системи.

У цій системі спочатку обробляються всі пакети, а згодом будуються мережеві потоки. Під час цього процесу нечіткий обробник збереже всі підозрілі пакети в пам’ять. Коли генерується заголовок потоку, підозрілий потік ще раз перевірятиметься нечітким обробником та виявлятимуться атаки.

1. Denial of Service (DoS) Attack Detection by Using Fuzzy Logic over Network Flows, https://www.researchgate.net/publication/26877049
2. SPADE, Silicon Defense, http://www.silicondefense.com/software/spice/.
3. Intrusion detection system, https://en.wikipedia.org/wiki/Intrusion_detection_system
4. https://www.networkworld.com/article/3073481/darpa-extreme-ddos-project-transforming-network-attack-mitigation.html

http://doi.org/10.5281/zenodo.3859687

Поступила 3.10.2019р.

УДК 621.3

О.Б. Полусин, Львів

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ НАНЕСЕННЯМ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

Abstract. An analysis of steganography methods was performed, which showed that broadband and statistical methods are more effective for the protection of multimedia objects. The use of other methods requires a lot of time or resources, so their introduction can be considered impractical.

Keywords: multimedia protection, digital watermark.

Вступ

Сучасне суспільство користується великою кількістю послуг, що стали більш доступніші за допомогою сучасних комп’ютерних мереж та інформаційних технологій. Сьогодні уся інформація представлена в цифровому вигляді, тому доступ до будь-якої інформації необхідно захистити від багатьох загроз: несанкціонованого доступу та використання, знищення, підробки, витоку, порушення ліцензійних угод, відмови відавторства та ін.

Захист інформації являється вкрай важливим завданням для усіх сфер діяльності, від комерційних до державних. Серед загроз для інформаційної сфери можна виділити: комп'ютерну злочинність; розголошення таємної чи

конфіденційної інформації, використання отриманої інформації для власного використання чи збагачення. Отже, розроблення ефективних методів захисту цифрової інформації, актуальні та мають важливе значення для держави й суспільства. Найбільшого розвитку в Україні та світі здобули методи криптографічного захисту. Альтернативний та не менш надійний захист сьогодні може бути створений на базі стеганографії.

В комп'ютерній стеганографії базовою вимогою являється цілісність елементу захисту, що внесений, незважаючи на можливі зміни, що можуть здійснюватися. Найперше дана вимога поширюється на такий елемент захисту як цифровий водяний знак (ЦВЗ).

Існують три основні властивості ЦВЗ, що надають перевагу над іншими методами та елементами захисту, а саме: непомітність ЦВЗ і відсутність необхідності збільшення розміру контейнера-носія, яких захищається; ЦВЗ не віддільний від файлу і не може бути вилучений без завдання змін, завдяки яким можливо виявити зовнішнє втручання; над файлом та ЦВЗ здійснюється однакове перетворення, що дозволяє досліджувати файл, який захищається, після спотворення чи видалення ЦВЗ. Широкодоступне програмне забезпечення, що знаходиться у вільному доступі через глобальну мережу, яке дозволяє здійснювати захист об'єктів мультимедіа та інформації в цілому, шляхом накладення ЦВЗ на об'єкт, базується на методах, що будуть досліджуватись в подальшому. Серед них існують такі методи: LSB-метод (заміна молодших біт), метод частотної області, широкосмуговий метод, статистичні методи (алгоритм Patchwork).

Існуючі методи мають велику кількість переваг, але лише у певному діапазоні для захисту об'єктів, тому на противагу перевагам існуєдосить велика кількість не вирішених недоліків, що дозволяють певним чином обійти захист об'єктів та використати їх за власною метою.

Аналіз

Переваги цифрового водяного знаку перед іншими методами захисту створює велику кількість досліджень для його вдосконалення. Дослідження цифрового водяного знаку сьогодні здійснюється великою кількістю науковців у всіх куточках світу. У наукових роботах показуються різноманітні методи вдосконалення нанесення ЦВЗ. Зокрема, у роботі [3] досліджувався спосіб формування цифрового водяного знаку для фізичних та електронних документів. В роботі [4] описується алгоритм вбудовування цифрових водяних знаків в цифрові зображення,який вдалось вдосконалити шляхом спрощення.

Постановка проблеми

Хоча цифровий водяний знак і являється найефективнішим елементом захисту даних, однак на сьогодні не можливо сказати, що нанесений ЦВЗ досконало забезпечить захист будь-яких даних, зокрема даних мультимедіа.

Метою статті є дослідження та аналізметодів нанесення цифрового водяного знаку на мультимедійні дані з метою їх захисту від несанкціонованого використання.

Виклад основного матеріалу

Цифровий водяний знак (ЦВЗ) - це технологія, створена для захисту мультимедійних файлів, що є об'єктам авторського права, для захисту від змін без відома автора та несанкціонованого використання. Цифрові водяні знаки можна розділити на два різновиди.

