СТЕГАНОГРАФІЯ ТА СТЕГОАНАЛІЗ / STEGANOGRAPHY & STEGANALYSIS

СИСТЕМАТИЗАЦІЯ СУЧАСНИХ МЕТОДІВ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Владислав Ковтун, Сергій Гнатюк, Олексій Кінзерявий

Національний авіаційний університет, Україна

КОВТУН Владислав Юрійович, к.т.н.

Рік та місце народження: 1978 рік, м. Кіровоград, Україна.
Освіта: Харківський військовий університет, 2000 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2010 року.
Наукові інтереси: інформаційна безпека, швидкі арифметичні перетворення у полях Галуа, криптографічні системи з відкритим ключем, криптоаналіз криптографічних перетворень з відкритим ключем.
Публікації: більше 50 наукових публікацій, серед яких наукові статті у міжнародних та вітчизняних фахових журналах, патенти і т.д.
E-mail: vladislav.kovtun@gmail.com

ГНАТЮК Сергій Олександрович, к.т.н.

Рік та місце народження: 1985 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, квантова криптографія, кібербезпека цивільної авіації, розслідування інцидентів інформаційної безпеки.
Публікації: більш ніж 100 наукових публікацій, серед яких монографії, наукові статті у міжнародних та вітчизняних фахових журналах, патенти та авторські свідоцтва на програмні продукти.
E-mail: s.gnatyuk@nau.edu.ua

КІНЗЕРЯВИЙ Олексій Миколайович

Рік та місце народження: 1989 рік, м. Кам'янець-Подільський, Хмельницька область, Україна.
Освіта: Кам'янець-Подільський національний університет ім. Івана Огієнка, 2011 рік.
Посада: аспірант кафедри безпеки інформаційних технологій з 2011 року.
Наукові інтереси: інформаційна безпека, криптографія, стеганографія.
Публікації: більш ніж 15 наукових публікацій, серед яких наукові статті, тези доповідей та авторські свідоцтва на програмні продукти.
E-mail: oleksiykinzeryavyy@gmail.com

Анотація. *Стеганографія є напрямком захисту інформації, що дозволяє організувати безпечний канал обміну даних за рахунок приховування факту існування приховуваного повідомлення. Останнім часом з'явилось досить багато методів комп'ютерної стеганографії, а їх систематизація залишалась актуальною науковою задачею. У зв'язку з цим, у статті проведено систематизацію сучасних методів комп'ютерної стеганографії. Визначено загально можливі місця приховування даних в комп'ютерних системах та мережах. Представлено загальний опис методів приховування в мультимедійних (цифрових) об'єктах, де особлива увага надається методам приховування в зображеннях, над якими ведеться більшість стеганографічних досліджень. До методів комп'ютерної стеганографії віднесено приховування даних у поліграфічній діяльності таметоди на основі псевдоголографії.*

Ключові слова: *захист інформації, комп'ютерна стеганографія, методи приховування даних, файлово-системні методи, мережеві методи, мультимедійні об'єкти, цифрова стеганографія, ортогональні перетворення зображень.*

Вступ

З розвитком комп'ютерно-комунікаційних технологій та їх інтеграцією в усі сфери життя, надають нам безліч можливостей. Так за наявності комп'ютера, планшета, мобільного телефону чи навіть телевізора можна вільно підключатися до глобальної мережі Інтернет, спілкуватися з іншими людьми на різних континентах, оплачувати рахунки, зберігати та передавати дані тощо. Для захисту того всього потоку даних, що передається в комп'ютерно-комунікаційних мережах можуть використовуватись системи комп'ютерної стеганографії (КС). Під *системою КС* розуміється сукупність методів та засобів необхідних для реалізації прихованого каналу передачі інформації. Під приховуванням розуміється процес вкраплення секретної інформації в дані іншого інформаційного об'єкту. КС використовується для рішення таких ключових задач: захист конфіденційної інформації від несанкціонованого доступу; захист авторського права на інтелектуальну власність; подолання систем моніторингу і управління мережевими ресурсами; «камуфлювання» програмного забезпечення [2]. Однак КС методи постійно досліджуються та розвиваються, тому з часом виникає актуальна потреба в проведені їх перекласифікації і доповненні.

З огляду на це, **метою роботи** є систематизації існуючих методів комп'ютерної стеганографії, що можуть використовуються для організації прихованого каналу зв'язку.

Основна частина

В системах КС основним об'єктом досліджень, на основі якого реалізуються методи приховування, являється контейнер. Під контейнером розуміється цифровий об'єкт (зазвичай це файл), в який вбудовується секретна інформація. За місцем приховування інформації в контейнерах виділимо такі групи методів КС: *файлово-системні*, *мережеві протоколи*, *мультимедійні об'єкти*. Розглянемо більш детальніше кожну з цих груп.

Файлово-системні

До даної групи відносяться методи, що використовують незайняті, зарезервовані місця в структурних представленнях файлів та файлових систем, а саме [2, 5, 29]: *1) методи використання зарезервованих або прихованих полів форматів файлів*, що полягають в використанні частини структури даних файлу, що не використовуються або за замовченням заповнена нулями; *2) методи використання незадіяних місць на магнітних носіях*, що полягають в використанні тих місць дисків, що не використовуються (наприклад, запис інформації в нульову доріжку); *3) методи базуючі на особливостях роботи файлових систем*, що полягає в зберіганні секретної інформації на жорсткому диску в незайняте число кластерів, які займає певний файл. Наприклад, система *FAT32* для зберігання *1Kb* інформації виділяється *4Kb*, з яких *1Kb* потрібен для зберігання файлу, а інші *3Kb* можна використати для зберігання інформації. Основною перевагою даних методів є простота реалізації, однак їм характерна низька ступінь скритності, пропускної здатність та слабка продуктивність [1].

