УДК 004:34

В.Г. Іванов, М.Г. Любарський, В.В. Карасюк, Н.А. Кошева, Ю.В. Ломоносов

Національний університет «Юридична академія України імені Ярослава Мудрого», Харків

ІДЕНТИФІКАЦІЯ І ЗАХИСТ МУЛЬТИМЕДІЙНИХ ДАНИХ

У роботі наголошується, що з розвитком інформаційного суспільства ростуть потоки інформації, швидкості її обробки і розповсюдження, і у зв'язку з цим виникає гостра необхідність в захисті інтересів суб'єктів, що використовують інформацію в своїй діяльності. Розглядаються питання надійного захисту інформації з використанням сучасних засобів і методів стеганографии. Показана можливість захисту авторських прав аудіо і відеофайлів за допомогою впровадження в них прихованих об'єктів – цифрових водяних знаків (ЦВЗ). Це досягається шляхом непомітної для людського ока або вуха зміни файлу. ЦВЗ можуть містити деякий автентичний код, тобто закодовану інформацію про власника або інформацію управління.

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

Постановка проблеми

Сучасний світ переживає фундаментальні й динамічні зміни, пов'язані з бурхливим розвитком новітніх інформаційних технологій. В економіках розвинених держав світу з кожним роком збільшується питома вага галузей виробництва інтелектуальних продуктів, зокрема об'єктів авторського права. В останні роки у зв'язку з інтенсивним розвитком мультимедійних технологій дуже гостро постало питання захисту авторських прав та інтелектуальної власності, представленої в цифровому вигляді [1, 2]. Особливо актуальною ця проблема стала з розвитком загальнодоступних комп'ютерних мереж, зокрема, мережі Internet. В даний час завдання захисту від несанкціонованого копіювання та забезпечення аутентифікації вирішуються, окрім заходів організаційно-юридичного характеру, також з використанням технологій цифрових водяних знаків (ЦВЗ), які були реалізовані на основі досягнень теорії та практики сучасної науки стеганографії. Ці досягнення викликані реакцією суспільства на актуальну проблему захисту авторських прав в умовах існування у глобальному комп'ютерно-інформаційному середовищі.

Тому, не дивлячись на очевидні переваги електронних засобів запису, збереження, передачі і обробки інформації виникає маса технологічних і правових питань, пов'язаних з дотриманням майнових інтересів володарів авторських прав. Аналізу та систематизації цих питань і присвячена представлена стаття.

Порівняльний аналіз сучасних технічних методів захисту авторських прав і інтелектуальної власності

Забезпечення надійного захисту інформації від несанкціонованого доступу є однією з якнайдавніших і не вирішених до теперішнього часу проблем [3 – 5]. Способи і методи утаєння секретних повідомлень відомі з давніх часів, причому дана сфера людської діяльності отримала назву **стеганографія.** Це слово походить від грецьких слів steganos (секрет, таємниця) і graphy (запис) і, таким чином, означає буквально "тайнопис". Також для захисту інформації інтенсивно використовувалися методи криптографії, які використовувалися з давніх часів.

Як відомо, мета криптографії полягає в блокуванні несанкціонованого доступу до інформації шляхом шифрування секретних повідомлень. Стеганографія має інше завдання, і його мета – приховати сам факт існування секретного повідомлення. При цьому, обидва способи можуть бути об'єднані і використані для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів) [6, 7, 8].

Так для захисту авторських прав на аудіо і відео файли використовується впровадження в них прихованих об'єктів – "Цифрових водяних знаків" (ЦВЗ), що досягається шляхом непомітного для людського ока або вуха зміни файлу [7, 8].

ЦВЗ можуть містити деякий автентичний код, тобто закодовану інформацію про власника або інформацію управління. Найбільш відповідними 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 усередині 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) і ін.

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

В даний час методи комп'ютерної стеганографії розвиваються двома основними напрямами:

1. Методи, засновані на використанні спеціальних властивостей комп'ютерних форматів;

2. Методи цифрової обробки сигналів, засновані на надмірності аудіо і візуальної інформації.

Перший напрям заснований на використанні спеціальних властивостей комп'ютерних форматів представлення даних, а не на надмірності самих даних. Спеціальні властивості форматів вибираються з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або прочитання (наприклад, використовується вільний кластерний простір файлів).

Основним напрямом комп'ютерної стеганографії є використання надмірності аудіо і візуальної інформації [9, 10, 11, 12, 13]. 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 послідовно йдуть. Всі ці числа не точні, 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

Так, графічні кольорові файли з схемою змішення RGB кодують кожну точку малюнка трьома байтами. Кожна така точка складається з аддитивних складових: червоного, зеленого, синього. Зміна кожного з трьох найменш значущих біт приводить 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 прогляданні зображення.

