УДК 004.056

Р. Г. Казаков
М. А. Очкуров

АЛГОРИТМ ДЛЯ ПРИХОВУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ У ЦИФРОВОМУ ЗОБРАЖЕННІ

Вінницький національний технічний університет.

Анотація

Запропоновано удосконалений алгоритм для приховування інформації, який базується на комбінації стеганографічного алгоритму LSB та криптографічного RSA.

Ключові слова: стеганографія, алгоритм LSB, алгоритм RSA, приховування інформації, зображення контейнера.

Abstract

An advanced algorithm is proposed for hiding information based on a combination of the LSB steganography algorithm and the RSA cryptographic.

Keywords: steganography, LSB algorithm, RSA algorithm, information hiding, container image.

Вступ

В наш час, коли кількість використання цифрових ресурсів досягає величезних обсягів, дослідження і впровадження стеганографії все більше схоже на вимушену міру [1-3]. Спілкування і обмін інформацією щоденно безлічі користувачів, що доволі часто є особистою справою, супроводжується незаконним копіюванням і розповсюдженням даних, нерідко навіть із метою збагачення. В результаті таких дій підвищується бажання до захисту особистої інформації та приватного обміну даними.

Стеганографія (із грецьк. steganos – секрет, таємниця; graphy – запис) – це приховування інформації в об'єктах різних форматів, при цьому повідомлення вбудоване в контейнер, що не привертає уваги, звісно, якщо не знати про факт існування такого повідомлення [4]. Це і є основна відмінність від криптографії. Але слід зазначити, що стеганографія ні в якому разі не є заміна криптографії, а скоріше її доповнення. Якщо додаткову інформацію приховати методами стеганографії, то буде зменшена ймовірність виявлення факту передачі інформації. Якщо ж додатково таку інформацію ще і зашифрувати, то отримаємо додатковий рівень захисту.

Приховування текстової інформації

За основу даного алгоритму вибрано вже відомий LSB, але з певними модифікаціями. Для початку було запропоновано вбудовувати приховану інформацію не тільки в найменш значущі біти, а і в молодші. Це підвищило б обсяги приховуваного повідомлення. Але разом з цим виріс би відсоток спотворень і втрачалась суть використання стеганографічних методів, тому що чим більше спотворень тим легше помітити факт передачі неозброєним оком.

Крім того є певні методи виявлення вкраплень інформації у мультимедійні файли. Наприклад, метод RS-атак або метод Хі-квадрат [5, 6]. Суть Хі-квадрата полягає в тому, щоб здійснювати атаку на один з каналів RGB, після чого привести обрахунки кожного з каналів до середнього арифметичного тим самим отримуючи результат вихідного зображення. Базується Хі-

квадрат на припущені того, що ймовірність появи сусідніх кольорів, які різняться між собою найменш значущим бітом, в порожньому стеганоконтейнері дуже мала. Тобто кількість пікселів двох сусідніх кольорів значно відрізняються для пустого контейнера і для виявлення необхідно всього лише порахувати кількість пікселів кожного кольору та застосувати кілька формул.

Слід також пам'ятати, що застосування Хі-квадрата буде більш ефективним, якщо це робити не до всього зображення, а до окремих його частин. Наприклад до рядків. Таким чином, якщо обрахована ймовірність для рядка буде більше 0.5, то в даному рядку є вкраплена інформація.

Тому альтернативним варіантом залишився той самий LSB, але із зміненою послідовністю заміни найменш значущих бітів. За допомогою генератора псевдовипадкових чисел послідовність з лінійної стає довільною, що зводить до мінімуму можливість виявлення за допомогою методу Хі-квадрата. Також покращена версія алгоритму приховування повідомлення передбачає додатковий захист у вигляді криптографічного алгоритму, який додає до приховування факту передачі повідомлення його шифрування. І тоді навіть у разі виявлення вкрапленого повідомлення потрібно буде додатково розшифрувати його вміст.

