УДК 004:34

В. Г. ІВАНОВ,
д-р техн. наук, проф.;
М. Г. Любарський,
д-р фіз.-мат. наук, проф.;
В. В. Карасюк,
канд. техн. наук, доц.;
Ю. В. Ломоносов,
канд. техн. наук, доц.,
Національний університет
«Юридична академія України
імені Ярослава Мудрого»,
м. Харків

ЗАХИСТ АВТОРСЬКИХ ПРАВ МУЛЬТИМЕДІЙНИХ ДАНИХ

Розглянуто питання надійного захисту інформації з використанням сучасних засобів і методів стеганографии. Показано можливість використання для захисту авторських прав аудіо- і відеофайлів за допомогою впровадження в них прихованих об'єктів – цифрових водяних знаків (ЦВЗ).

Ключові слова: мультимедійні дані, захист авторських прав, цифрові водяні знаки.

Сучасна практика повсякденної діяльності людини та суспільства характеризується неухильним зростанням ступеня використання інформації й нових інформаційних технологій. Інформація сьогодні з категорії наукової перетворилася на категорію суспільно-економічну, виступає таким же важливим і необхідним елементом розвитку суспільства, як сировина і енергія. Інформація є стратегічним ресурсом суспільства, що визначає рівень розвитку держави, його економічний потенціал. Наприклад, за деякими даними, обсяг витрат на розвиток інформаційної сфери в США перевищує витрати на розвиток паливно-енергетичного комплексу цієї країни.

Тому інтенсивне зближення інтересів права та інформатики сьогодні є об'єктивним і закономірним процесом, що свідчить про гостру необхідність у взаємному використанні результатів новітніх досягнень, отриманих цими науками. Це виявляється у двох взаємопов'язаних аспектах – прикладному і змістовному, а саме: використанні останніх досягнень в галузі інформаційних технологій, пристосованих або спеціально розроблених для розвитку і функціонування юридичної науки та практики, з одного боку, і юридичному

закріпленні питань, пов'язаних з упровадженням у будь-яку сферу суспільних відносин цих інформаційних технологій, – з іншого.

З розвитком інформаційного суспільства зростають потоки інформації, швидкості її обробки та розповсюдження, у зв'язку з чим виникає гостра потреба у захисті інтересів суб'єктів, що використовують у своїй діяльності інформацію, природа якої не укладається у звичні форми предметів правових відносин. Тому дуже важливо знайти такі правові механізми, які забезпечать правове регулювання нового класу суспільних відносин – інформаційних, що дозволить економічно ефективно розвивати дану галузь людської діяльності з виробництва та використання інформації, а також протистояти різним порушенням і злочинам у цьому середовищі.

Наприклад, відкрити сторінку в Інтернеті або розтиражувати книгу на CD-R набагато простіше, швидше й дешевше, ніж налагодити випуск і збут друкарській продукції. Достатньо лише придбати один примірник твору і сканер для його оцифрування. Проте в результаті вказаних дій автор твору, безумовно, позбавляється винагороди, на яку він міг би розраховувати при звичайному обороті примірників його твору на ринку.

При захисті прав автора сайту виникає проблема ідентифікації мережевих інформаційних ресурсів як об'єкта права: чи є вони різновидом бази даних або програмою для комп'ютера, чи можна віднести сайт до засобів масової інформації, який правовий статус мережевої публікації і так далі. Тому, попри явні переваги електронних засобів запису, передачі та обробки інформації виникає маса технологічних і правових питань, пов'язаних з дотриманням майнових інтересів володарів авторських прав.

Забезпечення надійного захисту інформації від несанкціонованого доступу є однією з якнайдавніших і дотепер не вирішених проблем [2; 5; 6]. Способи і методи утаєння секретних повідомлень відомі з давніх часів, причому дана сфера людської діяльності отримала назву *стеганографія*. Цей термін походить від грецьких «steganos» (секрет, таємниця) і «graphy» (запис) і,

таким чином, означає буквально «тайнопис». Також для захисту інформації з давніх часів інтенсивно використовувалися методи криптографії.

