Самчишин О. В., канд.тенх.наук,
професор кафедри захисту інформації та кібербезпеки,
Сметанін К. В., канд.техн.наук,
викладач кафедри захисту інформації та кібербезпеки,
Овчар Я., курсант 291 навчальної групи
Житомирський військовий інститут імені С.П. Корольова

СПОСІБ ШИФРУВАННЯ ДАНИХ НА ОСНОВІ ПІКСЕЛЬНОГО АЛФАВІТУ

Під комп'ютерною стеганографією розуміється приховування одних цифрових повідомлень в інших. Комп'ютерна стеганографія широко використовується при обміні секретними повідомленнями, написанні вірусних програм, у захисті авторських прав, для приховування даних від копіювання і т.д. Великою перевагою окремих стеганографічних програм є те, що за ними можна наперед визначити зміни, які мають відбутися у зовнішньому вигляді вихідного файлу (наприклад, сполучення кольорів у фотографії) при введенні шифрованих даних. І якщо зміни будуть дуже великими, з'явиться попередження про це, також буде запропоновано вибрати файл-контейнер більшого розміру.

Файл, який необхідно приховати, називають інформаційним, а файл, що використовується для приховування даних, називають файлом-контейнером. Контейнером може бути текстовий, графічний чи музичний файл, але найрозповсюдженішими носіями стали саме зображення.

Найбільш розповсюдженим, але найменш стійким є метод заміни найменших значущих біт або LSB-метод (LSB – Least Significant Bit). Він полягає у використанні похибки дискретизації, що завжди існує в оцифрованих зображеннях або аудіо- і відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація молодших біт у більшості випадків не викликає значної трансформації зображення і не виявляється візуально.

Іншим популярним методом вмонтовування повідомлень є використання особливостей форматів даних, де застосовується стискування із втратою даних (наприклад JPEG). Цей метод (на відміну від LSB) більш стійкий до геометричних перетворень і виявлення факту передавання, тому що є можливість у широкому діапазоні змінювати якість стиснутого зображення, що унеможливлює визначення походження спотворення. Так, наприклад, в графічних кольорових RGB-файлах (RGB – скорочено від англ. Red, Green, Blue - червоний, зелений, синій) кожна точка малюн-ка кодується трьома байтами, кожний з яких відповідає певній адитивній складовій кольору (червону, зелену і синю). Модифікація кожного з трьох молодших біт приводить до зміни менш 1% інтенсивності даної точки, що майже непомітно людському оку. Це дозволяє ховати в картинці обсягом 800 Кб біля 100 Кб даних.

З метою забезпечення високої стійкості зашифрованої інформації при передачі її каналами мережі ІТС та зниження рівня загрози несанкціонованого доступу до неї та/або атаки на шифр запропоновано змінити підхід щодо розв'язання задачі шифрування даних.

Поставлена задача вирішується так, що у способі шифрування/розшифрування даних на основі піксельного алфавіту монохромного зображення, присвоюють кожному елементу «нормативного алфавіту» статичний діапазон значень яскравості пікселів монохромного зображення. Далі формують «алфавіт шифрування» і здійснюють шифрування вихідного повідомлення та приховують отриманий шифротекст у цифрове зображення шляхом його деформації, зокрема розміщення пікселів з яскравіс-тю, що відповідають значенню «алфавіту шифрування» на позиції з виз-наченим ключем.

Особливість формування «алфавіту шифрування» полягає у поданні його в тріадній (трицифровій) формі, при цьому кожен його елемент відповідає величині яскравості пікселя монохромного зображення. Заміна символів вихідного повідомлення здійснюється на випадкове значення із заданого йому діапазону "алфавіту шифрування" (наприклад, літера «А» українського алфавіту може бути замінена числами: 000, 001 та 002), у результаті чого формується шифр.

Такий підхід дозволяє забезпечити: високу стійкість зашифрованої інформації за рахунок шифрування кожного символу повідомлення динамічним випадковим числом з діапазону значень яскравості відповідного символу; значне зниження рівня загрози несанкціонованого доступу до повідомлення та атаки на шифр за рахунок приховування шифротексту у позиції графічних даних із урахуванням ключа, який відомий тільки відправнику та адресату.

Спосіб шифрування даних на основі піксельного алфавіту монохромного зображення доцільно застосовувати для ефективного функціонування мереж інформаційно-телекомунікаційних систем при передачі інформації каналами зв'язку в умовах наявності загрози здійснення не-санкціонованого доступу до неї та/або атаки на шифр. При цьому розроблений спосіб дозволяє забезпечити достатньо високий рівень стійкості зашифрованої інформації.