Мережеві протоколи

Ще одним місцем з спеціальними характеристиками та можливістю приховування інформації можуть служити мережеві протоколи (наприклад, на основі моделей *TCP/IP* та *OSI*). За допомогою яких можуть утворюватись приховані канали зв'язку, використовуючи для цього поля ідентифікації в пакетах протоколу *IP*, поле порядкового номера в сегментах протоколу управління передачею *TCP*, не використовуване місце в заголовках пакетів *TCP* (шість не використовуваних, зарезервованих біта) та *IP* (два зарезервованих біта), приховування в *ICMP*пакетах, шляхом підміни типу чи коду переданого повідомлення [5, 37-39].

Мультимедійні об'єкти

Найбільшої популярності та масового дослідження мають методи, що базуються на використанні мультимедійних об'єктів. Також в літературі їх називають цифровою стеганографією [1, 2, 4], що базується на приховуванні інформації в цифрових об'єктах. До мультимедійних об'єктів відносять: текст, звук, зображення та відео. Вони, як правило, мають аналогову природу, завдяки чого в них завжди присутній природній шум, що сприяє більшій непомітності прихованої інформації.

Текстові методи приховування

Особливо складними з мультимедійних об'єктів для приховування даних з багатьох причин являються текстові файли. Це пов'язано з тим, що текстовий файл може бути оброблений при підготовці на друк, добавляння додаткової букви або знака пунктуації в тексті можуть бути легко розпізнанні випадковим читачем. Така ситуація спричиняє відносний дефіцит у текстовому файлі надлишкової інформації, особливо порівняно з графічними або звуковими файлами. Виділяють три групи текстових методів приховування інформації [2, 5, 6, 19, 49]:

– методи довільного інтервалу;
– синтаксичні методи;
– семантичні методи.

Методи довільного інтервалу в певних випадках показують досить непогані результати. По-перше, зміна кількості пробілів у кінці текстового рядка не викликає істотних змін у значенні фрази або реченні. По-друге, середньостатистичний читач навряд чи помітить незначні модифікації вільного місця сторінки тексту. До методів даної групи належать: *1. Метод зміни інтервалів між реченнями*, який дозволяє вбудовувати в текст повідомлення шляхом розміщення одного або двох відступів після кожного символу завершення речення. Даний метод простий в використанні, однак має ряд недоліків: для вбудовування незначної кількості біт потрібен текст значного розміру; залежить від структури текстового контейнера (в деяких текстових контейнерах можуть бути відсутні знаки завершення рядка, деякі текстові редактори можуть автоматично добавляти після крапки відступи). 2. *Метод зміни кількості відступів у кінці текстових рядків*, що

полягає в додаванні відступів у кінець кожного текстового рядка. Кількість добавлених відступів залежить від значення вбудованого біта. Два відступи кодують один біт на рядок, чотири відступа – два біти і так далі. Такий підхід дозволяє істотно збільшити, порівняно з попереднім методом, кількість інформації, яку можна приховати в тексті аналогічного об'єму. Даний метод може бути застосований до будь-якого тексту, при чому зміни у форматі останнього будуть у достатній мірі непомітними. Недоліком даного методу є те, що деякі програми обробки тексту можуть ненавмисно видаляти додатково внесені відступи; *3) Застосування методу зміни кількості відступів між словами вирівняного по ширині тексту* дозволяє приховувати дані у вільних місцях тексту, вирівняного по ширині. При цьому біти даних вбудовуються шляхом керованого вибору позицій, в яких будуть розміщені додаткові відступи. Один відступ між словами інтерпретується як «0», а два відступи – як «1». В середньому метод дозволяє вбудовувати по кілька біт в один рядок. Недоліком є те, що через обмеження, які накладаються вирівнюванням тексту по ширині, не кожен відступ між словами може використовуватися для вбудовування даних.

Синтаксичні методи полягають в зміні пунктуації, структури та стилю тексту. Дані методи слід використовувати з ретельною обачністю, бо зміна пунктуації може призвести до зниження сприйняття тексту, надати протилежного змісту чи привернути увагу цензора.

Семантичні методи подібні до синтаксичним. Вони визначають два синоніма, які відповідають значенням приховуваних біт. Наприклад, слово «проте» може бути поставлено у відповідність до «0», а слово «однак» – до «1». Для використання даних методів необхідно наявність таблиці синонімів. Якщо слову відповідає велика кількість синонімів, то можливо одночасно приховувати більшу кількість бітів. Проблемою даних методів для вбудовування біта інформації може перешкоджати особливість значення слова.