Як відомо, мета криптографії полягає у блокуванні несанкціонованого доступу до інформації шляхом шифрування секретних повідомлень. Стеганографія має інше завдання, її мета – приховати сам факт існування секретного повідомлення. При цьому обидва способи можуть бути поєднані й використані для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів) [1; 3; 4; 7; 8].

Для захисту авторських прав на аудіо- і відеофайли використовується запровадження в них прихованих об'єктів – «Цифрових водяних знаків» (ЦВЗ), що досягається шляхом непомітної для людського ока або вуха зміни файлу.

ЦВЗ можуть містити певний автентичний код, тобто закодовану інформацію про власника або інформацію управління. Найбільш поширеними об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, як правило, логотипи.

На відміну від друкарського водяного знаку, який є чим-небудь видимим (наприклад, логотип), цифровий водяний знак створюється так, щоб бути невидимим, або у випадку з аудіо кліпами – нечутним. Більш того, біти, що представляють водяний знак, повинні бути розкидані всередині файлу так, щоб вони не могли бути ідентифіковані або змінені. Цифровий водяний знак повинен бути стійким, щоб витримувати такі зміни файлу, як масштабування, обертання, компресія з втратами (lossy compression) та ін.

Невидимі ЦВЗ аналізуються спеціальним декодером, який покликаний виносити ухвалу про їх валідність.

У даний час методи комп'ютерної стеганографії розвиваються у двох основних напрямах: використання спеціальних властивостей комп'ютерних форматів; цифрова обробка сигналів, заснована на надмірності аудіо і візуальної інформації. Перший напрям базується на використанні спеціальних властивостей комп'ютерних форматів представлення даних, а не на надмірності самих даних. Спеціальні властивості форматів вибираються з урахуванням

захисту прихованого від безпосереднього прослуховування повідомлення, перегляду або прочитання (наприклад, використовується вільний кластерний простір файлів).

Основним напрямом комп'ютерної стеганографії є використання надмірності аудіо- і візуальної інформації. Цифрова фотографія – це матриця чисел, що представляють інтенсивність світла в певний момент часу. Цифровий звук – це матриця чисел, що представляє інтенсивність звукового сигналу в моменти часу, що проходять послідовно. Усі ці числа не є точними, оскільки не точні пристрої оцифрування аналогових сигналів є шуми квантування. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку і візуального образу. Їх заповнення відчутно не впливає на якість сприйняття, що і дає можливість для утаєння додаткової інформації

Наприклад, графічні кольорові файли з схемою змішення RGB кодують кожну точку малюнка трьома байтами. Кожна така точка складається з адитивних складових: червоного, зеленого, синього. Зміна кожного з трьох найменш значущих біт призводить до зміни менше 1 % інтенсивності даної точки. Це дозволяє приховувати в стандартній графічній картинці об'ємом 800 Кбайт близько 100 Кбайт інформації, що не помітно при перегляді зображення.

Інший приклад. Тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт у стерео режимі дозволяє приховати за рахунок заміни найменш значущих молодших розрядів на приховуваному повідомлення близько 10 Кбайт інформації. При цьому зміна значень відліків складає менше 1 %. Така зміна практично не виявляється при прослуховуванні файлу більшістю людей

Вбудовування повідомлення в цифровий контейнер (зображення або аудіо-файл) може проводитися за допомогою ключа (одного або декількох). Ключ – псевдовипадкова послідовність (ПСП) біт, породжувана генератором, що задовольняє певним вимогам (криптографічний безпечний генератор). Як основа для роботи генератора може використовуватися, наприклад, лінійний

рекурентний регістр. Тоді адресатам для забезпечення зв'язку може повідомлятися початкове заповнення цього регістра. Числа, що породжуються генератором ПСП, можуть визначати позиції відліків, що модифікуються, у разі фіксованого контейнера або інтервали між ними у разі потокового контейнера.

