Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

©Автори статей, 2011
©Упорядкування, Вінницький національний технічний університет, 2011

УДК 004.056

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ КЛЮЧОВОЇ ІНФОРМАЦІЇ

О. П. Войтович, к.т.н., доцент;
П. В. Козлюк, асистент;
А. І. Гладьо, студент
Вінницький національний технічний університет
o_voytovych@mail.ru

На сьогодні досить важливим є питання збереження ключової інформації на серверах, що підключені до глобальної мережі Інтернет. Існує досить велика кількість способів взломати сервер, в тому числі основаних на тому, що найбільш важлива інформація зберігається в базах даних. Найчастіше зловмисники направляють основні зусилля на взлом баз даних. Альтернативою зберігання ключових даних у базах даних є їх захист за допомогою стеганографічних систем.

Для того щоб приховати ключову інформацію сервера в зображеннях пропонується використовувати модифікацію алгоритму теорії графів (Стефан Хетцль і Петра Мютцель). Основним принципом є модифікація значень елементів таким чином, що при поблочному зчитуванні за модулем m, отримується секретне повідомлення. Дані в блоках не змінюються, а лише обмінюються. Як стеганоконтейнери використовуються зображення типу JPEG та JPEG2000, а вибірками є коефіцієнти ДКП і вейвлет-перетворення.

Нехай v та w будуть двома вершинами:

$$v = (\{p1, \ldots, pk\}, \{t1, \ldots, tk\});$$
$$w = (\{q1, \ldots, qk\}, \{u1, \ldots, uk\}),$$

де p та q – координати вибірок, а t і u – значення яких їм необхідно надати.

Існує ребро, що з'єднує значення і-ої вибірки зі значенням j-ї вибірки w, і запусується як (v, w)i, j $\in$ E, якщо v(spi) = uj; w(sqj) = ti.

Процес створення графу такий:

1. Створюється масив суміжностей. Для кожного значення s_i (елемент зображення, що використовується) створюється список можливих змін у визначеному радіусі r.

2. Створюється структура розповсюдженості вибіркових значень.

3. Сортування вершин по рангу – кількості ребер, що з'єднані з даною вершиною.

Спочатку обмінюються вершини, що мають найменший ранг для забезпечення більшої кількості вершин з парами. Вершини, що не мають пар змінюють своє значення на необхідне.

Для того щоб отримати дані, їх необхідно зчитати поблочно з зображення за модулем r у порядку визначеним секретним ключем.

Для вбудовування ключових даних у зображеннях, пропонується використовувати окремий програмний продукт, доступ до якого має лише головний адміністратор. Дані про кожний з серверів приховуються в окремому зображенні, таким чином створюючи альбом. Вважається, що альбом має резервну копію, для захисту від активних атак. При роботі через мережу Інтернет рекомендується використовувати 2048-розрядні SSL-сертифікати.

Таким чином, система працює аналогічно таким, що використовують бази даних для збереження інформації, але при цьому самі дані зберігаються у вигляді зображень, що рідко виступають об'єктами атак. Інформація про кожний сервер зберігається в окремому зображенні, і навіть якщо зловмисник зможе зчитати дані про один сервер – інші дані залишатимуться невідомими.