УДК 004.415.24/004.56.5

Н.В. КОШКІНА

Інститут кібернетики ім. В.М. Глушкова Національної академії наук України
просп. Академіка Глушкова, 40, Київ, 03680, Україна

СТІЙКІ ДО АКТИВНИХ АТАК МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

За матеріалами наукового повідомлення на засіданні Президії НАН України 26 грудня 2012 року

Наведено результати дослідження наявних і розроблення нових методів комп'ютерної стеганографії для зображень та аудіосигналів. Розглянуто проблему десинхронізації цифрового водяного знака з контейнером-носієм. Виконано аналіз впливу типових операцій оброблення контейнера на його амплітудний спектр. Наведено приклади створених методів вкраплення цифрових водяних знаків, стійких до стиснення із втратами, зашумлення, низькочастотної фільтрації, зсуву, повороту, масштабування, обрізування, друку-сканування та інших активних атак. Окреслено можливі сфери застосування цих методів.

Ключові слова: інформаційна безпека, стеганографія, цифрові водяні знаки, стійкість, десинхронізація, контейнери-зображення, аудіоконтейнери.

У сучасному суспільстві значна кількість послуг здійснюється за допомогою комп'ютерних мереж та інформаційних технологій, невпинний розвиток яких надзвичайно загострює проблему інформаційної безпеки. Найбільшого поширення в Україні та світі набула така наука про методи забезпечення конфіденційності й автентичності інформації, як криптографія. Проте існують важливі завдання інформаційної безпеки, які не можна розв'язати криптографічними методами. Криптографія, зокрема, не приховує сам факт існування конфіденційної інформації та її передавання по відкритому каналу зв'язку. Вирішити цю проблему можна, застосовуючи методи комп'ютерної стеганографії, яка вкраплює таємну інформацію в типові для певного середовища цифрові об'єкти-носії. При цьому перцепційна якість носіїв (контейнерів) не погіршується, тобто вкраплення не помітне і не привертає уваги сторонніх спостерігачів.

Деякі завдання захисту інформації вирішуються як криптографічними, так і стеганографічними методами. Це, наприклад, задача автентифікації цифрових даних, яку можна розв'язати, застосувавши технологію електронного цифрового підпису (ЕЦП), що впроваджено в Україні на законодавчому рівні. Таку задачу можна вирішити й за допомогою технології цифрових водяних знаків (ЦВЗ) — одного з напрямів комп'ютерної стеганографії. ЦВЗ мають корисні властивості, які зумовлюють їх незамінність порівняно з криптографічними методами:

- ЦВЗ перцепційно не помітні і не потребують збільшення розміру контейнерів, що підлягають захисту;
- ЦВЗ невіддільні від контейнерів-носіїв і, на відміну від спеціальних заголовків або ЕЦП, не можуть бути вилучені без втрати

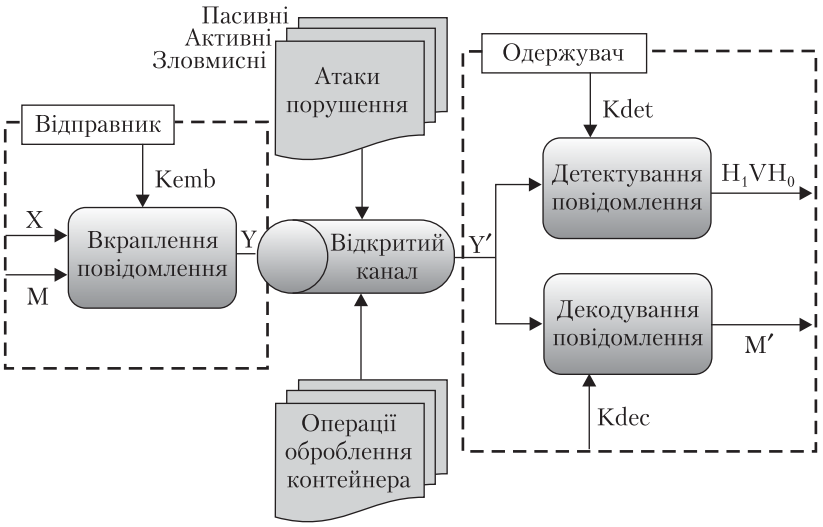

Рис. 1. Узагальнена схема функціонування стеганографічної системи

надійності сприйняття маркованих контейнерів;

• контейнер і вкраплений у нього цифровий водяний знак підлягають однаковим перетворенням, що дає можливість досліджувати ці перетворення навіть у разі спотворення чи видалення ЦВЗ;

• ЦВЗ дозволяють підтвердити автентичність даних не лише при їх збереженні «біт-у-біт», але й у разі зміни формату їхнього зберігання або, наприклад, передачі контейнера по зашумленому каналу зв'язку.