Звукові методи приховування

Особливий розвиток отримали методи приховування в звукових файлах. Приховування даних у звукових сигналах є особливо перспективним, оскільки слухова система людини (ССЛ) працює в над широкому динамічному діапазоні. ССЛ сприймає більш ніж мільярд до одного в діапазоні потужності і більш ніж тисяча до одного в частотному діапазоні. Хоча ССЛ і має широкий динамічний діапазон, вона характеризується досить малим різницевим діапазоном. Як наслідок гучні звуки сприяють маскуванню тихих звуків. Крім того, ССЛ не спроможна розрізняти абсолютну фазу, розпізнаючи тільки відносну. Виділяють наступні методи приховування в звукові файли: *1) кодування найменшого значущого біта (НЗБ)* [2, 5, 6, 19, 28, 30, 49], здійснюється шляхом заміни НЗБ кожної точки здійснення вибірки, представленої в двійковій послідовності. Це дозволяє приховати значний об'єм інформації, однак головним недолік методу є слабка стійкість до сторонніх впливів. Вбудована інформація може бути зруйнована через наявність шумів в каналі, в результаті передискретизації вибірки тощо; *2) метод фазового кодування* [1, 2, 5, 6, 19, 26, 28, 49], що полягає в заміні фази вихідного звукового сегмента на опорну фазу, характер зміни якої відображає собою дані, які необхідно приховати. Для того щоб зберегти різницеву фазу між сегментами, фази останніх відповідним чином узгоджують. Істотна зміна співвідношення фаз між кожними частотними складовими призводить до значного розсіюванню фази. Тим не менш, до тих пір поки модифікація фази в достатній мірі мала, може бути досягнуто приховування, невідчутне на слух. Модифікація може бути малою по відношенню до звичайного спостерігача, однак фахівці по спектральному аналізу здатні виявити дані зміни; *3) метод розширення спектру* [1, 2, 5, 6, 19, 49], що реалізується в наступному: сигнал даних множиться на сигнали несучої і псевдовипадкової шумової послідовності, що характеризується широким частотним спектром. У результаті цього спектр даних розширюється на всю доступну смугу. Надалі послідовність розширених даних послаблюється та додається до вихідного сигналу як адитивний випадковий шум; *4) приховування даних з використанням ехо-сигналу* [1, 2, 5, 6, 19, 26, 28, 49], полягає в введення в звуковий файл додаткового ехо-сигналу. Дані ховаються при зміні трьох параметрів ехо-сигналу: початкової амплітуди, швидкості загасання і зсуву. Коли зсув (затримка) між первинним і ехо-сигналом зменшується, починаючи з деякого значення затримки, ССЛ стає нездатною виявити різницю між двома сигналами, а ехо-сигнал сприймається тільки як додатковий резонанс. Дане значення важко визначити точно, оскільки воно залежить від якості звукозапису, типу звуку та від слухача. У загальному випадку для більшості звуків і більшості слухачів змішування відбувається при затримці, приблизно однієї мілісекунди. Окрім зменшення часу затримки для забезпечення непомітності також можна змінювати рівні початкової амплітуди та час згасання, які б не перевищували поріг чутливості ССЛ. Для того щоб у первинний сигнал закодувати більше одного біта, сигнал розкладається на менші сегменти. Кожен сегмент при цьому розглядається як окремий сигнал і в нього може бути вбудований шляхом ехо-відображення один біт інформації; *5) приховування за допомогою вставки тонів* [6], ґрунтується на поганій чутності та нечіткості низьких тонів у присутності компонент значно вищого спектра.

Методи приховування в зображеннях

Найбільш перспективними та масово досліджуваними є методи приховування в зображеннях. Це пов’язано з тим, що вони здатні приховувати досить великі об’єми інформації та характер змін при вбудовуванні секретної інформації може бути непомітним для людського зору людини. Методи, що працюють з зображеннями діляться на: просторові, частотні, розширення спектру, статистичні, спотворення та

методи обробки зображень для поліграфічної діяльності.

Просторові методи характеризуються в заміні найменш значимої частини зображення бітами секретного повідомлення [2, 4, 5, 19, 25-28, 42, 49]. Для цього використовується колір представлення пікселів зображення. Колір пікселя представлений кольоровою моделлю *RGB* представляється в вигляді відповідної суми червоного, зеленого та синього кольору. Для реалізації даних методів непотрібно виконувати складних обрахунків та перетворень. До них належать: *1) метод заміни НЗБ*[3-6, 10, 28, 29], що полягає в зміні НЗБ пікселя на біти секретного повідомлення. Якщо розглядати зображення з 24-розрядною глибиною кольору, то в один піксель можна приховати 3 біти секретної інформації (по одному біту на червоний, зелений та синій колір). При цьому характер змін не буде помітний людському оку. Однак даний метод є нестійким до активних та пасивних атак, і може бути з легкістю виявлений та знищений. Існує ряд модифікацій, що покращує стійкість до певних видів атак, а саме: методи випадкового та псевдовипадкового інтервалу [5, 26, 28], метод попередньої фільтрації [6] та найостанніша розробка LSB Matching [3, 41]; *2) метод блочного приховування* [4, 5, 26, 28], що полягає в розбитті зображення на блоки, де в кожен блок заноситься 1 біт секретної інформації. Вибір блоку для внесення може визначатися за допомогою ключа. Чим більший блок за розмірами, тим менше спотворення самого зображення і його статистичних властивостей. Даний метод має низьку стійкість до спотворень, як і попередній. До блочного приховування можна віднести *метод Дармстедтера-Делейгла-Квісквотера-Макка* [5], за яким кожен біт вбудовується в окремий блок. Спочатку зображення розбивається на блоки 8×8 пікселів. Потім проводиться класифікація пікселів окремого блоку на зони з приблизно однорідним значеннями яскравості. Кожна зона розбивається на категорії відповідно до індивідуальної (псевдовипадкової) маски. Вбудовування біта відбувається в залежності від співвідношення між середніми значеннями категорій кожної зони шляхом модифікації значень яскравості кожної категорії в кожній зоні; *3) методи заміни палітри* [4, 5, 26, 28, 29], що полягають на наявності в зображенні таблиці кольорів, яка являє собою список пар індексів, що визначає відповідність індексу до відповідного кольору. Кожному пікселю зображення ставиться у відповідність певний індекс в таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення загального зображення, конфіденційна інформація може бути прихована шляхом перестановки індексів та кольорів у палітрі. Існує $N!$ різних способів перестановки N кольорової палітри, чого цілком достатньо для приховування невеликого повідомлення. Однак будь-яка атака пов'язана з зміною палітри знищує вбудоване повідомлення; *4) метод Куттера-Джордана-Боссена* [5, 19, 22, 42] полягає вбудовуванні інформації в контейнер використовуючи властивість зорової системи людини. Ця властивість полягає в меншій чутливості до змін яскравості синього кольору в порівнянні з червоним і зеленим. Саме тому секретні біти будуть записуватись тільки в синій колір, змінюючи при цьому яскравість пікселя; *5) Метод квантування* відбувається таким чином, що інформація приховується за рахунок коригування різницевого сигналу Δ_i. Стеганоключ представляє собою таблицю, яка кожному можливому значенню Δ_i ставить у відповідність визначений біт.