Існує й інша сторона питання. Комп'ютерні технології дозволяють змінити будь-яке зображення до повного невпізнання, й у разі необхідності досвідчені фахівці-фальсифікатори можуть зробити монтаж так, що виявити фальсифікацію буде практично неможливо. У той же час у деяких випадках дуже важливо знати, була здійснена підробка отриманого цифрового зображення чи ні. Мова йде про відбитки пальців, фотографії з місця злочину, результати різного роду експертиз, фотографічні докази дослідницьких експериментів і т. д. Без маркування цифровими водяними знаками тут просто не обійтися. За бажанням за допомогою цифрових водяних знаків можна захистити не тільки зображення, поширювані в Інтернеті, але і взагалі будь-які зображення, зокрема такі офіційні документи, як водійські права, паспорт і т. п.

Для визначення достовірності отриманої інформації, тобто її аутентифікації, зазвичай використовуються засоби цифрового підпису. Проте вони не зовсім підходять для забезпечення аутентифікації мультимедійної інформації. Річ у тім, що повідомлення, забезпечене електронним цифровим підписом, повинне зберігатися і передаватися абсолютно точно, «біт у біт». Мультимедійна ж інформація може трохи спотворюватися як при зберіганні (за рахунок стиснення), так і при передачі (вплив одиночних або пакетних помилок в каналі зв'язку). При цьому її якість залишається допустимою для користувача, але цифровий підпис працювати не буде. Одержувач не зможе відрізнити істинне, хоча і дещо спотворене повідомлення, від помилкового. Крім того, мультимедійні дані можуть бути перетворені з одного формату в інший. При цьому традиційні засоби захисту цілісності працювати також не будуть.

Можна сказати, що ЦВЗ здатні захистити саме зміст аудио-, відеоповідомлення, а не його цифрове представлення у вигляді послідовності

біт. Крім того, важливим недоліком цифрового підпису є те, що його легко видалити із завіреного ним повідомлення, після чого приробити до нього новий підпис. Видалення підпису дозволить порушникові відмовитися від авторства або ввести в оману законного одержувача щодо авторства повідомлення.

Для ефективного виявлення підробки зображення може бути використана техніка маркування «водяними знаками», за допомогою якої позначаються невеликі блоки зображення.

Однією з перших технікою, вживаною для виявлення спотворень (модифікації) зображення, була техніка, заснована на впровадженні контрольних сум в найменший значущий біт (LSB). Уелтон [9; 10] запропонував техніку, в якій використовується залежна від ключа псевдовипадкова послідовність, що переміщується («гуляє») по зображенню. Контрольна сума будується з семи старших бітів і вставляється в LSB вибраних пікселів. Контрольну суму роблять такою, що переміщується («гуляє») для того, щоб запобігти модифікації груп пікселів з тією ж контрольною сумою.

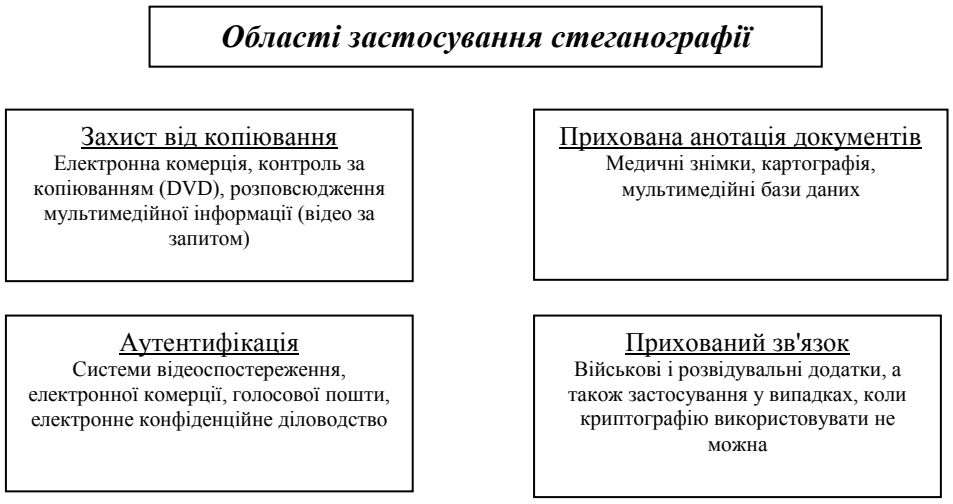

Рисунок. Потенційні сфери застосування стеганографії

Таким чином, як видно з рисунку, застосування ЦВЗ не обмежується застосуваннями безпеки інформації. Основні області використання технології ЦВЗ можуть бути об'єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації й прихований зв'язок.

