

УДК 004:34

Н.А. Кошева

inform@nulau.edu.ua

Національний університет «Юридична академія України імені Ярослава Мудрого»

## ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТА ПЕРСПЕКТИВИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

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 сформувався. 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. І звичайно, сильним каталізатором цього процесу є лавиноподібний розвиток Internet, в тому числі такі невіршені суперечливі проблеми Internet, як захист авторського права, захист прав на особисту таємницю, організація електронної торгівлі, комп'ютерна злочинність та кібертероризм

У зв'язку з широким розповсюдженням мультимедійних ІТ технологій в останнє десятиліття почалося бурхливе зростання кількості робіт в області цифрової (комп'ютерної) стеганографії. Слово «стеганографія» в перекладі з грецького означає «тайнопис». На відміну від криптографії, методи якої дозволяють зашифрувати повідомлення, методи стеганографії дозволяють приховати сам факт повідомлення. До початку 90-х років цією наукою займалося небагато вчених, оскільки вона носила закритий характер, але останнім часом завдяки бурхливому розвитку ІТ-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 в цифровому вигляді звук або зображення. Вже створені і вільно поширюються через Internet десятки стегопрограм, що говорить про початок формування ринку цієї спеціальної продукції. На сьогоднішній день склалися такі області застосування стеганографії:

- 1) вбудовування інформації з метою її прихованої передачі;
- 2) вбудовування цифрових водяних знаків (ЦВЗ) - watermarking;
- 3) вбудовування ідентифікаційних номерів - fingerprinting;
- 4) вбудовування заголовків - captioning.

Одним з найбільш ефективних методів захисту авторських прав та інтелектуальної власності, представленої у цифровому вигляді, є вбудовування в об'єкт, що захищається невидимих міток - ЦВЗ. Назву метод вбудовування цифрових водяних знаків (watermarking) отримав від відомого способу захисту цінних паперів від підробки. ЦВЗ, на відміну від звичайних водяних знаків, можуть бути як видимими, так і не видимими. Спеціальний декодер аналізує невидимі ЦВЗ і виносить рішення щодо їх коректності. Самі ЦВЗ, поміщені в нерухомі зображення, аудіо-та відео-файли, містять автентичний код, інформацію про власника, керуючу інформацію.

Багато спільного з методом ЦВЗ має метод вбудовування ідентифікаційних номерів виробників (fingerprinting). Назва цього методу дослівно перекладається як «відбитки пальців», і кожна захищена за допомогою цього методу копія має свій унікальний вбудований номер. Наявність ідентифікаційного номера дозволяє виробникові відслідковувати подальшу долю свого продукту. «Відбитки пальців» швидко вкажуть на зловмисника, якщо хто-небудь з покупців зайнявся незаконним тиражуванням.

Для підпису медичних знімків, нанесення легенди на карту застосовується метод невидимого вбудовування заголовків (captioning). Метою в цьому випадку є дотримання лікарської таємниці і компактне зберігання різномірної інформації як єдиного цілого.

Метод вбудовування цифрової інформації з метою її прихованої передачі розробляється в закритому режимі в спеціалізованих організаціях для створення прихованих систем управління та обміну інформацією в глобальному масштабі.

Оскільки розробка методів цифрової стеганографії почалася зовсім недавно, то тут є багато проблем, які вимагають розв'язання:

- Розробка методів перешкодостійкої аутентифікації;
- Розробка методів захисту інформації від несанкціонованого копіювання;
- Розробка методів відстеження поширення інформації по мережах зв'язку;
- Розробка методів пошуку інформації в мультимедійних базах даних.