Наведені приклади свідчать про важливість і актуальність розвитку методів комп'ютерної стеганографії. Ця наука дедалі частіше привертає увагу вчених України. Проблематику комп'ютерної стеганографії досліджували й висвітлювали у своїх монографіях В.Г. Грибунін [1], О.В. Аграновський [2], В.О. Хорошко, М.Є. Шелест [3], Г.Ф. Конахович, О.Ю. Пузиренко [4]. Упродовж понад 10 років розвитком стеганографії займається також колектив відділу № 140 Інституту кібернетики ім. В.М. Глушкова НАН України.

Комп'ютерна стеганографія розвивається в кількох напрямах, що мають як багато спільних рис, так і певні характерні відмінності, зумовлені особливостями практичного застосування. Зокрема, серед стеганосистем виділяють системи прихованого передавання даних і системи цифрових водяних знаків.

Системи прихованого передавання даних використовують для організації таємної комунікації. Оригінальний вміст контейнера X не відіграє жодної ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача вкрапленого в нього повідомлення M (рис. 1).

Разом з тим факт відправлення контейнера від відправника до одержувача не повинен виглядати дивним, а також не має бути помітних відхилень контейнера від норми. Основна мета таких систем — приховати наявність стеганоканалу, унеможливити розрізнення пустих і заповнених контейнерів без знання таємного ключа. Системи прихованого передавання даних зазвичай будують так, щоб протидійна відносно легальних користувачів стеганосистеми сторона (порушник) не мала можливості втрутитися в контейнер і змінити дані, що передаються. Однак при цьому порушник здатен здійснювати пасивні атаки, спрямовані на виявлення стеганоконтейнерів. Результатом їх подальшого аналізу може стати оцінка секретних параметрів системи та читання

прихованих повідомлень. Для систем прихованого передавання даних потрібна суттєво вища, ніж для систем ЦВЗ, пропускна здатність стеганоканалу, під якою розуміють відношення розміру контейнера до розміру повідомлення.

Інший вид стеганосистем — системи ЦВЗ, актуальні для багатьох практичних застосувань, таких як завадостійка автентифікація аудіо- та візуальних даних (зокрема, контроль цілісності знімків камер спостереження, записів телефонних розмов), автентифікація власника (захист авторських прав), автентифікація джерела даних, контроль телевізійного та радіомовлення, контроль копіювання тощо. Користувачі стеганосистем ЦВЗ мають не один, а два об'єкти інформаційного інтересу — передусім їх цікавить власне контейнер, але не менш важливим є і вкраплене повідомлення. Основна мета таких систем — зберегти цілісність повідомлення після певного ряду можливих модифікацій стеганоконтейнера. Характерними атаками виступають:

— *активні атаки порушника*, тобто такі, що змінюють дані контейнера з метою знищення або спотворення ЦВЗ;

— *зловмисні атаки порушника*, тобто атаки, спрямовані на отримання оцінки секретних параметрів системи, що дасть можливість виконувати функції легальних користувачів;

— *ненавмисні атаки сторонніх осіб*, спричинені обробленням контейнера з метою поліпшення його якості (з погляду об'єкта, на який спрямована дія, ці атаки також можна вважати активними).

Цифровий водяний знак має порівняно невеликий розмір, що дає змогу вкрапити його так, щоб забезпечити стійкість до потенційно можливих ненавмисних і активних атак.

Збереження вкрапленої інформації після модифікацій контейнера-носія, що не спричиняють втрату його перцепційної якості, — одна з базових вимог до систем ЦВЗ. Автором досліджено наявні методи вирішення цього завдання і розроблено ефективні нові.

