

ЗАХИСТ АВТОРСЬКИХ ПРАВ І ЗМІСТУ ЦИФРОВИХ ДАНИХ

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, які використовують в своїй діяльності інформацію, встає питання про захист авторських прав на інтелектуальну власність, яка представлена у цифровому вигляді.

Задача надійного захисту інформації від несанкціонованого доступу є однією з якнайдавніших і не вирішеної остаточно до теперішнього часу проблеми [1, 2, 3, 4]. Способи і методи приховування секретних повідомлень відомі з давніх часів, причому, дана сфера людської діяльності отримала назву *стеганографія*.

Як відомо, мета криптографії полягає в блокуванні несанкціонованого доступу до інформації шляхом шифрування секретних повідомлень. Стеганографія має інше завдання, і її мета – приховати сам факт існування секретного повідомлення.

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

ЦВЗ можуть містити певний автентичний код, тобто закодовану інформацію про власника або інформацію управління. Для зображення 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.

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

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. Основним напрямом комп'ютерної стеганографії є використання надмірності аудіо і візуальної інформації [4, 5]. Цифрова фотографія – це матриця чисел, що представляють інтенсивність світла в певний момент часу. Цифровий звук – це матриця чисел, що представляє інтенсивність звукового сигналу в послідовні моменти часу. 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 приховування додаткової інформації

Є і інший бік 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. При бажанні 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.

Проведений аналіз тенденцій розвитку комп'ютерної стеганографії показує, що найближчими роками інтерес до розвитку цих методів посилюватиметься все більше і більше. Сильним каталізатором цього процесу є лавиноподібний розвиток комп'ютерної мережі загального користування Internet, зокрема такі невирішені суперечливі проблеми Internet, як захист авторського права, захист прав на особисту таємницю, організація електронної торгівлі, протиправна діяльність хакерів, терористів і тому подібне.

Література:

1. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 261 с.
2. *Хорошко В.А., Шелест М.Е.* Введение в компьютерную стеганографию. – К.: НАУ, 202. – 140 с.;
3. *Кошкина Н.В.* Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы // Проблемы управления и информатики. – 2010. – № 5. – С. 132-144. ;
4. *Иванов В.Г., Ломоносов Ю.В., Любарский М.Г.* Сжатие изображений на основе автоматической и нечеткой классификации фрагментов // Проблемы управления и информатики. – К. – 2009. – № 1– С. 52-63.;
5. *Иванов В.Г., Любарский М.Г., Ломоносов Ю.В.* Сокращение содержательной избыточности изображений на основе классификации объектов и фона // Проблемы управления и информатики. – К. – 2007. – № 3. – С. 93-102.