Інший приклад. Тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт в 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.

Є і інша сторона питання. Комп'ютерні технології дозволяють змінити будь-яке зображення до повного невпізнання, і при необхідності досвідчені фахівці-фальсифікатори можуть зробити монтаж так, що виявити фальсифікацію буде практично неможливо. В той же час в 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 так далі Без маркіровки цифровими водяними знаками тут просто не обійтися. За бажання 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 тому подібне.

Для визначення достовірності отриманої інформації, тобто її аутентифікації, зазвичай використовуються засоби цифрового підпису. Проте, ці засоби не зовсім підходять для забезпечення аутентифікації мультимедійної інформації. Річ у тім, що повідомлення, забезпечене електронним цифровим підписом, повинне зберігатися і передаватися абсолютно точно, «біт в 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 маркіровки «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 [14, 15] запропонував техніку, в якій використовується залежна від ключа псевдовипадкова послідовність, що перемішується («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.

Необхідно сказати, що застосування ЦВЗ не обмежується застосуваннями безпеки інформації. Основні області використання технології ЦВЗ можуть бути об'єднані в чотири групи (рис. 1): захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації і прихований зв'язок.

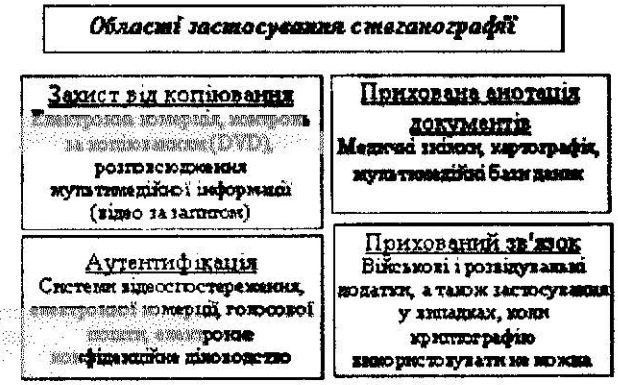

Рис. 1. Потенційні області застосування стеганографії

Внаслідок того, що обробка будь-яких зображень в середовищі загальнодоступних графічних пакетів не представляє 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, в 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.

В той же час дослідження зображення з цифровим водяним знаком на наявність авторства – хвилинна справа. Для цього досить 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 визнати, що підписувати свої графічні роботи сьогодні стало нормою, і відповідними програмами користуються як професіонали, так і любителі. Призначене для цих цілей ПЗ достатньо дешеве і різноманітне. Серед застосувань, що є на ринку, можна знайти і професійні пакети з широкими можливостями по редагуванню створюваних водяних знаків, і безкоштовні програми – прості і з мінімумом варіантів обробки міток, що вставляються.

Програма Photo WaterMark дає можливість швидко захистити фотографії від незаконного копіювання за рахунок традиційного накладення друкарських водяних знаків. Водяний знак можна або створити в середовищі даної програми (як текстовий або мальований об'єкт) і тут же упровадити в одне або декілька зображень, або скористатися раніше створеним вами водяним знаком, вставивши його як графічний файл. У пакеті зручно організовані операції по корегуванню 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.

У відмінності від друкарського, побачити цифровий водяний знак без спеціальної програми, яка по його наявності в змозі ідентифікувати достовірність зображення, неможливо.

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

Digimarc – провідна компанія на світовому ринку, в області 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 ряд додаткових даних), які повністю підтверджують авторське право на зображення.

Модуль MarcSpider Tracking, що входить в MyPictureMarc Professional, є спеціальним модулем для відстежування зображень з авторськими знаками у всіх 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 Internet.

Висновки

Аналіз тенденцій розвитку комп'ютерної стеганографії показує наявність невирішених проблем Internet, таких як захист авторського права, захист прав на особисту тайну, організація електронної торгівлі, комп'ютерна злочинність і кібертероризм.

Останнім часом завдяки бурхливому розвитку IT-технологій, цифрових апаратно-програмних засобів з'явилися нові можливості для цифрової стеганографії. Надзвичайно висока затребуваність стегопродукції пов'язана з наявністю у неї унікальних споживчих якостей, що дозволяють вбудовувати, приховувати спеціальне повідомлення в файл-контейнери, що містять у цифровому вигляді звук або зображення. Вже створені і вільно поширюються через Internet десятки стегопрограм, що говорить про початок формування ринку цієї спеціальної продукції. Але тут є багато проблем, які вимагають розв'язання:

- розробка методів перешкодостійкої аутентифікації;
- розробка методів захисту інформації від несанкціонованого копіювання;
- розробка методів відстеження поширення інформації з мереж зв'язку;
- розробка методів пошуку інформації в мультимедійних базах даних;
- розробка стійких до зовнішніх дій методів формування ЦВЗ;
- розробка методів не виявлення ЦВЗ в мультимедійних даних.