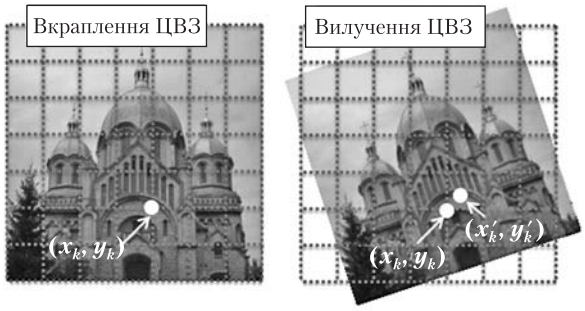

Рис. 2. Десинхронізація ЦВЗ у контейнері-зображенні

У процесі досліджень було здійснено класифікацію можливих спотворень контейнерів за різними основами. Так, усі можливі спотворення поділяються на два класи: спотворення значень елементів контейнера (шумоподібні) — $f'(x_k, y_k) = f(x_k, y_k) + \xi$ та спотворення місцеположень елементів контейнера (геометричні) — $(x_k, y_k) \rightarrow (x'_k, y'_k)$. Геометричні спотворення не призводять до знищення цифрового водяного знака, однак є причиною десинхронізації ЦВЗ із контейнером і, як наслідок, неможливості вилучення водяного знака без знання його нового місцеположення (x'_k, y'_k) (рис. 2).

Ефективна система ЦВЗ серед інших вимог має забезпечувати синхронізацію водяного знака з контейнером-носієм. Зважаючи на це, було виконано дослідження та порівняльний аналіз методів синхронізації ЦВЗ [5], зокрема методів на базі шаблонів, структурних ЦВЗ, особливих точок, перетворення Радона та перетворення Фур'є – Мелліна.

Проведений аналіз показав перспективність подальшого вивчення і розвитку методів на основі особливих точок, оскільки вони є досить універсальними, використовують оригінальні дані контейнера і не привносять у нього додаткових шумів. Крім того, синхронізуючу інформацію неможливо видалити без відчутного спотворення контейнера, і паралельно із забезпеченням синхронізації можна ідентифікувати ділянки, не придатні для вкраплення (гладкі).

Приклади конкретних методів маркування, які було розроблено й реалізовано:

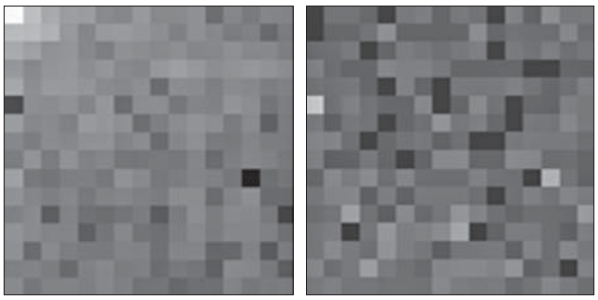

Рис. 3. Фрагмент низькочастотної ділянки спектра зображення і різниця спектрів оригіналу (зліва) та скан-копії (справа) для цього фрагмента

• методи вкраплення ЦВЗ у зображення із синхронізацією на базі особливих точок, виділених за допомогою детектора кутів Харріса [6, 7];

• методи вкраплення ЦВЗ у цифрову музику, що ґрунтуються на властивостях перетворення Фур'є та вейвлет-перетворення [8, 9];

• метод вкраплення ЦВЗ у мовні сигнали із синхронізацією на базі особливих точок, що визначаються у вейвлет-субсмугах сигналу як місцеположення значних стрибків енергії [10].

Тестування стійкості цих методів до активних атак, зокрема стиснення із втратами, геометричних перетворень (зсуву, масштабування, повороту, обрізування), низькочастотної фільтрації та зашумлення, показало або 100% збіг вкрапленого та вилученого ЦВЗ, або результат, що приводиться до вищенаведеного шляхом застосування кодів корекції помилок. Це свідчить про можливість практичного застосування розробок.

