УДК 621.391.7

А. О. Азарова
Я. В. Чайковська

МЕТОД ЗАХИСТУ ПРОЦЕСІВ ЕЛЕКТРОННОГО ВРЯДУВАННЯ ШЛЯХОМ КВАНТУВАННЯ

Вінницький національний технічний університет

Анотація
В роботі розглянуто та детально проаналізовано вразливість стеганографічних алгоритмів вбудовування цифрових водяних знаків в PDF файли, а саме на основі квантування.
Ключові слова: стеганографія, PDF файли, цифрові водяні знаки.

Abstract
The paper considers and analyzes in detail the vulnerability of the steganographic algorithms for embedding digital watermarks into PDF files, in particular quantization.
Keywords*:* steganography, PDF files, digital watermarks.

Вступ

У сучасному світі стеганографічні методи широко застосовуються в системах безпеки. При цьому забезпечення цілісності на сьогодні є не менш актуальною задачею, ніж забезпечення конфіденційності інформації. Цифрові водяні знаки сьогодні є діючим інструментом для захисту авторських прав різних цифрових документів, отже потребують аналізу та вдосконалення.

Метою роботи є аналіз вразливостей стеганографічних алгоритмів для вбудовування цифрових водяних знаків.

Результати дослідження

Сьогодні методи цифрової стеганографії широко використовуються для захисту інформації та інформаційної безпеки. В їх основу покладено модифікацію цифрових контейнерів – стегоконтейнерів з метою непомітного впровадження певних бітових послідовностей. Основні напрями застосування стеганографічних алгоритмів: надсилання стегоповідомлень, вбудовування цифрових водяних знаків (ЦВЗ) (watermarking) та ідентифікаційних номерів (ІН) (fingerprinting), вбудовування заголовків (captioning) [1]. ЦВЗ здебільшого використовують з метою захисту авторських прав та уникнення незаконного копіювання і використання цифрової інформації. ЦВЗ можуть бути помітними та непомітними. За надійністю ЦВЗ поділяють на крихкі, напівкрихкі та надійні. Надійні ЦВЗ використовуються у системах захисту інформації від несанціонованного копіювання. При цьому ЦВЗ у PDF файлах повинні бути непомітними для людини, щоб забезпечити належну якість, що особливо важливо для використання. Тому мінімізація візуальних викривлень або застосування маскування є однією з основних умов для практичної реалізації стеганографічного алгоритму для вбудовування ЦВЗ. Виділяють декілька способів вбудовування ЦВЗ. Адитивні методи основані на додаванні до вибраної підмножини відліків оригінального цифрового контейнера згенерованої послідовності псевдовипадкових чисел. В алгоритмах злиття у оригінальний контейнер вбудовується певне інформаційне повідомлення значно меншого обсягу. Перевагою таких методів є допустимість незначних викривлень у оригінальному контейнері, а також можливість вбудовування певної корисної інформації, яка є надійнішим підтвердженням прав власності на інформацію, ніж послідовність псевдовипадкових чисел [2].

Існуючі методи, що вирішують задачу захисту авторського права шляхом вбудовування ЦВЗ, можна розділити на дві групи [2]: група методів, які приховують інформацію в просторовій області зображення та методи, що вбудовують ЦВЗ в частотну область. Методи першої групи вбудовують інформацію безпосередньо в первинну область даних файлу, що робить їх нестійкими до багатьох спотворень, особливо до компресії з втратами. Це призводить до часткового чи навіть повного знищення вбудованого ЦВЗ. Більш стійкими до різного роду спотворень та компресії є методи другої групи. До відомих методів відносяться методи на основі використання дискретного косинус перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення

Карунена-Лоєва та ін. [2]. Найбільш поширеними перетвореннями в стеганографії є ДКП та вейвлетперетворення, тому що крім можливості використання в стеганографічних перетвореннях, вони ефективно використовуються під час ущільнення зображень.

У роботі [3] запропоновано метод приховування інформації з розширенням спектра, що використовує вейвлет-перетворення; в роботі [4] – метод вбудовування інформації зі збереженням гістограми контейнера, який гарантує його точне відтворення; в роботі [5] докладно розглянуто застосування, аналіз та оцінку стеганографічних методів на прикладі PDF файлів. У роботах [6–8] висвітлено різні методи виявлення прихованої інформації у PDF файли.

Також було розглянуто вбудовування ЦВЗ в PDF файли за допомогою методу розширення спектра в роботі [9]. У запропоновано новий метод вбудовування ЦВЗ на основі перетворень конформної алгебри. Було розглянуто і аналіз властивостей з погляду вбудовування ЦВЗ у PDF файли у роботі [10]. Отже, існують алгоритми, що забезпечують успішне приховування інформації та додавання цифрових водяних знаків у PDF файли. Разом з тим, переважна більшість розроблених методів призначена для використання у PDF файли без стиснення. При цьому не була розглянута проблема створення PDF файли для приховування інформації та додавання цифрових водяних знаків у PDF файли зі стисненням без втрат (loseless). Отже, залишаються актуальними розроблення та практична реалізація нових стеганографічних методів, що можуть бути застосовані для використання як контейнер подібних PDF файлів.двох різних повідомлень при використанні одного і того ж сеансового та приватного ключа, тому актуальним залишається питання і підвищення стійкості цих методів цифрового підписування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.
2. Азарова А. О. Вибір, планування та реалізація стратегії розвитку підприємства [Текст] / А. О. Азарова, Н. С. Желюк // Актуальні проблеми економіки, №12. – 2010. – С. 91–100.
3. Азарова А. О. Розробка методики визначення економічної безпеки підприємства [Текст] / А. О. Азарова, О. В. Гаврилова // Збірник наукових праць «Економіка: проблеми теорії та практики». – Дніпропетровськ : ДНУ, 2004. – Вип.191, т. III. – С. 719–727.
4. Азарова А. О. Математичні моделі оцінювання стратегічного потенціалу підприємства та прийняття рішень щодо його підвищення [Текст] / А. О. Азарова, О. В. Антонюк. — Вінниця : ВНТУ, 2012. – 168 с.
5. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.
7. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації" / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
8. Свідоцтво про реєстрацію авторського права на твір №79707. Розробка контролеру кодового доступу до сейфа на мікроконтролері Arduino / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80960. Дата реєстрації 14.06.2018 р.
9. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах" / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.
10. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.

Чайковська Янна В'ячеславівна — бакалавр, Вінницький національний технічний університет, Вінниця, e-mail: yanna.chaikovska@gmail.com.

Науковий керівник: ***Азарова Анжеліка Олексіївна*** — к.т.н., проф. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету, м. Вінниця, e-mail: azarova.angelika@gmail.com.

Chaikovska Yanna — bachelor degree, Vinnitsa National Technical University, Vinnitsa, e-mail: yanna.chaikovska@gmail.com.

Supervisor: ***Yaremchuk Yuriy E.*** — Ph.D., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.