Унаслідок того, що обробка будь-яких зображень у середовищі загальнодоступних графічних пакетів не являє особливої складності, зображення з друкарськими (видимими) водяними знаками ніколи не приймаються як речовий доказ. Таким чином, друкарський водяний знак не може вважатися юридичним доказом авторського права на зображення, наприклад, у суді. Якщо зображення були помічені тільки друкарськими водяними знаками, то у разі підозри в крадіжці пошук оригіналу в базах даних зображень для визначення власника авторського права – важке і дуже дороге завдання.

У той же час дослідження зображення з цифровим водяним знаком на наявність авторства провести дуже легко. Для цього достатньо запустити спеціальну програму, наприклад, EIKONAmark, і провести ідентифікацію на предмет наявності конкретного ідентифікаційного номера. Програма практично миттєво підтвердить авторство або повідомить про те, що зображення не було ідентифіковане і як таке, що належить конкретному авторові.

Варто відзначити, що підписувати свої графічні роботи сьогодні стало нормою, і відповідними програмами користуються як професіонали, так і аматори. Призначене для цих цілей ПЗ достатньо дешеве і різноманітне. Серед застосувань, що є на ринку, можна знайти і професійні пакети з широкими можливостями з редагування створюваних водяних знаків, і безкоштовні програми – прості та з мінімумом варіантів обробки міток, що вставляються.

Програма Photo WaterMark дозволяє швидко захистити фотографії від незаконного копіювання за рахунок накладення друкарських водяних знаків. Водяний знак можна або створити в середовищі даної програми (як текстовий або мальований об'єкт) і тут же впровадити в одне або декілька зображень, або скористатися раніше створеним водяним знаком, вставивши його як графічний файл. У пакеті зручно організовано операції з корегування водяного знаку – його можна повертати, застосовувати спецефекти, змінювати його прозорість (зокрема до нуля, роблячи водяний знак невидимим), положення і розміри (є можливість автоматичної підгонки розміру і положення водяного знаку, зміни

параметрів шрифту і заливки). Додатково можна вказати на зображенні відомості про дату і час, а також про фотоапарат, яким робилися знімки.

На відміну від друкарського, побачити цифровий водяний знак без спеціальної програми, яка може ідентифікувати достовірність зображення, неможливо.

ПЗ даного класу орієнтоване більшою мірою на крупні компанії, часто не має демонстраційних версій і коштує достатньо дорого, тому зупинимося лише на двох пакетах, що мають розраховані на фотографів-професіоналів і навіть на аматорів відносно дешеві версії. З їх основними функціями можна ознайомитися на практиці перед придбанням.

Digimarc – провідна компанія на світовому ринку в галузі розробки спеціалізованого ПЗ для впровадження цифрових водяних знаків. Її додатки для захисту авторського права використовують такі компанії, як Adobe, Hewlett-Packard, Macrovision, Philips, Hitachi, і багато інших. Цифрові водяні знаки, створені за технологією Digimarc, дозволяють користувачам включати в аудіозаписи, зображення, відеофільми і друкарські документи цифровий код, який абсолютно непомітний і в той же час легко ідентифікується.

Провідний пакет від Digimarc – MyPictureMarc – вставляє цифрові водяні знаки за технологією Digimarc (знак ©, персональну інформацію про ваш ID і низку додаткових даних), які повністю підтверджують авторське право на зображення.

Модуль MarcSpider Tracking, що входить до MyPictureMarc Professional, є спеціальним модулем для відстежування зображень з авторськими знаками в усіх публічно відкритих областях Інтернету, де торгують цифровим контентом. Про результати пошуку складається регулярний звіт з інформацією про те, де і коли були знайдені ваші зображення.