Просторові методи не забезпечують високої надійності і мають слабкий захист до пасивних та активних атак. Набагато кращу стійкість забезпечують *частотні методи* [2, 5, 19, 25, 26, 28, 49]. Вони базуються на використанні ортогональних перетворень (компресії) застосовуваних до зображень. Методи компресії діляться на стиснення без втрат та з ними. Стиснення без втрат є досить не ефективним та в більшості випадках можуть призводити до збільшення розміру зображення. В даних зображеннях краще використовувати методи приховування в просторовій області. Зовсім іншим випадком являються методи стиснення з втратами. Вони забезпечують досить гарні результати компресії. Основними моделями стиснення з втратами є дискретно косинусне перетворення (ДКП) [17, 24], вейвлет-перетворення (ВП) [47, 48, 50] та фрактальне стиснення зображень [2, 17]. На основі даних методів компресії базується ряд методів приховування даних.

ДКП використовується в зображеннях формату *JPEG*. Розглянемо більш детальніше як відбувається стиснення зображення за ДКП (рис. 1):

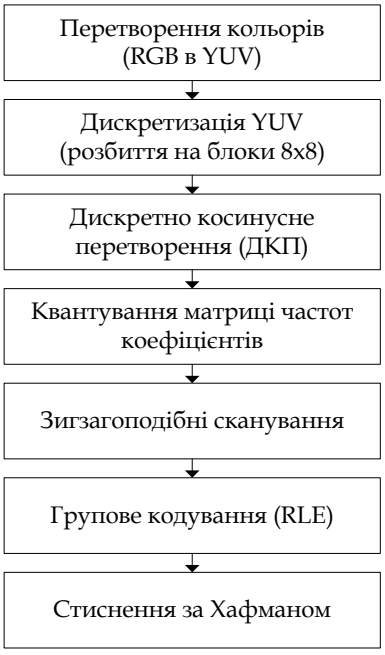

Рис. 1. Модель ДКП стиснення зображень

1. Спочатку відбувається перетворення кольорової моделі *RGB* в іншу *YUV*. В зв'язку з тим, що більша частина візуальної інформації, сприймаюча людським оком, складається з компонентів яскравості *Y*, а до кольорових компонент *U* і *V* менш чутлива, то відкидаючи частину кольорових даних можна забезпечити стискання зображення.

2. Дискретизація YUV кольорів, відбувається проріджуванням кольорових компонентів з коефіцієнтом 2. В результаті чого отримується в 2 рази стиснене зображення без будь-якого візуального погіршення.

3. Відбувається розбиття зображення на невеликі блоки розміром 8×8. Над яким потім відбувається перетворення за допомогою ДКП. На цьому етапі відбувається деяка втрата інформації в зв'язку з неможливістю точного перетворення.

4. В результаті ДКП перетворення отримується матриці частотних коефіцієнтів. Для зменшення їх розрядності використовують матриці квантування. За допомогою яких більшість високочастотних та середньо частотних коефіцієнтів перетворюється на 0.

5. Відбувається зигзагоподібні сканування матриці для об'єднання нульових коефіцієнтів в групи.

6. Відбувається групове кодування, в результаті чого кожний не нульовий коефіцієнт вектора записується в вигляді пари двох чисел, де перше число це кількість нулів перед цим числом, а друге – значення даного елемента вектора.

7. Потім застосовується метод одноразового кодування Хаффмана. За яким спочатку аналізується вся послідовність символів і часто повторювальним серіям біт ставиться у відповідність короткі маркери.

На кожному етапі компресії за ДКП можебути реалізовуване приховування інформації. Існує ряд методів працюючих з ДКП: *1) метод Коха і Жао* [2, 5, 6, 19, 23], що полягає в виборі з C блока ДКП коефіцієнтів два значення. Їх різницю порівнюють з деякою відносною величиною P. Якщо потрібно внести «0» то ця різниця робиться більшою ніж P, а при внесенні «1» – меншою; *2) метод Бенгама-Меммона-Ео-Юнга* [2, 5, 6], що являється модифікацією попереднього методу. Різниця полягає в тому, що блоки вибираються псевдовипадково. Кожен вибраний блок перевіряється з граничними значеннями P_l (блок не повинен містити граничні переходи яскравості) та P_h (не повинен бути с верх монотонним).В разі не відповідності блок відкидається. Також вибирається не два а три коефіцієнти з блоку, перші два з них порівнюються з граничним числом P. Якщо потрібно внести «0», то третій коефіцієнт роблять меншим любого із перших двох, при внесенні «1» все навпаки; *3)* метод Хсу і Ву [2, 5, 6, 36] полягає в вбудовуванні в масив коефіцієнтів ДКП блоків зображення цифрового водяного знака, який представляє собою двійкове зображення розміром $A\times Z$; *4) метод Фрідріх* [2, 5, 19], в загальному являється поєднанням двох методів, де один скриває в низькочастотні коефіцієнти ДКП, а інший в середньо частотні коефіцієнти.

