ТЕХНОЛОГІЯ ТА ПРОГРАМНІ ЗАСОБИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Поповський В.В., Чорний С.В.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Леніна, 14 каф. телекомунікаційних систем, тел. (057) 702-13-20,
E-mail: tkc@kture.kharkov.ua ; svch1mail@gala.net ; факс (057) 702-13-20

Technology and software for data hiding has been proposed. It based on hiding the confidential message in files of different formats, like .exe, .mpg, .wav, .doc, etc. This steganographic technology has 6 levels of data protection: one steganographic and five cryptographic. As cryptographic methods has been used method close to "one-time notebook" and data mixing. Technology allows using as a keys songs and video, as well as generated stochastic sequences.

Вступ

Інформатизація сучасного суспільства та збільшення потоків інформації у телекомунікаційних системах ведуть до збільшення інформаційного впливу на суспільні процеси. При цьому значно зростає важливість збереження конфіденційності інформації [1-3], як фактору, що забезпечує захист певних соціальних процесів від стороннього впливу, зокрема з боку терористичних, кримінальних проявів, тощо.

Основна частина

Авторами пропонується технологія та програмні засоби для прихованого (стеганографічного) обміну інформацією, що не є власністю держави, по відкритих каналах зв'язку або її прихованого збереження у відкритих (загального користування) базах даних (носіях).

Технологія заснована на приховуванні конфіденційного повідомлення у комп'ютерних файлах-контейнерах та передачі їх по відкритих каналах цифрових телекомунікаційних систем або збереженні на відкритих носіях.

Перевагою технології перед відомими є те, що у якості файлів-контейнерів, файлів конфіденційних повідомлень та ключів можуть використовуватись файли довільних форматів (зокрема, .mpg, .wav, .jpg, .exe, тощо). Технологія забезпечує 6 рівнів захисту інформації від несанкціонованого викриття.

Перший рівень захисту забезпечується стеганографічним приховуванням інформації у файлі-контейнері.

Конфіденційне повідомлення перед включенням у файл-контейнер додатково криптографічно захищається. Авторами використано метод криптографічного перетворення близький до методу «одноразового блокноту», як потенційно найбільш стійкого. Можливо також використання і інших методів на вибір користувача. Процедури криптографічного перетворення та упаковки-дешифрування захищаються окремими ключами і складають відповідно 2-й та 3-й рівні захисту.

На четвертому рівні захисту для підвищення криптостійкості конфіденційне повідомлення перемішується.

На пятому рівні для запобігання використання запропонованого программного забезпечення для викриття прихованих повідомлень третіх осіб методом «брутальної сили» проводиться аутентифікація повідомлення до конкретного користувача.. Ефективність цього рівня захисту залежить від того скільки копій программного забезпечення зробить та розповсюдить його користувач. Захист від несанкціонованого копіювання ключів та программного забезпечення, що розглядається забезпечується шляхом його постійного зберігання на переносному індивідуальному носієві (флеш, CD).

Шостий рівень захисту забезпечується періодичною зміною користувачем ключів.

Технологія дозволяє використовувати у якості ключів файлі довільних форматів, або спеціально генеровані випадкові послідовності. Наприклад, текстове конфіденційне повідомлення може бути криптографічно захищене відомим звуковим файлом (піснею) або відео відповідної довжини. Це дозвляє відкрито зберігати та передавати ключову

інформацію без втрати її конфіденційності, приховуючи лише факт використання відомих звукових та відео записів у якості ключів.

Після виконання всіх процедур конфіденційне повідомлення ззовні виглядає, як неконфіденційний файл-контейнер обраного формату. Наявність прихованого змісту відомими програмами, що призначені для обробки файлів використаних форматів, та антивірусними програмами не виявляється. Повідомлення може бути вилучено лише за допомогою аутентифікованої версії пропонованого програмного забезпечення при точному знанні використаних для упаковки ключів.

Програмне забезпечення включає процедури кодування-упаковки повідомлень, дешифрування повідомлень, генерування користувачем випадкових ключів, перевірку статистичних властивостей ключів (рівномірності та незалежності).

Технологія та програмні засоби, що пропонуються, дозволяють

організовувати прихований обмін конфіденційною інформацією між абонентами по загальнодоступних каналах цифрових телекомунікаційних систем;

організувати приховане зберігання конфіденційної інформації користувачів на відкритих носіях або у базах даних;

приховано передавати ключову інформацію разом із конфіденційним змістом.

Програмне забезпечення готове до використання як окремий програмний продукт у операційній системі MS Windows і не потребує інсталяції на конкретному компьютері.

