УДК 004.415.5
О. Ізбянський
(Тернопільський національний технічний університет імені Івана Пулюя)

ДОСЛІДЖЕННЯ СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДО РІЗНОГО ВИДУ АТАК

В наш час інформація перетворюється на найдорожчий ресурс. На сьогодні в інформаційному просторі, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Комп'ютерні системи активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. Внаслідок цього проблеми захисту інформації набули великої актуальності задля попередження заподіяння збитку інтересам власника інформації.

Одним із способів захисту даних є використання цифрової стеганографії, що базується на приховуванні інформації в цифрових об’єктах. Цифровий водяний знак (ЦВЗ) – це технологія створена для вирішення проблеми захисту авторських прав на певну комп’ютерну інформацію. Останнім часом ЦВЗ активно впроваджується в ІТ-бізнес, як спосіб захисту авторських прав на розроблене програмне забезпечення.

Алгоритм використання ЦВЗ для захист авторських правможе виглядати наступним чином:

1. Власник інформації вбудовує в ЦВЗ в предмет інтелектуальної власності за допомогою спеціалізованого програмного забезпечення. ЦВЗ може містити ідентифікаційні дані власника) або ж алгоритм ЦВЗ буде спрямований лише на присутність чи відсутність знаку.

2. Власник розповсюджує файл, захищений ЦВЗ для широкого загалу.

3. При виникненні конфлікту власник зможе довести право власності на об'єкт.

Загалом ЦВЗ можуть бути видимими та невидимими. Існують два основних типи накладання ЦВЗ:

- в просторовій області (метод заміни найменш значущого біту, метод псевдовипадкового інтервалу, метод блокового приховування та ін);
- в частотній області (метод Коха і Жао, метод Хсу і Ву та ін).

Методи першої групи передбачають приховування інформації в пікселях видимого зображення. Для методів другої групи необхідно провести спектральний аналіз зображення з допомогою рядів Фур'є чи вейвлет-перетворень. Отриманий спектр використовується для приховування ЦВЗ в певних частотах зображення.

Дослідження стійкості методів ЦВЗ до різного типу атак є основною метою стеганоаналізу, зокрема, для отримання якісних і кількісних оцінок надійності використовуваного стеганоперетворення, а також побудова методів виявлення приховуваної в контейнері інформації, її модифікації або руйнування.

За рівнем забезпечення таємності стеганосистеми поділяються на теоретично стійкі, практично стійкі і нестійкі системи. Основними видами атак, які проводяться на стеганосистему є:

- атаки проти вбудованого повідомлення;
- атаки проти стегодетектора;
- атаки проти протоколу використання ЦВЗ;
- атаки проти безпосередньо ЦВЗ.

В доповіді більш детально буде розкрито методики накладання цифрових водяних знаків на зображення, проаналізовано стійкість алгоритмів ЦВЗ для різних типів файлів та різного типу атак.