Використання ВП (застосовується в форматі *JPEG2000*) полягає в ієрархічному розкладанні вхідного сигналу на послідовності так званих базових компонент з послідовно зменшуваним розрідженням і пов'язаних з ними компонентів деталей (дозволяє добре локалізувати низькочастотні деталі сигналу в частотній області, а високочастотні – в часовій). На кожному рівні розкладання базова компонента і компонента деталей містять інформацію, необхідну для відновлення базового сигналу на наступному рівні більш з високою роздільною здатністю. Основна ідея використання дискретного ВП у процесі обробки зображення полягає в розкладанні зображення в під зображення різних просторових та частотних областях. Таке розкладання реалізується R разів, де результатом являється набір $3R+1$ матриць. Кожна матриця піддається скалярно-векторному квантуванню, подальшому кодуванню та стисненню за кодом Хаффмана. Вибір числа рівнів квантування проводиться виходячи з потрібного стискання і відповідного розподілу бітів між матрицями.

В роботах [8, 13-15] представлено метод шаблонного вбудовування даних у вейвлет коефіцієнти на основі таблиці відповідності між захищеними даними та значеннями шаблону, що, на відміну від існуючих, забезпечує високу швидкість вбудовування.

Фрактальне стиснення зображень – це алгоритм заснований на застосуванні систем ітеріруемих функцій (IFS, як правило афінних перетворень) до зображення. Даний алгоритм відомий тим, що в деяких випадках дозволяє отримати дуже високі коефіцієнти стиснення (до 1000 раз при прийнятній візуальній якості) для реальних фотографій природних об'єктів, що недоступно для інших алгоритмів стиснення зображень в принципі. Існує ряд методів, що використовують процес фрактального стиснення зображення для приховування інформації [12]. Ефективність фрактального стиснення залежить від міри мінімізації двох параметрів при відповідності до певних обмежень, що забезпечують необхідну якість зображення. Цими параметрами є розмір стиснутого зображення і затрати часу на компресії.

У роботі [7] представлена модель вбудовування даних у фрактальний код зображень, яка на відміну від існуючих, враховує взаємозв'язки між стеганографічними перетвореннями і забезпечує збільшення обсягу даних, що вбудовуються, за умови стійкості до пасивних атак.

Методи розширення спектру використовуються в техніці радіо зв'язку для забезпечення високої завадостійкості [2, 5, 19, 25, 26, 28, 45, 49]. Основна ідея даних методів полягає в розширені смуги частот сигналу до більших розмірів ніж це потрібно для передачі реальної інформації. Розповсюдження інформації відбувається по всьому діапазону, при втраті сигналу в деяких смугах частот їх можна відновити використовуючи непошкоджені смуги. Прикладом служить метод *Сміта-Комісси* [36] в якому повідомлення побітно модулюється шляхом множення на ансамбль ортогональних сигналів. Потім промодульоване повідомлення вбудовується в контейнер зображення.

Методи псевдоголографії базуються на перетворенні зображення в одновимірну послідовність так, щоб близьким відлікам в цій послідовності відповідали «далекі» точки основного

зображення. Перетворення зображення в таку послідовність називається псевдоголографічною розгорткою цифрового зображення, що дає можливість при отриманні частини зображення побачити в ньому ціле зображення, але з меншими розмірами [51, 52].

Статистичні методи базуються на статистичних властивостях зображення [5, 25, 28]. При вкрапленні інформації вони змінюють статистичні властивості зображення так, щоб ніякими методами статистичного стегоаналізу було неможливо визначити чи це зображення справжнє або модифіковане [1].

Методи спотворення полягають в послідовному проведені модифікацій контейнера відповідно до секретного повідомлення [25, 28]. Однак для вилучення повідомлення необхідно мати знання про початковий (не модифікований) вигляд контейнеру і його відмінність від стегоконтейнеру. Такі системи є неефективними, оскільки для вилучення секретного повідомлення потрібно мати доступ до оригіналу контейнера, а це передбачає необхідність ще одного таємного каналу для передачі даних.

Ще одним та досить важливими методами приховування в зображення є *методи обробки зображень для поліграфічної діяльності* [18, 29, 32]. Складність реалізації даних методів пов'язана з тим, що описані вище методи не підходять для приховування інформації. Оскільки вкраплення відбувається на матеріальний носій з нанесеним на нього зображенням. Також дані методи ускладнюються наявністю двох додаткових операцій обробки зображення: роздрукування на принтері, сканування зображення з матеріального носія. Дані операції повинні враховуватись в поліграфічних методах, бо вони певним чином обробляють зображення і вносять зміни в його структуру. Вкраплення інформації відбувається шляхом: 1) розбиття зображення на блоки; 2) для кожного блоку обраховується середнє значення яскравості; 3) в блоці вибирають та змінюють декілька точок яскравості растра так щоб середнє значення яскравості не змінювалося. Певний спосіб кодування інформації значеннями яскравостей точок растра в блоці може бути вибраний, виходячи із вимог завадостійкості системи та фізичних властивостей приладів сканування та друку. Прикладами служать методи вкраплення інформації за рахунок варіації направлених ліній, варіації масштабу і фази.