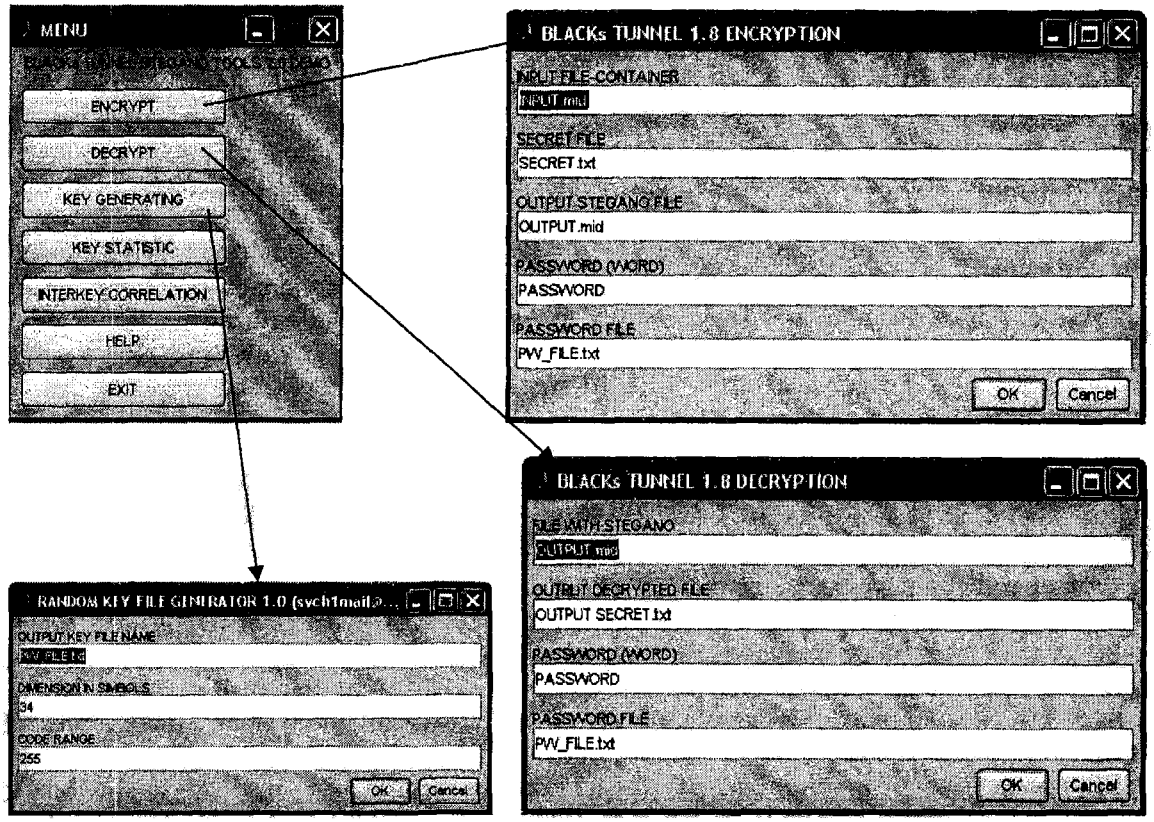

Рис.1. Взаємозв'язок основних робочих меню

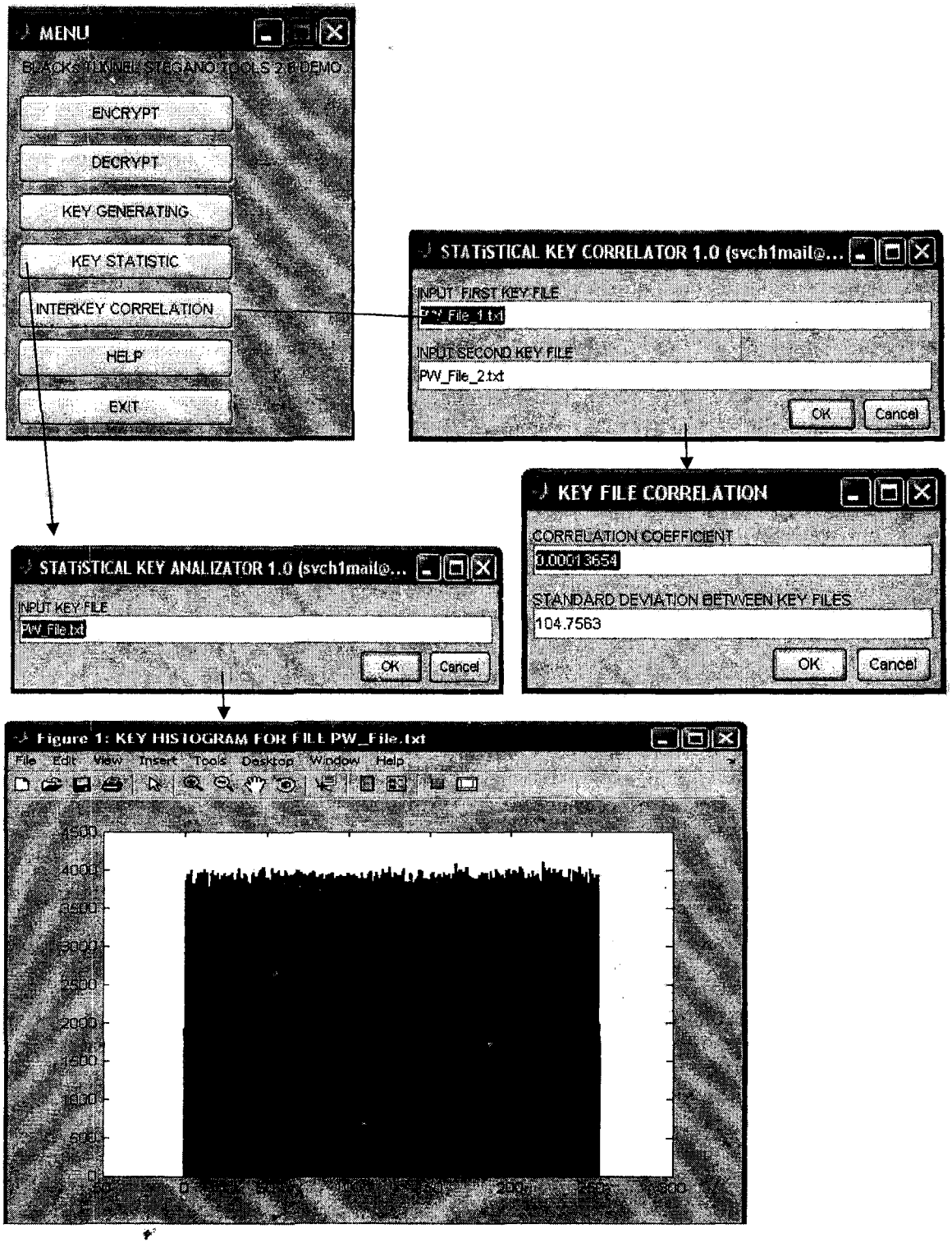

Рис.2. Взаємозв'язок головного меню з допоміжними та з результатами аналізу ключів.

Діалогова оболонка системи має три основних меню, які забезпечують кодування, декодування та генерацію ключів, та два допоміжних меню для статистичного та кореляційного аналізу ключів.

Взаємозвязок основних та допоміжних меню з головним меню програми показано на рис.1 та рис.2.

Программа має пять робочих меню. Три з них (ENCRYPT, DECRYPT, KEY GENERATING) дозволяють здійснювати основні операції, до яких належать кодування, декодування інформації та, у загальному випадку, генерування ключів. Решта меню (KEY STATISTIC, INTERKEY CORRELATION) дозволяють отримати гістограму розподілу кодів у ключі та коефіцієнт взаємо, або автокореляції ключів.

Технологія прихованої передачі інформації, що пропонується, орієнтована на використання ключів, розмір яких дорівнює розміру повідомлення, що приховується та використання нового ключа для кожної передачі інформації (метод одноразового блокноту). Проте, у разі потреби, користувачем можуть бути використані і короткі ключі.

Суттєвою перевагою запропонованої технології є можливість використання наряду з спеціально генерованими ключами, ключів, що зберігаються у базах даних загального користування (Інтернеті), наприклад у каталогах звукових та відео