Видимі ЦВЗ – це один із різновидів захисту, що здійснюється шляхом накладення елемента захисту, який можливо побачити візуально, на об’єкт який необхідно захистити. Зазвичай це інформація у вигляді тексту або логотипу, який накладається на зображення, з метою ідентифікації автора та підтвердження оригінальності документів, таких як: паспортів, водійських посвідчень та кредитних карт з фотографіями.

Ще одним із різновидів являються невидимі ЦВЗ – тобто елемент захисту, який накладений на об’єкт який необхідно захистити неможливо побачити візуально, а лише після здійснення певних операцій над об’єктом, що захищається. Невидимий ЦВЗ може містити в собі не лише логотип чи текст, а й велику кількість ідентифікуючої інформації про автора та створення самого об’єкта, це так звані «метадані».

Об’єктимультимедіа в цьому випадку будуть контейнерами (носії) даних. Основна перевага полягає в наявності умовної залежності між подією підміни об'єкту ідентифікації і наявності елементу захисту прихованого водяного знаку. Підміна об'єкту ідентифікації, приведе до виводу про підробку всього документа.

Видимі ЦВЗ досить просто видалити або замінити. Для цього можуть бути використані графічні або текстові редактори. Про те невидимі ЦВЗ являються вбудовуваними вставками, що не сприймаються людським оком або вухом.

Тому ЦВЗ повинні відповідати наступним вимогам:

— непомітність для користувачів;

— індивідуальність алгоритму нанесення (досягається за допомогою стеганографічного алгоритму з використанням ключа);

— можливість для автора виявити несанкціоноване використання файлу;

— неможливість видалення неуповноваженими особами;

— стійкість до змін носія-контейнера (до зміни його формату і розмірів, до масштабування, стискування, повороту, фільтрації, монтажу, аналогових і цифрових перетворень).

Кожна дія завжди передбачена певним алгоритмом. Алгоритм накладання ЦВЗ на мультимедійний об’єкт має три основні етапи: 1) генерація ЦВЗ; 2) накладення ЦВЗ в кодері; 3) виявлення ЦВЗ в декодері [1].

Нехай W - ЦВЗ, K - ключі, I - контейнери, B – прихована інформація, в такому випадку генерація ЦВЗ можна представити у вигляді:

$$F: I * K * B \rightarrow W, \quad W= F(I, K, B), \tag{1}$$

де функція F може бути довільною, але на практиці на дану функцію накладають обмеження через певні вимоги ЦВЗ.

Оскільки $F(I, K, B) \approx F(I+з, K, B)$, можемо зробити висновок, що при не значному зміні контейнера ЦВЗ не зміниться.

Процес накладення ЦВЗ W (i, j) на початковий об’єкт I (i, j) описується так:

$$\varepsilon: I * W * L \rightarrow I_W, \quad I_W (i, j) = I_0 (i, j) \oplus L(i, j)W(i, j)p(i, j), \tag{2}$$

де L(i, j) – маска накладання ЦВЗ, враховуючи характеристики зорового сприйняття людини, необхідно для зменшення видимості ЦВЗ; p(i, j) – проектуюча функція, що залежить від ключа; $\oplus$- оператор суперпозиції, що включає в себе додавання, усічення та квантування.

Дана функція здійснює розміщення ЦВЗ по усіх області об’єкта мультимедіа. Вона дозволяє реалізувати розподіл інформації по паралельних каналах. Окрім цього, функція має певну структуру та кореляційні властивості, що може використовуватись для протидії різнотипним атакам на ЦВЗ.

Для ідентифікації автора та перевірки справжності отриманого об’єкту, необхідно отримати інформацію з накладеного ЦВЗ. Цей процес стає можливим завдяки декодеру, який перевіряє наявність ЦВЗ для подальших дій. Звичайне декодування (D) має наступний вигляд:

$$D: I_w * K \rightarrow \{0,1\}, \; D (I_{w,} W) = D (I_w, F(I_w, K)) = \begin{cases} 1, \text{якщо } W \text{ наявне} \\ 0, \text{якщо } W \text{ ненаявне}, \end{cases} \tag{3}$$

Під час перевірки декодером об’єкта на наявність ЦВЗ, можливим стає виникнення певних помилок, тобто існує ймовірність, що декодер не виявить ЦВЗ, який накладений або хибне виявлення ЦВЗ у об’єкті, який не захищений ним. Тому надійність працездатності декодера характеризують ймовірністю хибного виявлення ЦВЗ.

Створення, накладення та отримання ЦВЗ не потребує великих затрат часу та ресурсів, про те проблема постає в універсальності ЦВЗ у зв’язку з різноманітними вимогами, які повинен виконувати ЦВЗ. Тому більшість досліджень сьогодні спрямовані на покращення захисту цифровим водяним знаком. На даний час існує велика кількість методів, що дозволяють приховувати інформацію та ЦВЗ у об’єкти мультимедіа.

