Секція 8. Захист інформації

КОМБІНУВАННЯ LSB-МЕТОДУ ТА КРИПТОГРАФІЧНОЇ СИСТЕМИ ХІЛЛА ДЛЯ ПРИХОВАНОГО ПЕРЕСИЛАННЯ ЗАШИФРОВАНИХ ПОВІДОМЛЕНЬ

Захарків Т. І.; Кухарська Н. П., к.ф.-м.н., доцент
Львівський державний університет безпеки життєдіяльності
м. Львів, Україна

Сьогодні інформацію, у зв'язку з бурхливим розвитком інформаційних технологій і їх широким застосуванням практично у всіх сферах людської діяльності, можна поставити в один ряд з загальноприйнятими матеріальними цінностями. Проблеми побудови систем захисту інформації широко обговорюються у сучасному відкритому друці [1 – 2]. Поряд з організаційними і апаратними засобами захисту інформації розглядаються дисципліни, предметом вивчення яких є розробка алгоритмів програмних методів захисту. До їх числа належать криптографія та стеганографія.

Криптографічні методи захисту, як відомо, базуються на використанні криптографічних перетворень інформації, які проводяться на основі застосування відповідних математичних законів, з метою виключення доступу до конфіденційної інформації сторонніх осіб, а також з метою забезпечення цілісності інформації [1, 3]. У сучасних умовах, як показує аналіз спеціалізованих літературних джерел та ресурсів мережі Internet, методи традиційної криптографії у ряді випадків не цілком задовольняють потреби користувачів через те, що їх застосування не дозволяє зберегти в таємниці сам факт передачі секретної інформації, її об'єм і джерело. Із створенням цифрового інформаційного середовища згадані вище проблеми стало можливим вирішувати методами комп'ютерної стеганографії [1, 4, 5], які дають змогу скрито вбудовувати додаткову інформацію (секретні відомості) в цифрові дані — різні файли, програми, пакети протоколів. На сьогодні перспективним напрямком (з точки зору забезпечення стійкості до виявлення прихованої інформації) вважається захист інформації, який передбачає симбіоз криптографічних та стеганографічних алгоритмів.

Метою цієї роботи є розробка в системі *MathCad* програмного комплексу приховання у *BMP*-файлах зашифрованих інформаційних повідомлень для подальшої їх передачі засобами телекомунікаційних мереж. Такий комплекс поєднує переваги і криптографічних, і стеганографічних методів захисту інформації.

Приховання текстового повідомлення реалізовано найбільш розповсюдженим стеганографічним методом — *LSB* (*Least Significant Bit*, заміни найменшого значущого біта) [4, 5]. Алгоритм цього методу базується на тому факті, що молодші розряди цифрових даних несуть дуже мало корис-

ної інформації, через що їх можна використовувати для вбудовування додаткових відомостей — інформаційних бітів конфіденційного текстового повідомлення. Така процедура інтегрування в файл растрового зображення секретних відомостей майже не впливає на його якість, що є наслідком психофізіологічних особливостей сприйняття цифрових зображень людиною. Популярність *LSB*–методу обумовлена доступністю його реалізації і можливістю приховувати у відносно невеликих файлах інформацію досить великого об'єму (пропускна здатність створюваного приховуваного каналу зв'язку становить від 12,5 до 30 %). Щоправда, якщо використовувати тільки *LSB*–метод, то передане повідомлення фактично буде незахищене від несанкціонованого прочитання у випадку, якщо зловмиснику відомо, що при пересиланні повідомлення застосовувався саме цей метод. Найпростішим способом підвищення стеганостійкості алгоритму є використання конгруентних співвідношень для визначення псевдовипадкової позиції запису біту текстового повідомлення в зображенні-носієві. Однак цієї дії виявляється недостатньо. Ефективнішою є процедура попереднього шифрування вихідного повідомлення: у випадку несанкціонованого видобування його із контейнера перед зловмисником стоятиме ще одна задача — необхідність дешифрування. У даній роботі пропонується зашифровувати текстове повідомлення, застосовуючи криптосистему Хілла [3]. Криптографічна система Хілла є блочним шифром, алгоритм якого базується на лінійній алгебрі та теорії матриць. Шифрування секретних відомостей, що підлягають прихованню та пересиланню каналами зв'язку, було здійснено на основі реалізації варіанту алгоритму з алфавітом 256 символів та матрицею-ключем розміру 5×5.

Результати тестування показали ефективність запропонованого способу підвищення надійності обміну прихованою інформацією. На основі використання двох рівнів обробки інформаційного повідомлення (криптографічного і стеганографічного) можна розробити нові більш стійкі методи розв'язання задач комп'ютерної стеганографії. Зауважимо, у загальному випадку така криптостеганографічна система володітиме стійкістю, яка еквівалентна стійкості використовуваних у ній алгоритмів шифрування.

Література

1. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. — К. : Юниор, 2003. — 464 с.

2. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / Малюк А. А. — М. : Горячая линия – Телеком, 2004. — 280 с.

3. Мухачев В. А. Методы практической криптографии / В. А. Мухачев, В. А. Хорошко — К. : ООО «Полиграф-Консалтинг», 2005. — 215 с.

4. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин., И. Н. Оков, И. В. Туринцев — М. : СОЛОН–Пресс, 2002. — 261 с.

5. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК–Пресс, 2006. — 249 с.