Обраним алгоритмом став RSA, фундаментом якого є властивості простих, але дуже великих чисел. Для створення ключа обирається два великих простих числа. Чим більші числа використовуються, тим більш крипто-стійкими вони будуть вважатись. Наприклад, UNIX-програма ssh-keygen генерує ключі довжиною 1024 біта за замовчуванням. Така довжина ключа є мінімальною для алгоритму RSA в силу його особливостей. А для асиметричних алгоритмів заснованих на теоріях при використанні еліптичних кривих, мінімально надійною довжиною ключа є 163 біта, хоча рекомендованою є довжина від 191 біта [7].

RSA алгоритм дозволяє шифрувати інформацію в кількох режимах [8]:

– таємний ключ відправника, у такому разі повідомлення може розшифрувати будь-яка людина, яка має в наявності відкритий ключ.

– відкритий ключ отримувача, дає змогу дешифрувати повідомлення власнику таємного ключа, але процес дешифровки буде успішним при наявності відкритого ключа, тому що вони є парними

– таємний ключ відправника та відкритий ключ отримувача повідомлення, тільки тоді повідомлення може бути розшифрованим на стороні отримувача.

В описаному варіанті модифікації використано саме третій варіанту шифрування. Вивести закритий ключ з відкритого вкрай важко, якщо взагалі можливо. Для цього необхідно вирішити задачу розкладу дільників величезного цілого числа (необхідно розкласти на співмножники 129-значне число). До цих пір аналітичними методами вона не була вирішеною, тому вважається, що RSA можливо зламати лише шляхом грубого перебору. А до того часу поки Bruteforce attack буде реалізовано, актуальність переданої інформації скоріше за все буде втрачено.

Висновки

Стеганографічні та криптографічні методи виконують поставлені задачі. Але їх поєднання може значно посилити ефект захисту інформації. Для досягнення максимального результату необхідно прискіпливо віднестись до вибору методів, та слід пам'ятати про конкретну задачу, для якої створюється поєднання методів.

Отримана комбінація алгоритмів дозволяє мінімізувати виявлення прихованої текстової інформації в цифровому зображенні за допомогою методу Хі-квадрата і RS-атак. Вибір криптографічного алгоритму як і один з його режимів роботи був обраний з метою надання додаткового захисту вкрапленому повідомленню. Тобто передбачався сценарій, в якому зловмиснику вдалось виявити факт передачі вбудованого повідомлення і відомо криптографічний алгоритм та відкритий ключ. Але навіть із такою інформацією розроблений алгоритм є досить стійким і потребує значних затрат часу на злам, витрачаючи який буде збільшуватись ймовірність того, що зловмисник не отримає ніякої користі з добутої інформації, так як актуальність її із часом буде втрачено.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
2. Кузнецов О. О. Стеганография : навч. посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. — Х.: Вид. ХНЕУ, 2011. — 232 с.
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
4. Бабич І. В. Огляд стеганографічних методів перетворення інформації в зображеннях / І.В. Бабич, С.А. Паламарчук, Н.А. Паламарчук, В.В. Овсянніков // Захист інформації. — 2012. — № 1. — С. 18-24.
5. Корольов В.Ю., Поліновський В.В., Герасименко В.А. RS-стеганоаналіз. Принципи роботи, недоліки та концепція метода його обходу // Вісник Вінницького політехнічного інституту. — 2010. — № 6. — С. 66 – 71.
6. Навроцький Д. О. Дослідження результатів стеганорафічного приховування повідомлень у файлах зображення як засобу забезпечення захисту інформації / Д. О. Навроцький // Вісник Національного технічного університету України «КПІ». — 2012. — №50. — С. 121-128.
7. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / С.В.Мельник, С.В.Кондакова // Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.- практ. конф. – К.: Наук.-вид. відділ НА СБ України, 2010. – С. 134-138.
8. Певнев В.Я. RSA и простые числа // Системи обробки інформації, 2016, випуск 8 (145).- С.118-120.

Казаков Роман Геннадійович – студент групи 2КІ-18м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: justriko85@gmail.com.

Науковий керівник: **Очкуров Микола Андрійович** – старший викладач кафедри обчислювальної техніки, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Roman G. Kazakov – student of the 2KI-18m group, faculty of information technology and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: justriko85@gmail.com.

Supervisor: **Mykola A. Ochkurov** – art. lecturer in computer engineering, faculty of information technology and computer engineering, Vinnytsia National Technical University, Vinnytsia.