Аналіз тенденцій розвитку комп'ютерної стеганографії показує, що в найближчі роки інтерес до розвитку її методів буде посилюватися все більше і більше. Передумови до цього вже сформувалися. Зокрема, загальновідомо, що актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, бурхливий розвиток інформаційних технологій забезпечує можливість реалізації нових методів захисту.

Список літератури

1. Інтеграція права й інформатики: прикладний та змістовний аспекти / В.Г. Іванов, В.Ю. Шепітько, М.Г. Любарський та ін.; За заг. ред. В.Г. Іванова, В.Ю. Шепітька – Х.: Право, 2012 – 250 с.

2. Основи інформатики та обчислювальної техніки: Підручник / В.Г. Іванов, В.В. Карасюк, М.В. Гвозденко; За заг. ред. В.Г. Іванова. – Х.: Право, 2012. – 312 с.

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

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

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

6. 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.

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

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

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

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

11. Іванов В.Г. Сжатие изображений на основе автоматической и нечеткой классификации фрагментов / В.Г. Іванов, Ю.В. Ломоносов, М.Г. Любарский // Проблемы управления и информатики. – К.,2009. – № 1. – С. 52-63.

12. Иванов В.Г. Сокращение содержательной избыточности изображений на основе классификации объектов и фона / В.Г. Іванов, Ю.В. Ломоносов, М.Г. Любарский // Проблемы управления и информатики. – К., 2007. – № 3. – С. 93-102.

13. Кошкина Н.В. Самосинхронизирующаяся система робастных цифровых водяных знаков для речевых сигналов / Н.В. Кошкина // Проблемы управления и информатики. – 2012. – № 2. – С. 136 -145.

14. S. Walton, «Information Authentication for a Slippery New Age», Ur. Dobbs Journal, vol. 20, no. 4. – P. 18-26, Apr 1995.

15. R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, «A Digital Watermark», Proc. of the IEEE Int. Conf. on Image Processing, vol. 2, pp. 86-90, Austin, Texas, Nov 1994.

Надійшла до редколегії 5.10.2012

Рецензент: д-р техн. наук. проф. В.Б. Дудикевич, Національний університет «Львівська Політехніка», Львів.

ИДЕНТИФИКАЦИЯ И ЗАЩИТА МУЛЬТИМЕДИЙНЫХ ДАННЫХ

В.Г. Иванов, М.Г. Любарский, В.В. Карасюк, Н.А. Кошева, Ю.В. Ломоносов

В работе отмечается, что с развитием информационного общества растут потоки информации, скорости ее обработки и распространения, и в связи с этим возникает острая необходимость в защите интересов субъектов, использующих информацию в своей деятельности. Рассматриваются 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). Это достигается путем незаметного для человеческого глаза или уха изменения файла. ЦВЗ могут содержать некоторый аутентичный код, т.е. закодированную информацию о собственнике либо управляющую информацию.

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

AUTHENTICATION AND PROTECTION OF MULTIMEDIA DATA

V.G. Ivanov, M.G. Lyubarskiy, V.V. Karasyuk, N.A. Kosheva, Y.V. Lomonosov

It is in-process marked that the threads of information, speeds of its treatment and distribution, grow with development of informative society, and in this connection there is a sharp necessity for defence of interests of subjects, utillizings information in the activity. 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. It is arrived at by unnoticeable for a human eye or ear of change of file. Digital thread-marks can contain some authentic code, I.e. the coded information about an owner or managing information.

***Keywords:** multimedia information, defence of copyrights, digital thread-marks.*

УДК 681.3.06

Р.В. Королев

Харьковский университет Воздушных Сил им. Ивана Кожедуба, Украина

АНАЛИЗ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ RC4

В работе проведены исследования зависимости расположения единичного элемента в S-блоке с значениями индексных элементов i, j, использование которых приводит к формированию псевдослучайных последовательностей малого периода.

***Ключевые слова:** генератор псевдослучайных чисел, RC4.*

Введение

Постановка проблемы. Существенное повышение производительности микропроцессоров в 90-е годы обусловило в криптографии усиление интереса к программным методам реализации шифроалгоритмов — как к возможной альтернативе аппаратным схемам на регистрах сдвига. Одним из самых первых программных криптоалгоритмов, получивших широкое распространение, стал алгоритм RC4.

Алгоритм RC4 — это поточный шифр с переменной длиной ключа, разработанный в 1987 году Рональдом Райвистом для компании RSA Data Security. Как и его «компаньон», блочный шифр RC2,