Методи приховування в відео послідовностях

Використання відео файлів для приховування в багато чому схоже до зображень. Оскілки потік відео даних складається з сукупності зображень. Одним із алгоритмів стиснення відео послідовностей є формат *MPEG*. Стиснення по формату *MPEG* полягає в наступному, що із всього потоку даних передаються тільки повністю декілька основних кадрів, для інших передаються лише їх відмінності від основних та інших кадрів. Відео потік по формату *MPEG* має ієрархічну синтаксичну структуру. Послідовність відео даних розділяються на групи кадрів, неодмінно слідуючи один за одним при відтворенні. Далі кадри поділяються на шари та макроблоки. Найнижчий рівень блоку із блоків містить відомості про яскравість та кольоровість макроблоку. В стандарті *MPEG* використовується три типи кадрів: 1) *I*-кадри – кодуються без посилань на інші кадри, містять нерухоме зображення і додатково використовуються для побудови інших типів кадрів; 2) *P*-кадри – передбачувані кадри, які кодуються з посиланням на попередній (з точки зору приймача) прийнятий (*I*) або (*P*) кадр; 3) *B*-кадри – двох сторонні інтерпольовані кадри, які кодуються найбільш складним чином. Такий кадр може будуватися і на основі попереднього кадру, і на основі подальшого кадру, і як інтерполяція між попереднім і наступним кадром. Стиснення відбувається подібно до зображень за допомогою ДКП за деякими відмінностями. *I*-кадри стискаються звичайним ДКП. *P*-кадри та *B*-кадри розбиваються на блоки 8×8 пікселів і потім порівнюються з деяким опорним кадром. Потім можливі 3 випадки: 1) окремий блок у кодованому *P*-кадрі співпадає з розташованим в цій же позиції блоком опорного кадру. Тоді достатньо вказати, що блок залишився таким же; 2) окремий блок у кодованому кадрі збігається з блоком опорного кадру, що знаходиться в іншій позиції. Тоді для його кодування необхідно задати вектор зміщення; 3) окремий блок у кольоровому кадрі може не збігатися ні з одним з блоків опорного кадру. Тоді він буде кодуватися повністю. Існує декілька методів приховування даних в відео послідовності стиснених за форматом *MPEG* [1, 11, 19]: *1. Метод приховування інформації на рівні коефіцієнтів*, що реалізується додавання псевдовипадкового масиву до ДКП коефіцієнтів відео. У процесі вбудовування інформації безпосередньо беруть участь тільки значення яскравості в *I*-кадрах. Метод при його застосуванні значно погіршується якість відео. Існує правило, щоб забезпечити хорошу якість відео слід брати коефіцієнт посилання меншими 1, і кількість пікселів на один біт секретної інформації повинен бути достатньо великим більшим 100000. *2. Метод приховування інформації на рівні бітової площини*. За цим методом приховувана інформація, що складається з L бітів деякої послідовності $B_j (j = 0,1,...,L-1)$, впроваджується в потік відеоданих шляхом заміни спеціально обраних, підходящих кодових слів коду змінної довжини, замінюючи найменш значущий біт їх оцифрованого значення на значення B_j. Для перевірки правильності внесення змін, що не будуть помітні після декодування, необхідно вибирати тільки кодові слова, для яких знайдеться хоча б одне інше кодове слово, яке задовольняє умовам: 1) однакова довжина нульової серії; 2) розходження між значеннями коефіцієнтів ДКП дорівнює 1; 3) однакова довжина кодових слів. Даний метод за своєю нескладною реалізацією може приховувати великі об'єми даних, однак приховувана інформація може бути легко видалена. Для цього достатньо просто повторно накласти довільну послідовність, причому якість відео трохи погіршиться, а приховувана інформація буде знищена. *3. Метод вбудовування за рахунок*

енергетичної різниці між коефіцієнтами. В його основі лежить диференціальне вбудовування енергії (ДВЕ) приховуваної інформації. У разі *MPEG*, *JPEG* кодованих відеоданих ДВЕ може бути здійснено в області коефіцієнтів. За яким біт секретної інформації впроваджується в обрану область модифікацією різниці енергій *D* між високочастотними коефіцієнтами ДКП в верхній частині цієї області (під область *A*) і її нижній частині (під область *B*). Позитивною властивістю алгоритму ДВЕ є те, що для видалення інформації потрібно проводити обчислювальні операції, більш складніші ніж вбудовування нової довільної послідовності.

Висновки

Таким чином, у цій роботі проводиться систематизація сучасних методів приховування інформації в комп'ютерних системах та мережах. На основі чого було виділено поділ даних методів на групи за місцем приховування інформації. Серед них в достатній мірі були описані методи приховування в мультимедійних об'єктах, а саме методи працюючі з комп'ютерною графікою. Так, сучасні методи приховування в комп'ютерній графіці працюють лише з двома її типами (растровою та фрактальною). Однак існує ще векторна та *3D*графіка над якими не проводилися дослідження по можливостям приховування даних. Тому, подальші дослідження за цим напрямом будуть спрямовані на розробку нових методів та оцінки їх можливостей, що можуть дати досить перспективні результати.

Література

[1] Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.

[2] Сорока Н. И. Теория передачи информации : конспект лекций [для студентов специальности 1-53 01 07 «Информационные технологии и управление в технических системах»] / Н. И. Сорока, Г. А. Кривинченко. — Минск : БГУИР, 2005. — 301 с.

[3] Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — М. : Горячая линия – Телеком, 2010. — 232 с.

[4] Методы цифровой стеганографии для защиты изобразительной информации / В.Н. Горбачев, Е.М. Кайнарова, А.И. Кулик, И.К. Метелев. — М. : МГУП, 2011. — 224 с.

[5] Конахович Г. Ф. Компьютерная стеганография : теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

[6] Тарасов Д. О. Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д. О. Тарасов, А. С. Мельник, М. М. Голобородько // Інформаційні системи та мережі : [збірник наукових праць]. — Львів : Видавництво Національного університету «Львівська політехніка», 2010. — С. 365-373.

[7] Золотавкін Є. А. Методи та засоби підвищення стеганографічної стійкості захисту інформації до пасивних атак: автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21 / Золотавкін Євген Анатолійович. — К., 2010. — 20 с.

[8] Лукічов В. В. Методи та засоби стеганографічного захисту інформації в комп'ютерних системах і мережах на основі вейвлет-перетворень : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21 / Лукічов Віталій Володимирович. — К., 2010. — 20 с.

[9] Золотавкін Є. А. Детектування таємного вмісту у стиснених фрактальним алгоритмом зображеннях / Є. А. Золотавкін, А. С. Васюра // Наукові праці Вінницького національного технічного університету. — 2008. — № 3. — С. 1-9.

