ВИДИ АТАК НА СТЕГОСИСТЕМУ ТА ЗАХИСТ ВІД НИХ

Грицюк В.К.
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14,
каф. Інформаційно – мережної інженерії, тел. (057) 702-14-29)

In this publication, we consider the types of attacks on the stegosystem and methods for countering them.

Steganography is a communication method. The task of steganography is to hide the very fact of the existence of secret data during its transmission, storage or processing. In other words, hiding the existence of information means not only the impossibility of detecting a hidden message in an intercepted message, but also generally making it impossible to raise any suspicions about this. A common feature of steganographic methods is that the hidden message is embedded in a certain object (container) that does not attract attention, which is then openly forwarded to the addressee.

Існує два принципово різних способу передачі по відкритому каналу зв'язку конфіденційної інформації. Один із способів полягає в тому, щоб замаскувати передану секретну інформацію іншої інформацією. В цьому випадку секретні символи вбудовуються у відкритий текст. Завдання вбудовування та виділення повідомлень з іншої інформації виконує стегосистема. Стегосистема ж утворює стегоканал, по якому передається приховане повідомлення. Цей канал вважається підданим впливам з боку порушників.

Порушник може бути пасивним, активним і зловмисним.

Пасивний порушник може лише виявити факт наявності стегоканала і (можливо) читати повідомлення.

Діапазон дій активного порушника значно ширше. Приховане повідомлення може бути їм видалено або зруйновано.

Дії злочинного порушника найбільш небезпечні. Він здатний не тільки руйнувати, а й створювати помилкові стего.

Для здійснення тієї чи іншої загрози порушник застосовує атаки.

1. Атаки проти вбудованого повідомлення – спрямовані на видалення або псування ЦВЗ шляхом маніпулювання стего. Прикладами таких атак можуть бути лінійна фільтрація, стиск зображення, додавання шуму, вирівнювання гістограми, зміна контрастності і т. д.

2. Атаки проти стегодетектора – спрямовані на те, щоб ускладнити чи зробити неможливою правильну роботу детектора. При цьому водяний знак у зображенні залишається, але втрачається можливість його прийому. У цю категорію входять такі атаки, як афінне перетворення (тобто масштабування, зрушення, повороти), усічення зображення, перестановка пікселів і т. д.

3. Атаки проти протоколу використання ЦВЗ – в основному пов'язані зі створенням хибних ЦВЗ, помилкових стего, інверсією ЦВЗ, додаванням кількох ЦВЗ.

4. Атаки проти самого ЦВЗ – спрямовані на оцінювання і витяг ЦВЗ з стегоповідомлення. У цю групу входять такі атаки, як атаки змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації.

Відповідно до цієї класифікації всі атаки на системи вбудовування ЦВЗ можуть бути розділені на чотири групи:

1) атаки, спрямовані на видалення ЦВЗ;

2) геометричні атаки, спрямовані на спотворення контейнера;

3) криптографічні атаки;

4) атаки проти використовуваного протоколу вбудовування та перевірки ЦВЗ.

Для підвищення надійності стегосистем можна запропонувати ряд поліпшень.

Різні методи протидії пропонувалися для вирішення проблеми прав власності. Перший спосіб полягає в побудові незворотного алгоритму ЦВЗ. ЦВЗ повинен бути адаптивним до сигналу і вбудовуватися за допомогою односпрямованої функції, наприклад, хеш – функції.

Другий спосіб вирішення проблеми прав власності полягає у вбудовуванні в ЦВЗ деякої тимчасової позначки, що надається третьою, довіреної стороною. У разі виникнення конфлікту особа, яка має на зображенні більш ранню тимчасову позначку, вважається справжнім власником.

Для захисту від атак типу афінного перетворення можна використовувати додатковий (опорний) ЦВЗ. Цей ЦВЗ не несе в собі інформації, але використовується для «реєстрації» виконуваних порушником перетворень. У детекторі ЦВЗ є схема, що виконує зворотне перетворення.

Іншим методом захисту від подібних атак є блоковий детектор. Модифіковане зображення розбивається на блоки, і для кожного блоку аналізуються всі можливі спотворення. Для кожної зміни визначається коефіцієнт кореляції ЦВЗ. Перетворення, після якого коефіцієнт кореляції виявився найбільшим, вважається реально виконаним порушником.

Перелік використаних джерел

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН – ПРЕС, 2002. – 270 с.

2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. – М.: Горячая линия – Телеком, 2010.