УДК 004.415.24:004.056.5

ПОБУДОВА АУДІОСТЕГОСИСТЕМИ З ПСЕВДОВИПАДКОВИМ РОЗПОДІЛОМ ПОВІДОМЛЕННЯ ПО КОНТЕЙНЕРУ

Павлюк Т.Р.

Кухарська Н. П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук, доцент

Комп'ютерна стеганографія за останні роки остаточно перетворилася з технічного мистецтва в напрямок наукових досліджень у сфері захисту інформації, набувши статусу самостійної прикладної науки, що вивчає способи і методи приховування секретних повідомлень у файлах різних форматів, мережевих пакетах, і т. п., а також методи виявлення стеганографічних систем. Зокрема, останнім часом значного розвитку набули методи стеганографічного приховування інформації у звукових файлах.

Слухова система людини (ССЛ) здатна до сприйняття надзвичайно широкого динамічного діапазону. Мінімальна величина тиску, спричиненого звуком, який ледве сприймається на слух людиною, становить 20мкПа, тобто 0,00002 Па. Максимальний рівень звукового тиску, при якому настає відчуття болю у вухах, дорівнює 20 Па. Таким чином, відношення між найбільш тихим і найбільш гучним звуками, котрі може сприйняти ССЛ, - один до мільярд. Людина здатна чути звуки з частотою коливань від 16 до 20 000 за секунду. Динамічний діапазон при цьому, як бачимо, становить п’ять порядків величини. Найкраще вухо людини сприймає звукові коливання з частотою від 2000 до 4000 Гц. Крім того, ССЛ характеризується високою чутливістю до адитивного флуктуаційного (білого) шуму. Людина може вловити відхилення у звуковому файлі аж до однієї десятимільйонної (70 дБ нижче рівня зовнішніх шумів).

У той же час, коли слух людини здатен до сприйняття звуку широкого динамічного діапазону, він характеризується досить малим різницевим діапазоном. Як наслідок, при одночасному прослуховуванні гучного і тихого звуку виникає феномен маскування, коли гучніший звук заглушує більш тихий. Крім того, слухова система людини не здатна розрізняти абсолютну фазу, розпізнаючи лише відносну. Саме ці особливості слухового апарату людини дають змогу стенографам успішно застосовувати аудіосередовище з метою приховування в ньому конфіденційної інформації.

Цифровий запис аудіосигналів базується на виконанні двох операцій над аналоговими сигналами. Це операції дискретизації і квантування. У реальних пристроях ці операції здійснюються одночасно. У результаті дискретизації аналоговий аудіосигнал замінюється

послідовністю відліків, а в результаті квантування кожен відлік представляється послідовністю біт. Таким чином, вихідний аналоговий сигнал замінюється масивом цілих чисел, кожне з яких обмежене числом розрядів, що дорівнює кількості біт квантування. Чим більша розрядність двійкового числа, використовуваного для представлення відліку, тим точніше відображається значення амплітуди.

Метою наших досліджень є побудувати аудіостегосистему з псевдовипадковим розподілом повідомлення по звуковому контейнеру формату WAVE.

Формат WAVE був обраний з тих міркувань, що він ідеально підходить для реалізації стеганографічних перетворень через свою надлишковість. В області даних аудіофайлів формату WAVE зберігаються нестиснуті і жодним чином незмінені дані, отримані безпосередньо з аналогово-цифрового перетворювача. Через це, реалізовувати стеганографічні алгоритми на файлах такого типу у порівняні з іншими є дещо простіше і зрозуміліше.

Найбільш доступний спосіб, за допомогою якого можна вбудувати конфіденційні дані у звуковий файл, передбачає заміну молодших розрядів цифрових аудіосигналів на біти приховуваного повідомлення. Використання такого підходу дає змогу приховати досить великий обсяг інформації в одному звуковому файлі. Наприклад, у файл довжиною 16 Мбайт таким чином можна вбудувати 1 Мбайт інформації (за умови, що розмір відліків 16 біт і замінюватися буде тільки один останній біт кожного відліку). При цьому спотворення звукового файлу будуть незначними. Зміна останнього біта у відліку призведе до незначної зміни амплітуди сигналу, що неможливо визначити на слух.

У найпростішому випадку проводиться заміна молодших розрядів послідовно розташованих відліків звукового файлу. У розробленому нами програмному комплексі використано підхід, який полягає у псевдовипадковому розподілі секретного повідомлення по аудіоконтейнеру. Відстань між двома вбудованими бітами є функцією, яка обчислюється як кількість одиниць у двійковому значенні номера попередньо модифікованого відліку помножена на деякий коефіцієнт. Цей коефіцієнт відіграє роль ключа, що може приймати будь-які цілі значення. Він має бути відомим як відправнику, що пересилає аудіоконтейнер з вбудованим секретним повідомленням мережею Internet, так і його отримувачу.

ЛІТЕРАТУРА

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : Изд-во "МК-Пресс", 2006. – 288 с.