зв'язку. або зберігаються як такі

Але, більшість стеганографічних алгоритмів дозволяють приховувати невеликі об’єми інформації. Але на практиці часто виникає потреба в прихованій передачі значних масивів даних. Тому дослідження в напрямку розробки методу, що приховує великі об'єми інформації в відомих графічних форматах, для їх подальшої передачі є актуальним.

Метою дослідження є розробка стеганографічних методів і алгоритмів, які вбудовують і приховують великі об'єми інформації в графічні зображення формату JPEG з подальшою передачею цієї інформації х.

Список використаних джерел:

1. Аграновский А.В. Стеганографія, цифрові водяні знаки і стеганоаналіз / Аграновский А.В., Балакін А.В., Грибунин В.Г., Сапожников С. - М.: Книга ВНЗ, 2009. - 220 с.

к.т.н., доц. Чешун В.М. (ХмНУ)
к.т.н., доц. Орленко В.С. (ХмНУ
к.т.н., доц. Шваб В.К. (ВІКНУ)
Гончар Р.М. (ХмНУ)
Халіманенко С.М. (ВІКНУ)

Оптимальне нерівномірне кодування в підвищенні криптостійкості шифрів

В умовах стрімкого розвитку інформаційних технологій, постійного збільшення обсягів інформації в кіберпросторі і зростання її цінності, а також через появу нових загроз щодо її цілісності і конфіденційності надзвичайної актуальності набувають заходи кібербезпеки. Одним із базових заходів є криптографічний захист даних, про що свідчить поява і масштабне використання великої кількості методів та алгоритмів симетричного й асиметричного шифрування з різними функціональними можливостями і принципами дії (алгоритми DES-базовий, подвійний і потрійний DES, IDEA, ГОСТ 28147, Діффі-Хелмана, RSA тощо) та спроби їх постійного вдосконалення.

Підвищення криптостійкості алгоритмів шифрування можна досягти попередньою підготовкою вхідних даних, в ході якого забезпечується порушення статистичних даних повторюваності символів вхідного тексту, тобто, збільшення характеристик його ентропії. Одним із варіантів такої підготовки вхідного тексту може бути застування методів оптимального нерівномірного кодування - ОНК (кодування Шеннона-Фано, Хафмана).

В узагальненому алгоритмі підготовки даних до криптографічного шифрування із застосуванням ОНК можна виділити три базових операції:

1. Заміна кодових комбінацій K_i символів вхідного тексту, що мають однакову розрядність, кодовими комбінаціями K_i' різної розрядності із урахуванням статистичних характеристик появи зазначених символів в тексті.

2. Формування двійкового представлення вихідного тексту у вигляді послідовності кодових комбінацій заміни K_i' різної розрядності.

3. Розподіл одержаної послідовності на кодові комбінації K_j'' однакової

розрядності згідно з вимогами застосовуваного криптографічного алгоритму.

Особливістю реалізації етапу 3 є розподіл видозміненої стиснутої двійкової послідовності на кодові комбінації фіксованої розрядності K_j'' без урахування характеру входження в неї початкових символів повідомлення K_i, що зумовлює можливість виникнення нетипових ситуацій.

Оскільки характер розподілу нерівномірних кодових комбінацій K_i' між рівномірними кодовими комбінаціями K_j'' без урахування особливостей реалізації алгоритму ОНК апріорно є непередбачуваним зловмиснику, такий підхід, окрім зменшення розмірів призначеного для передачі двійкового коду вихідного тексту, збільшує ентропійні властивості зашифрованого тексту і його стійкість до зламу незалежно від застосовуваного методу криптографічного шифрування.

к.т.н., доц. Чорненький В.І. (ХмНУ)
к.т.н., доц. Чешун В.М. (ХмНУ)
д.т.н., проф. Яцків В.В. (ЗНУ
Солодєєва Л.В. (ВІКНУ)

Смарт-генерація псевдовипадкових чисел для формування криптоключів системи клієнт-банк

Генератори псевдовипадкових чисел (ГПВЧ) або послідовностей сьогодні є одним із основних елементів систем захисту інформаційних ресурсів від зловмисних посягань. Перевагою генерованих ГПВЧ паролів доступу порівняно з створюваними людиною є значно більший показник ентропії, оскільки символи таких паролів є незалежними і позбавлені апріорної вади зручності запам’ятовування для користувача, якою першочергово користуються хакери систем авторизації.

Завдяки здатності генерувати двійкові коди з високою ентропією ГПВЧ широко застосовуються в системах криптографічного захисту починаючи від формування ключів шифрування таблиць Віженера, реалізації алгоритмів симетричного і асиметричного шифрування, і до формування векторів ініціалізації режимів застосування алгоритмів шифрування, хешування з паролями, створення систем цифрового підпису в системах клієнт-банк тощо. Недостатня ентропія джерела псевдовипадкових чисел системи клієнт-банк може стати причиною її краху.

Оскільки алгоритмічно-генеровані псевдовипадкові послідовності характеризуються циклічною повторюваністю, для підвищення їх «непередбачуваності» застосовується додаткове джерело ентропії, призначення якого може полягати у визначенні стартового значення генерованої послідовності або у підвищенні показників ентропії генерованих значень іншим чином.

Перенесення банківських послуг в сферу мобільних технологій зумовлює зацікавленість в створенні повноцінних, зручних і надійних систем клієнт-банк на базі пристроїв мобільного зв’язку. Відповідно, однією із функцій подібних пристроїв мають стати функції ГПВЧ.