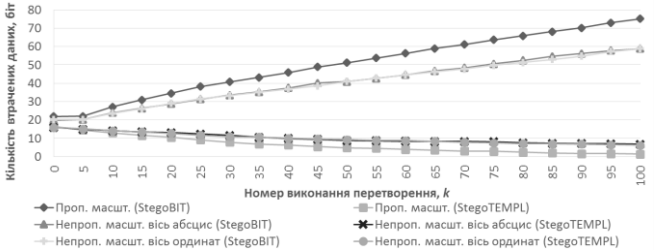

Рис. 7. Результати вилучення інформації з розширених стеганоконтейнерів після виконання перетворень масштабування

Розроблені алгоритми були порівняні з методом Карпінцева-Яремчука на стійкість до афінних перетворень, середні коефіцієнти втрат яких представлені в табл. 3.

Таблиця 3

Середні коефіцієнти втрат до афінних та майже афінних перетворень

	Перенесення, %	Поворот, %	Майже поворот, %	Зсув, %	Масштабування, %
Метод Карпінцева-Яремчука	20,3	48,68	48,38	29,62	38,04
StegoBIT	0,3	0,53	0,55	1,69	0,87
StegoTEMPL	3,47	5,41	4,64	7,27	4,04

Згідно результатів дослідження можна зробити висновок, що розроблені алгоритми StegoBIT і StegoTEMPL підвищують стійкість до афінних перетворень у порівнянні із методом Карпінцева-Яремчука. Однак, при накладанні перетворень повороту, майже повороту, зсуву і масштабування утворюється похибка округлення нових координат опорних точок векторних об'єктів, що впливає на коректність вилучення інформації. При зменшенні кількості приховуваної інформації в одну криву Без'є та при оптимальному виборі параметрів приховування можна забезпечити більшу стійкість до афінних перетворень розробленими алгоритмами.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи, та лістинги (коди) ПЗ (StegoInSVG-Bitwise, StegoInSVG-Template).

ВИСНОВКИ

У дисертаційній роботі розв'язано актуальне наукове завдання щодо розробки нових методів приховування даних у векторні зображення для підвищення стійкості стеганографічного захисту інформації до активних атак на основі афінних перетворень.

В ході розв'язання поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено аналіз сучасних методів приховування інформації, що використовують у якості контейнера векторні зображення. Проведено порівняння стійкості даних методів до афінних перетворень, яке показало недостатню стійкість розглядуваних стеганографічних методів відносно даних атак. З огляду на це, постає необхідність розробки нових методів приховування інформації у векторні зображення, стійких до активних атак на основі афінних перетворень.
2. Формалізовано вимоги до вибору контейнера, визначено множину параметрів приховування інформації у векторні зображення, які, за рахунок врахування особливостей побудови векторних зображень та стеганографічних перетворень, дозволяють впливати на вибір допустимих контейнерів та на процес приховування даних у точково-задані криві.
3. Запропоновано метод побітового приховування інформації у точково-задані криві векторних зображень, який дозволяє приховувати дані шляхом поділу кривих на сукупності сегментів, не призводячи при цьому до погіршення якості самого зображення з забезпеченням стійкості до активних атак на основі афінних перетворень.
4. Запропоновано метод шаблонного приховування інформації у точково-задані криві векторних зображень з наперед визначеною таблицею співвідношень різних значень елементів шаблону різним крокам побудови точково-заданих кривих, який дозволяє за один поділ кривої на сегменти здійснювати приховування цілого блоку біт з забезпеченням стійкості до активних атак на основі афінних перетворень.
5. Запропоновано структурну модель процесу прихованої передачі інформації резервним каналом зв'язку, що дозволяє формувати множину стеганоконтейнерів, стійких до афінних перетворень.
6. Розроблено алгоритми StegoBIT та StegoTEMPL, які підвищуються стійкість до атак на основі афінних перетворень. У порівняні з методом Карпінцева-Яремчука середній коефіцієнт втрат інформації зменшився: до атаки перенесення на 16,83%, до атаки повороту на 43,27%, до майже повороту на 43,74%, до атаки зсуву на 22,35% та до атаки масштабування на 34%. Максимальний коефіцієнт втрат при багаторазовому застосуванні афінних перетворень до стеганоконтейнерів склав: за алгоритмом StegoBIT до атаки перенесення 1,85%, повороту 12,54%, майже повороту 8,98%, масштабування 7,19% та зсуву 52,61%; за алгоритмом StegoTEMPL до атаки перенесення 1,52%, повороту 3,87%, майже повороту 2,16%, масштабування 5,29% та зсуву 55,33%.