[10] Михнев А. С. Комбинированный метод скрытой передачи зашифрованных сообщений с использованием LSB-метода и конгруэнтных последовательностей / А.С. Михнев, А.С. Запевалов, С.С. Михнев // Научный журнал «Збірник наукових праць Севастопольського національного університету ядерної енергії та промисловості». — 2009. — №2. — С. 165-169.

[11] Моденова О. В. Стеганография и стегоанализ в видеофайлах / О.В. Моденова // журнал «Прикладная дискретная математика». — 2010. , Прилож. № 3. — С. 37–39.

[12] Золотавкін Є. А. Шляхи підвищення ефективності стеганографічного використання фрактального алгоритму стиснення зображень / Є. А. Золотавкін, А. С. Васюра // Вісник Вінницького політехнічного інституту. — 2006. — №6. — С. 180-186.

[13] Лукічов В. В. Метод вбудовування даних у зображення за можливості JPEG-стиснення / А. С. Васюра, В. В. Лукічов // Оптико-електронні інформаційно-енергетичні технології. — 2008. — Т. 16, №2. — С. 42-47.

[14] Лукічов В. В. Метод шаблонного вбудовування даних у вейвлет коефіцієнти на основі критерію стеганографічної стійкості / А.С. Васюра, В.В. Лукічов // Наукові праці Вінницького національного технічного університету. — 2009. — №1.

[15] Лукічов В. В. Підвищення ефективності методу шаблонного вбудовування даних у зображення / А. С. Васюра, В. В. Лукічов // Наукові праці Вінницького національного технічного університету. — 2008. — №3.

[16] Защита информации. INSIDE: [информационно-методический журнал]. — СПб. : Издательский дом «Афина» — 2007. — №3. — 100 с.

[17] Тропченко А. Ю. Методы сжатия изображений, аудиосигналов и видео : учебное пособие / А. Ю. Тропченко, А. А. Тропченко. — СПб. : СПбГУ ИТМО, 2009. — 108 с.

[18] Митекин В. А. Модели стеганографической системы и обобщенного алгоритма встраивания ЦВЗ в полиграфические изделия / В. А. Митекин, А. В. Сергеев, В. А.

Федосеев, Д. М. Богомолов //Компьютерная оптика. — 2007. — Том 31, № 4. — С. 95-101.

[19] Бабич І. В. Огляд стеганографічних методів перетворення інформації в зображеннях / І.В. Бабич, С.А. Паламарчук, Н.А. Паламарчук, В.В. Овсянніков // Захист інформації. — 2012. — № 1. — С. 18-24.

[20] Навроцький Д. О. Дослідження результатів стеганорафічного приховування повідомлень у файлах зобрження як засобу забезпечення захисту інформації / Д. О. Навроцький // Вісник Національного технічного університету України «КПІ». — 2012. — №50. — С. 121-128.

[21] Лагун А. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А. Лагун, І. Лагун // Захист інформації і безпека інформаційних систем. — Л. — 2013. — С. 98-99.

[22] Кущ С. Алгоритм формування стеганограм на основі LSB-методу / С. Кущ, Д. Прогонов // Захист інформації і безпека інформаційних систем. — Л. — 2013. — С. 110-111.

[23] Андрущенко Д. Анализ стойкости метода Коха-Жао стеганографического встраивания информации в статические изображения / Д. Андрущенко, Г. Козина // науково-технічний збірник Національного технічного університету України «КПІ». — 2008. — С. 70-73.

[24] Введение в цифровую обработку изоражений : [учебно-методическое пособие по курсу «Основы компьютерной видеографики»] / под ред. проф. К. В. Филатова. — Таганрог : Изд-во ТРТУ, 2002. — 89 с.

[25] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah Ma. Al-Qershi Image Steganography Techniques: An Overview, International Journal of Computer Science and Security (IJCSS), Volume 6, Issue 3, 2012.

[26] Johnson N. F. A Survey of steganographic techniques / N.F. Johnson, S. Katzenbeisser // Information Hiding Techniques for Steganography and Digital Watermarking. — Ed. London : Artech House, 2000. — PP. 43-78.

[27] Cheddad A. Digital Image Steganography: Survey and Analysis of Current Methods / A. Cheddad, J. Condell, K. Curran, P. Kevitt // 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008.

[28] Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. — К. : Юниор, 2003. — 501 с.

[29] Алефиренко В. М. Основы защиты информации : практикум [для студ. спец. «Техническое обеспечение безопасности» и «Моделирование и компьютерное проектирование радиоэлектронных средств» дневной, вечерней и заочной форм обучения / В. М. Алефиренко, Ю. В. Шамгин. — Мн. : БГУИР, 2004. — 43 с.

[30] Барсуков В.С. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации / В.С. Барсуков, А.П. Романцов // Специальная техника. — 1999. — № 6.

[31] Васина Т. С. Обзор современных алгоритмов стеганографии / Т. С. Васина // электронное научно-техническое издание «Наука и образование». — 2012.

[32] Федосеев В. А. Выделение защитной информации на изображениях текстурированных полиграфических изделий : автореф. дис. на здобуття наук. ступеня канд. физ.-мат. наук : спец. 05.13.17 «Теоретические основы информатики» / В. А. Федосеев. — С., 2012. — 16 с.

[33] Коваленко М.П. Использование искусствен-ных нейронных сетей при внедрении цифровых водяных знаков в графические изображения / М. П. Коваленко, Я. Д. Смирнов // VIII Международная научно-практическая конференция «Эффективные инструменты современных наук». — Prague. Publishing house «Education and Science» s.r.o. — 2012. — С. 87-97.

[34] Коваленко М. П. Исследование однородности искажений частотных коэффициентов ДКП матрицы, вносимых JPEG-сжатием и медианной фильтрацией цифровых изображений / М. П. Коваленко // Технические науки: теоретические и прикладные аспекты. — 2012.