файлів. Однією з особливостей є можливість передавати ключову інформацію, по домовленості між абонентами, разом із конфіденційним повідомленням. При цьому ключем може бути файл, що використовується як контейнер для стеганографічного приховування інформації.

Конфіденційність передачі інформації у такому разі забезпечується якщо аутентифікована версія програми є лише у абонентів та про факт такої домовленості щодо ключів стороннім особам невідомо.

Висновок

Використання запропонованої технології та програмних засобів для передачі або зберігання конфіденційної інформації, що не є власністю держави, надає широкі можливості звичайним користувачам гарантованого збереження конфіденційності даних. Використання методів стеганографії суттєво розширює можливості використання каналів зв'язку загального користування для обміну конфіденційною інформацією.

Література:

1. Поповський В.В. та ін. Організація конфіденційного діловодства. ДУІКТ, Київ-2007,376с.
2. Поповский В.В., Персиков А.В. Защита информации в телекоммуникационных системах. Т1,СМИТ, Харьков-2006, 237с.
3. Поповский В.В., Персиков А.В. Защита информации в телекоммуникационных системах. Т2,СМИТ, Харьков-2006, 291с.
4. Черный С.В., Хижняк И.А. Метод цифровой стеганографии на основе сложения изображений. Материалы второй международной конференции «Современные информационные системы. Проблемы и тенденции развития».Харьков-Туапсе-2007,с101-102.