7. Розроблено методику проведення експериментального дослідження, яка дозволяє дослідити розроблені. На основі запропонованої методики та алгоритмів розроблено програмні засоби, що дозволило верифікувати отримані результати. Упровадження зазначених розробок та їх експериментальне дослідження підтвердило достовірність теоретичних гіпотез і висновків дисертаційної роботи.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. *Кінзерявий О.М.* Метод шаблонного приховування даних у векторні зображення / О.М. Кінзерявий, В.Ю. Ковтун, О.Л. Стокіпний // Захист інформації. — 2014. — Т.16, №2. — С. 139-146.
2. *Кінзерявий О.М.* Експериментальне дослідження стійкості методу побітового приховування даних відносно атак на основі афінних перетворень / О.М. Кінзерявий, В.Ю. Ковтун // Захист інформації. — 2014. — Т.16, №4. — С. 304-311.
3. *Кінзерявий О.М.* Стеганографічний метод приховування даних у векторних зображеннях / О.М. Кінзерявий, В.Ю. Ковтун, С.О. Гнатюк, В.М. Кінзерявий // Вісник Інженерної академії України. — 2013. — №3-4. — С. 66-68.
4. *Кінзерявий О.М.* Експериментальне дослідження методу побітового приховування даних у векторні зображення / О.М. Кінзерявий, В.Ю. Ковтун // Безпека інформації. — 2014. — Т.20, №1. — С. 66-70.
5. *Кінзерявий О.М.* Систематизація сучасних методів комп'ютерної стеганографії / О.М. Кінзерявий, В.Ю. Ковтун, С.О. Гнатюк // Безпека інформації. — 2013. — Т.19, №3. — С. 209-217.
6. *Кінзерявий О.М.* Блоковий симетричний криптоалгоритм «LUNA» / В.М. Кінзерявий, В.П. Кваснiков, С.О. Гнатюк, О.М. Кінзерявий // Захист інформації. — 2011. — Т.13, №3. — С. 77-86.
7. *Кінзерявий О.М.* Нові ефективні алгоритми шифрування інформації / В.М. Кінзерявий, С.О. Гнатюк, О.М. Кінзерявий // Захист інформації. — 2012. — Т.14, №4. — С. 132-142.
8. *Кінзерявий О.М.* Стеганографічний метод приховування даних у векторних зображеннях / О.М. Кінзерявий // Інфокомунікації - сучасність та майбутнє : третя міжнародна науково-практична конференція молодих вчених — О., 2013. — Ч.3. — С. 160-162.
9. *Кінзерявий О.М.* Побітове приховування даних у SVG зображення на основі кривих Без'є / О.М. Кінзерявий // Безпека інформаційних технологій : четверта міжнародна науково-технічна конференція. — К., 2014. — С. 53-54.
10. *Кінзерявий О.М.* Шаблонний метод приховування даних у векторні зображення на основі розбиття кривих Без'є / О.М. Кінзерявий // Захист інформації і безпека інформаційних систем : третя міжнародна науково-технічна конференція. — Л., 2014. — С. 86-87.
11. *Кінзерявий О.М.* Побітовий метод приховування у векторні зображення стійкий до афінних перетворень / О.М. Кінзерявий, Б.С. Дорошенко // Механізми управління безпекою підприємств в сучасних умовах господарювання. — К., 2013. — С. 91-94.
12. *Kinzeryavyy O.* Method of template hiding data in vector images structure / O. Kinzeryavyy, V. Kinzeryavyy // The sixth world congress «Aviation in the XXI-st century». — K., 2014. — V.1. — C. 568-572.

13. *Кінзерявий О.М.* Експериментальне дослідження стійкості методу побітового приховування даних у векторні зображення відносно афінних перетворень / О.М. Кінзерявий, В.М. Кінзерявий // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації. — К., 2015. — С. 48-52.

14. *Кінзерявий О.М.* Дослідження стійкості методу шаблонного приховування інформації у векторні зображення / В.Ю. Ковтун, О.М. Кінзерявий // Безпека інформації у інформаційно-телекомунікаційних системах : сімнадцята міжнародна науково-практична конференція. — К., 2015. — С. 54-55.

АНОТАЦІЯ

Кінзерявий О. М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Національний авіаційний університет, Київ, 2015.

У дисертаційній роботі розв'язано актуальне наукове завдання щодо розробки нових стеганографічних методів приховування інформації у векторні зображення для підвищення стійкості до активних атак на основі афінних перетворень. Формалізовано вимоги щодо вибору контейнера і визначено параметри приховування інформації у векторні зображення. Розроблено метод побітового приховування інформації у точково-задані криві векторних зображень, який, за рахунок розбиття кривих на сукупності сегментів з фіксованим кроком зміни параметра побудови кривих, дозволяє вбудовувати один біт секретного повідомлення за один поділ кривої, забезпечуючи при цьому стійкість до афінних перетворень. Також, розроблено метод шаблонного приховування інформації у точково-задані криві векторних зображень, який, за рахунок таблиці співвідношень значень елементів шаблону різним крокам зміни параметра побудови кривих, дозволяє вбудовувати за один поділ кривої цілий блок даних, при цьому забезпечуючи стійкість до афінних перетворень. На основі запропонованих методів розроблено нові стеганографічні алгоритми StegoBIT і StegoTEMPL, які дозволяють приховувати інформацію у криві Без'є третього ступеня та підвищити стійкість до афінних перетворень. На основі даних алгоритмів розроблено програмне забезпечення, що може бути використане для підвищення ефективності стеганографічного захисту інформації.