[35] Коваленко М. П. Исследование статистических свойств искажений частотных коэффициентов ДКП матрицы в условиях воздействия на изображение JPEG-сжатия / М. П. Коваленко // Журнал научных публикаций аспирантов и докторантов. 2012. — №2. — С. 96-99.

[36] Кузнецов О. О. Стеганография : навч. посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. — Х. : Вид. ХНЕУ, 2011. — 232 с.

[37] Ahsan K. Practical Data Hiding in TCP/IP / K. Ahsan, D. Kundur // Proc. ACM Wksp. Multimedia Security, December 2002.

[38] Bennett N. R. JPEG Steganalysis & TCP/IP Steganography : Ph.D. dissertation / N. R. Bennett. — University of Rhode Island, 2009.

[39] Murdoch S. J. Embedding covert channels into TCP/IP / S. J. Murdoch, S. Lewis // In Proc. IH, 2005.

[40] Швидченко И. В. Стойкие криптостеганографические алгоритмы / И. В. Швидченко // Искусств. интеллект. — 2008. — № 4. — С. 282-290.

[41] Ker A. D. Steganalysis of LSB Matching in Grayscale Images / A. D. Ker // IEEE Signal Processing Letters. — Vol. 12, No. 6. — june 2005.

[42] Ажбаев Т. Г. Анализ стойкости современных стеганографических алгоритмов / Т. Г. Ажбаев, И.М. Ажмухамедов // Вестник Астраханского государственного технического университета. — 2008. — С. 56-61.

[43] Geetha S. Detection of Stego Anomalies in Images Exploiting the Content Independent Statistical Footprints of the Steganograms / S. Geetha, Siva S. Sivatha Sindhu, N. Kamaraj. — Informatica (Slovenia), 2009. — P. 25-40.

[44] Васина Т.С. Обзор современных алгоритмов стеганографии / Т.С. Васина // Наука и образование: электронное научно-техническое издание. — 2012.

[45] Навроцький Д. О. Дослідження результатів стеганографічного приховування повідомлень у файлах зображення як засобу забезпечення захисту інформації / Д.О. Навроцький // Вісник Національного технічного університету України «КПІ». — № 50. —2012.

[46] Fridrich J. Practical steganalysis of digital images - state of the art / J. Fridrich, M. Goljan // In: Proc. of SPIE Photonics West.—San Jose, California, USA — 2002.

[47] Столниц Э. Вейвлеты в компьютерной графике: [теория и приложения] / Э. Столниц, Т. Дероуз, Д. Салезин. —М. : Ижевск РХД, 2002. — 272 с.

[48] Воробьев В. И. Теория и практика вейвлет-преобразования / В. И. Воробьев, В. Г. Грибунин. — С.-Петербург : ВУС, 1999. — 180 с.

[49] Стасюк О.І. Сучасні стеганографічні методи захисту інформації / О.І. Стасюк, С.О. Гнатюк, Н.І. Довгич, М.С. Літош // Захист інформації. — 2011. — №1 (50). — С. 56–63.

[50] Иванов М.А. Применение вейвлет-преобразований в кодировании изображений / М.А. Иванов // Новые информационные технологии в науке и образовании. — 2004. — № 24. — С. 157–175.

[51] Урывская Д.А. Разработка и применение псевдоголографических разверток цифровых изображений: автореф. дис. на соискание уч. степени канд. физ.-мат. наук : спец. 05.13.17 «Теоретические основы информатики» / Д. А. Урывская. — С., 2012. — 16 с.

[52] Головатюк О.Ю. Розробка програмного забезпечення реалізації прихованих цифрових водяних знаків з використанням методів псевдоголографії / О.Ю. Головатюк // Сучасні інформаційні технології та програмне забезпечення комп'ютерних систем. — К., 2013 р. — С. 149-151.

УДК 004.056.5 (045)

Ковтун В.Ю., Гнатюк С.А., Кинзерявый А.Н. Систематизация современных методов компьютерной стеганографии

Аннотация. *Стеганография является направлением защиты информации, который позволяет организовать безопасный канал обмена данных за счет сокрытия факта существования тайного сообщения. В последнее время появилось достаточно много методов компьютерной стеганографии, а их систематизация оставалась актуальной научной задачей. В связи с этим, в статье проведена систематизация современных методов компьютерной стеганографии. Определены общие возможные места сокрытия данных в компьютерных системах и сетях. Содержит общее описание методов сокрытия в мультимедийных (цифровых) объектах, где особое внимание уделяется методам сокрытия в изображениях, над которыми ведется большинство стеганографических исследований. К методам компьютерной стеганографии отнесено сокрытие данных в полиграфической деятельности и методы на основе псевдоголографии.*

Ключевые слова: *защита информации, компьютерная стеганография, методы сокрытия данных, файлово-системные методы, сетевые методы, мультимедийные объекты, цифровая стеганография, ортогональные преобразования изображений.*

Kovtun V.Yu., Gnatyuk S.O., Kinzeryavyy O.M. Modern methods of computer steganography systematization

Abstract. *Steganography is the direction of information security, which allows you to organize secure data exchange channel by hiding the existence of secret messages. Recently, there are many methods of computer steganography, and their systematization remained relevant scientific problem. In the paper the systematization of modern computer steganography methods was carried out. The general possible places to hide data in computer systems and networks were defined. The general description of data hiding methods in multimedia (digital) objectswas included where attention was directed to methods of hiding in images because this is most popular object of steganographic research. Data hiding in polygraphy and methods based on pseudo holography were referred to computer steganography.*

Key words: *information security, computer steganography, methods of data hiding, file-system methods, network methods, multimedia objects, digital steganography, orthogonal transformation of images.*

Отримано *07 вересня 2013 року*, затверджено редколегією *23 жовтня 2013 року*