Дуже проста в роботі програма EIKONAmark призначена для трансформації ідентифікаційного номера власника авторського права (ID) в невидиму цифрову мітку і вставки її в зображення. Ідентифікаційний номер може бути доповнений логотипом автора, який також буде вставлений як

невидима водяна мітка. Як логотип можуть використовуватися тільки бінарні зображення. EIKONAmark дуже зручно застосовувати для захисту авторського права і визнання авторства цифрових зображень у разі їх незаконного копіювання і використання, оскільки вона без проблем дозволяє визначити наявність або відсутність в зображенні конкретного цифрового водяного знаку.

Існує ще один великий клас технічних засобів захисту авторських прав, які отримали назву Digital Rigths Managment (DRM) – управління цифровими правами. Це технологія, а точніше, технології, що створюють захист від копіювання мультимедійного контента і що забезпечують тим самим дотримання авторських прав.

Зазвичай засоби DRM супроводжують твори (файли, диски), що захищаються, а також вбудовуються в засоби відтворення (програми-оболонки для перегляду, кишенькові, DVD-програвачі) і запису (DVD-рекордери, Video Capture cards).

Хоча DRM покликані перешкодити лише неправомірному копіюванню творів, як правило, вони не допускають, або обмежують будь-яке копіювання, зокрема, оскільки неможливо технічними засобами автоматично відрізнити «законне» копіювання від «незаконного».).

Таке обмеження можливостей користувача викликає критику DRM з боку правозахисників, що змусило основного розробника цієї технології компанію Apple практично відмовитися від використання DRM на користь вільного використання цифрового контента в мережі Інтернет.

Список літератури:

1. *Алиев А. Т.* Вопросы построения криптостеганографических систем. Модель стеганографического канала передачи данных / А. Т. Алиев, А. В. Аграновский // Информационное противодействие угрозам терроризма. – 2006. – № 8. – С. 79–91.

2. *Грибунин В. Г.* Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 261 с.

3. *Кошкина Н. В.* Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы / Н. В. Кошкина // Проблемы управления и информатики. – 2010. – № 5. – С. 132–144.

4. *Кустов В. Н.* Методы встраивания скрытых сообщений / В. Н. Кустов, А. А. Федчук // Защита информации. Конфидент. – 2002. – № 3. – С. 34–37.

5. *Хорошко В. А.* Введение в компьютерную стеганографию / В. А. Хорошко, М. Е. Шелест. – К. : НАУ, 202. – 140 с.

6. *Хорошко В. О.* Основи комп'ютерної стеганографії : навч. посіб. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчик. – Вінниця : Вінницький держ. техн. ун-т, 2003. – 143 с.

7. *Швидченко И. В.* Анализ криптостеганографических алгоритмов / И. В. Швидченко // Проблемы управления и информатики. – 2007. – № 4. – С. 149–155.

8. *Швидченко И. В.* Криптостеганографический алгоритм с использованием методов сегментации / И. В. Швидченко // Проблемы управления и информатики. – 2010. – № 5. – С. 145–153.

9. *Schyndel R.G. van.* A Digital Watermark / R.G. van Schyndel, A. Z. Tirkel, and C. F. Osbome // Proc. of the IEEE Int. Conf. on Image Processing. – Austin, Texas, Nov. 1994. – Vol. 2. – P. 86-90.

10. *Walton S.* Information Authentication for a Slippery New Age / S. Walton // Ur. Dobbs Journal. – Apr 1995. – Vol. 20. – № 4. – P. 18–26.

Иванов В. Г., Любарский М. Г., Карасюк В. В., Ломоносов Ю. В. **Защита авторских прав мультимедийных данных.**

Рассмотрены вопросы надежной защиты информации с использованием современных средств и методов стеганографии. Показана возможность использования для защиты авторских прав аудио и видеофайлов при помощи внедрения в них скрытых объектов – цифровых водяных знаков (ЦВЗ).

Ключевые слова: мультимедийные данные, защита авторских прав, цифровые водяные знаки.

Ivanov V.G., Lyubarskiy M.G., Karasyuk V.V., Lomonosov Y.V. **Defence of copyrights by multimedia information.**

The questions of reliable priv are examined with the use of modern tools and methods of стеганографии. Possibility of the use for defence of copyrights is rotined audio and videofiles through introduction in them of the hidden objects – digital thread-marks.

Key words: multimedia information, defence of copyrights, digital thread-marks.