Ключові слова: стеганографічний захист інформації, векторні зображення, метод побітового приховування даних, метод шаблонного приховування даних, криві Без'є, афінні перетворення.

ABSTRACT

Kinzeryavyy O.M. Steganographic methods of hiding data in vector images that are resisted to active attacks based on affine transformations. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 - information security systems. – National Aviation University, Kyiv, 2015.

Dissertation is devoted to solve the actual scientific task of developing new steganographic methods for hiding information in vector images to increase resistance to active attacks, based on affine transformations. The requirements of the container selection are formalized and the parameters of hiding information in vector images are defined. It is developed the method of bitwise information hiding in point-set curves vector images, which, by breaking curves into the aggregate segments with fixed step of change the parameter of curves construction, allows to embed one bit of the secret message per one division of the curve, while providing resistance to affine transformations. Also, it is developed the method of template information hiding in a point-set curves of vector images, which, due to the correlation table of values of template element with different steps of the curve construction parameter, allows embedding a block of data for a single division of the curve, thus providing resistance to affine transformations. The new steganographic algorithms StegoBIT and StegoTEMPL, which allow hiding information in Bezier curves of the third degree, while providing resistance to affine transformations, are developed on the basis of the proposed methods. The software that can be used to improve the stenographic information security is developed on the basis of the proposed algorithms.

Keywords: steganographic data protection, vector images, bitwise method of data hiding, template method of data hiding, Bezier curves, affine transformation.

АННОТАЦИЯ

Кинзерявый А. Н. Стеганографические методы сокрытия данных в векторные изображения, устойчивые к активным атакам на основе аффинных преобразований. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Национальный авиационный университет, Киев, 2015.

В диссертационной работе решена актуальная научная задача по разработке новых стеганографических методов сокрытия информации в векторные изображения для повышения стойкости к активным атакам на основе аффинных преобразований.

Проведен анализ современных стеганографических методов сокрытия информации в векторные изображения. Определены возможные виды активных атак применяемых к векторным изображениям, направленных на уничтожение секретной информации. Проведено сравнение устойчивости рассмотренных методов к данным видам атак, что позволило обосновать необходимость разработки новых более эффективных стеганографических методов сокрытия информации в векторные изображения, необходимых для реализации скрытого канала связи через глобальную сеть Интернет.

В работе определено множество параметров сокрытия данных в векторные изображения, которые, за счет учета особенностей построения векторных изображений (степени точечно-заданных кривых, их допустимой длины относительно опорных точек) и стеганографических преобразований (точность координат опорных точек, допустимой погрешности округления при изъятии данных и количества информации, что скрывается в одну кривую), позволяют

формализовать требования к выбору контейнеров и влиять на процесс сокрытия информации в точечно-заданные кривые. Разработан метод побитового сокрытия информации в точечно-заданные кривые векторных изображений, который, за счет влияния последовательности данных на процесс сегментации кривых с фиксированным шагом изменения параметра построения заданных кривых (разбиение кривых на сегменты происходит лишь при встраивании нулевого/единичного бита скрываемой последовательности данных), обеспечивает высокое быстродействие сокрытия, изъятие секретного сообщения и повышает устойчивость к активным атакам на основе аффинных преобразований. Разработан метод шаблонного сокрытия информации в точечно-заданные кривые векторных изображений, который, за счет влияния последовательности данных на процесс сегментации кривых согласно определенной таблицы соотношений значений элементов шаблона к различным шагам изменения параметра построения заданных кривых (при разбивке кривой на два сегмента встраивается блок данных), что, в отличие от побитового метода, позволяет уменьшить размеры стеганоконтейнеров, повысить скорость встраивания и устойчивость к активным атакам на основе аффинных преобразований.

На основе предложенных методов разработаны два новых стеганографические алгоритмы StegoBIT и StegoTEMPL. Предложенные алгоритмы позволяют скрывать информацию в кривые Безье третьей степени путем их разделения на совокупности сегментов по алгоритму де Кастельжо и повышают стойкость к аффинным преобразованиям.

Для практического исследования алгоритмы StegoBIT и StegoTEMPL были программно реализованы в виде программ StegoInSVG-Bitwise и StegoInSVG-Template соответственно, что позволило осуществлять встраивания информации в кривые Безье SVG изображений. На основе выбранной методики проведения экспериментального исследования были исследованы скоростные характеристики предложенных алгоритмов, их устойчивость к аффинным преобразованиям, коэффициент искажения и размеры стеганоконтейнеров при различных значениях стеганоключей и параметров сокрытия, что позволило оценить их эффективность, дать рекомендации и верифицировать предложенные стеганографические средства защиты информации. Результаты диссертационной работы внедрены в учебном процессе кафедры безопасности информационных технологий Национального авиационного университета и в научно-технических разработках ООО «Сайфер ЛТД» и «Каскад Групп Украина». Внедрение и экспериментальные исследования предложенных разработок подтвердили достоверность теоретических гипотез и выводов диссертации.

Ключевые слова: стеганографическая защита информации, векторные изображения, метод побитового сокрытия данных, метод шаблонного сокрытия данных, кривые Безье, аффинные преобразования.