Сучасні системи ЦВЗ, як правило, спрямовані на захист цифрових даних. Тому алгоритми, що входять до їх складу, адаптовані до специфіки цифрових каналів передавання даних. Наприклад, багато алгоритмів вкраплення ЦВЗ у зображення враховують специфіку стандарту стиснення із втратами JPEG [1], що дозволяє їм бути стійкими до цього виду атак за побудовою. Разом з тим технології ЦВЗ можна з успіхом застосовувати і для захисту інформації на паперових або пластикових носіях, що дасть можливість значно розширити сферу потенційних користувачів цих технологій. Комерційна доступність перцепційно якісного перетворення аналогової інформації в цифрову форму і навпаки зумовлює необхідність пошуку нових засобів протидії підробленню важливих документів: паспортів, водійських прав, посвідчень особи, довідок, договорів, пластикових карток тощо. З цієї ж причини затребувані й ефективні методи захисту авторських зображень, які щодня друкуються у ЗМІ, методи, що дозволяють контролювати безпечність факсимільного зв'язку тощо.

Для захисту паперових документів використовують, наприклад, гільйош, але він є видимим, що не завжди зручно (маркування фото людини, написів тощо). Крім того стеганотехнології дозволяють приховати наявність такого рівня захисту для користувачів, що не мають секретного ключа.

Зважаючи на актуальність завдання захисту інформації на паперових носіях, було розроблено низку методів вкраплення ЦВЗ у зображення, стійких до процесів друку та сканування. Ці методи є спектральними і ґрунтуються на властивостях дискретного перетворення Фур'є (ДПФ). Перш ніж їх створити, було проведено ряд теоретичних досліджень, зокрема, класифіковано наявні під час друку-сканування спотворення і вивчено їх вплив на коефіцієнти ДПФ зображення. В результаті було виявлено ділянки, які під час друку-сканування спотворюються найменше і дозволяють виконати модифікації зі збереженням візуальної якості контейнера, — це низькочастотні коефіцієнти амплітудного спектра з високими амплітудами [11].

Справедливість теоретичних міркувань було підтверджено експериментально. Так, на рис. 3 подано результати експерименту, в якому зображення було роздруковане на струминному принтері *Epson Stylus Photo R220* з роздільною здатністю 720 dpi, а потім відскановане на планшетному сканері *HP scanjet 4400c* з роздільною здатністю 300 dpi.

У лівій частині рисунка представлено амплітудний спектр вихідного зображення, де темні пікселі відповідають низьким амплітудам. У правій частині — відповідна попередньому фрагменту різниця спектрів оригінального та відсканованого зображень, де світлі пікселі відповідають максимальному спотворенню. Неважко помітити, що темні пікселі зліва чітко відповідають світлим пікселям справа.

Далі було запропоновано вкраплювати у низькочастотні коефіцієнти спектра з високими амплітудами біти ЦВЗ або за допомогою заміни молодших значущих бітів відповідних коефіцієнтів, або змінюючи відносне значення пар цих коефіцієнтів. У комбінації з кодами корекції помилок це дозволяє зберегти цілісність ЦВЗ після друку та сканування носія.

Також було запропоновано модифікацію методу відносної заміни значень коефіцієнтів дискретного косинусного перетворення [4], стійку до друку-сканування. Стійкості до цієї атаки вдалося досягти збільшенням розміру блоків зображення-контейнера до величини, за якої спектральні коефіцієнти блоків оригіналу та його скан-копії є достатньо близькими за значеннями, тобто завдяки впровадженню так званого зонального підходу [12].

Загалом ці та інші отримані результати можна використовувати в інформаційних системах військового призначення, сфері урядового зв'язку, для захисту цінних паперів від фальсифікації, захисту права власності на авторські об'єкти, що друкуються в ЗМІ, розміщуються в Інтернеті чи в будь-який інший спосіб доступні широкому загалу. Під час розгляду судових справ системи ЦВЗ, частиною яких є розроблені методи, дають можливість визначити власника, довести цілісність і оригінальність спірного цифрового або роздрукованого об'єкта. Певну частину розробок можна використовувати для захисту від незаконного копіювання, відстежування джерела порушень ліцензійних угод та вирішення інших завдань інформаційної безпеки.