Класичний метод заміни молодших біт (LSB-метод) базується на тому, що молодші розряди мультимедійних об'єктів несуть малу кількість інформації і їх зміна не впливає на якість об'єктів. Перевагою даного методу являється проста реалізація та можливість передачі великого обсягу інформації. Проте введення додаткової інформації призводить до спотворення статистичних характеристик контейнера і легкого виявлення ЦВЗ за допомогою статистичних атак, таких як оцінка ентропії та коефіцієнтів кореляції. Для зниження ознак, що призводять до виявлення ЦВЗ потрібно здійснювати корегування статистичних характеристик. До недоліків даного методу можна віднести його чутливість до операцій цифрової обробки: стиснення, застосування фільтрації, конвертації кольорів, геометричних перетворень, додаткового зашумлення та зміни формату контейнера.

У методах, що діють у частотній області, дані приховуються у коефіцієнтах частотного представлення контейнера. Для цього найчастіше використовуються перетворення, які застосовуються у сучасних алгоритмах стиснення із втратами. Приховання інформації може проводитися як в початкове зображення, так і одночасно із здійсненням стиснення зображення-контейнера. Вони забезпечують більшу стійкість до геометричних перетворень і виявлення каналу передачі (порівняно з методом LSB), оскільки є можливість у широкому діапазоні варіювати якість стисненого зображення, що робить неможливим визначення походження спотворення.

Широкосмуговий метод застосовується для розширення смуги частот сигналу до ширини спектра, значно більшої, ніж це необхідно для передачі реальної інформації. Розширення спектру здійснюється двомаметодами: метод прямого розширення спектра за допомогою псевдовипадкової послідовності і метод стрибкоподібного переналаштування частоти. При цьому корисна інформація розподіляється по усьому діапазону, тому за втрати сигналу у деяких смугах залишається достатньо інформації для її відновлення. Вагомою перевагою даних методів являється те, що сигнал, розподілений по усій смузі спектра, його важко виділити, тому їм властиві стійкість до випадкових та умисних спотворень. Недоліком вважають можливість здійснення стегоаналізу за рахунок цифрової обробки з використанням шумозгладжувальних фільтрів[3].

Статистичні методи приховують інформацію зміною деяких статистичних властивостей зображення. Наприклад, алгоритм Patchwork базується на припущенні, що значення пікселів незалежні і однаково розподілені, тобто: спочатку псевдовипадковим генератором у відповідності до секретного ключа, що генерується, вибираються два пікселі зображення. На наступному етапі здійснюється збільшення та зменшення яскравості пікселів на однакову величину. Дану операцію повторюють велику кількість

разів, після чого знаходиться сума значень усіх різниць, що проводились:

$$S_n = \sum_{i=0}^{n}\big((a_i + c) - (b_i - c)\big) = 2cn + \sum_{i=1}^{n}(a_i - b_i), \qquad (4)$$

де a_i та b_i – значення яскравості двох вибраних пікселів з кроком i, c – величина, на яку змінюється яскравість на кожному кроці алгоритму.

Даний метод забезпечує високу стійкість до цифрової обробки та майже унеможливлює виявлення ЦВЗ без відповідного секретного ключа, однак йому властиві відсутність стійкості до перетворень (повороти, масштабування, зсуву) та досить мала пропускна здатність (для передачі 1 біта прихованого повідомлення необхідно 20000 пікселів).

Кожен із наведених методів володіє своїми перевагами і недоліками. Переваги LSB-методу – це простота в реалізації та передача великого об'єму інформації,методи, що застосовують у частотній області, можемо вважати стійкішими до спотворень та операцій цифрової обробки, але вони можуть приховати менший обсяг даних. Наявність секретного ключа у широкосмугових та статистичних методах, що використовують псевдовипадкове кодування, підвищує їх надійність, а розподіл прихованих бітів по усьому контейнері зумовлює високу стійкість до випадкових та умисних спотворень, що враховується під час побудови ЦВЗ.

Висновок. Дослідження відомих методів захисту мультимедійних даних за допомогою цифрового водяного знаку, що використовуються в даний час, дозволили виділити їх основні характеристики, переваги та недоліки. В процесі досліджень був проведений попередній аналіз методів, який показав, що для захисту мультимедійних об'єктів ефективнішими будуть широкосмугові та статистичні методи. Використання інших методів потребує великих затрат часу або ресурсів, тому їх запровадження можна вважати недоцільним.

1. *Грибунин В.Г., Оков И.Н., Туринцев И.В*. Цифровая стеганография – М.: СОЛОН-ПРЕСС, 2009 – 272 с.

2. *Горпенюк А.Я., Стороженко А.О.* Дослідження та порівняльний агаліз стеганографічних методів для впровадження даних у цифрові файли, електронний ресур [http://ena.lp.edu.ua]

3. *Сагайдак Д.А., Файзуллин Р.Т*. Способ формирования цифрового водяного знака для физических и электронных документов, Компьютерная оптика, том 38, №1, 2014 – с.94-104.

http://doi.org/10.5281/zenodo.3859689

Поступила 30.09.2019р.