СПИСОК ЛІТЕРАТУРИ

1. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.
2. *Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В.* Основы компьютерной стеганографии. — М.: Радио и связь, 2003. — 152 с.
3. *Хорошко В.А., Шелест М.Е.* Введение в компьютерную стеганографию. — К: Національний авіаційний університет, 2002. — 152 с.
4. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. — К.: МК-Пресс, 2006. — 288 с.
5. *Кошкина Н.В.* Методы синхронизации цифровых водяных знаков // Кибернетика и системный анализ. — 2008. — № 1. — С. 180–188.
6. *Кошкина Н.В.* О методе защиты интеллектуальной собственности на основе выделения точечных особенностей изображения // Захист інформації. — 2007. — № 4. — С. 52–63.
7. *Кошкина Н.В.* Стойкая к геометрическим преобразованиям система маркировки изображений // Питання оптимізації обчислень: матер. XXXV міжнар. конф. (24–29 вересня 2009, Ялта, Україна). — Т. 1. — С. 351–355.
8. *Кошкина Н.В.* Определение инварианта к сжатию с потерями для аудиосигналов // УСИМ. — 2010. — № 3. — С. 86–93.
9. *Кошкина Н.В.* Метод встраивания цифровых водяных знаков в аудиосигналы на основе вейвлет- и Фурье-преобразований // Проблемы управления и информатики. — 2010. — № 6. — С. 134–143.
10. *Кошкина Н.В.* Самосинхронизирующаяся система ЦВЗ для аудиосигналов // Проблемы управления и информатики. — 2012. — № 2. — С. 136–145.
11. *Кошкина Н.В.* Выделение инварианта для процесса печати и сканирования в задачах компьютерной стеганографии // УСИМ. — 2007. — № 1. — С. 30–38.
12. *Кошкина Н.В.* О стеганографических методах защиты информации на бумажных носителях // Компьютерная математика. — 2007. — № 1. — С. 68–76.

Н.В. Кошкина

Институт кибернетики им. В.М. Глушкова
Национальной академии наук Украины
просп. Академика Глушкова, 40, Киев, 03680, Украина

СТОЙКИЕ К АКТИВНЫМ АТАКАМ МЕТОДЫ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Приведены результаты исследований существующих и разработки новых методов компьютерной стеганографии для изображений и аудиосигналов. Рассмотрена проблема десинхронизации цифрового водяного знака с контейнером-носителем. Выполнен анализ влияния типичных операций обработки контейнера на его амплитудный спектр. Приведены примеры созданных методов внедрения цифровых водяных знаков, стойких к сжатию с потерями, зашумлению, низкочастотной фильтрации, сдвигу, повороту, масштабированию, обрезке, печати-сканированию и другим активным атакам. Показаны возможные области применения этих методов.

Ключевые слова: информационная безопасность, стеганография, цифровые водяные знаки, стойкость, десинхронизация,контейнеры-изображения,аудиоконтейнеры.

N.V. Koshkina

Glushkov Institute of Cybernetics
of National Academy of Sciences of Ukraine
40 Glushkov Ave., Kyiv, 03680, Ukraine

METHODS OF COMPUTER STEGANOGRAPHY THAT ARE ROBUST TO THE ACTIVE ATTACKS

The report presents the results of examination of the existing methods and developing some new methods of computer steganography for images and audio-signals. The problem of desynchronization between digital watermark and its carrier was studied. The analysis of effects of typical processing operations for cover signal on its amplitude spectrum was performed. The examples of the developed methods of watermarking that are robust to lossy compression, additive noise, low-pass filtering, shift, rotation, scaling, cropping, print-scan and other active attacks are given. Also the possible applications of these methods are shown.

Keywords: information security, steganography, digital watermark, robustness, desynchronization, image carrier, audio-carrier.

Наталія КОШКІНА

Кандидат фізико-математичних наук,
старший науковий співробітник Інституту кібернетики ім. В.М. Глушкова НАН України.

У 1999 р. закінчила Сумський державний педагогічний університет ім. А.С. Макаренка, з 2001 по 2004 рр. навчалася в аспірантурі, а з 2010 р. є докторантом Інституту кібернетики ім. В.М. Глушкова НАН України. 2005 року захистила кандидатську дисертацію на тему «Ефективні спектральні алгоритми для вирішення задач цифрової стеганографії» (науковий керівник — чл.-кор. НАН України, доктор фізико-математичних наук В.К. Задірака).

Є автором та співавтором більш ніж 30 наукових праць.

Лауреат Премії Президента України для молодих учених 2012 р. (разом з кандидатами фізико-математичних наук О.Ю. Нікітіною та І.В. Швідченко).

Коло наукових інтересів — інформаційна безпека, стеганографія, стеганоаналіз, дискретні ортогональні перетворення, цифрове оброблення сигналів і зображень.