УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 2, pp. 164-173

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ ОРГАНІЗАЦІЇ ПРИХОВАНОГО КАНАЛУ ЗВ'ЯЗКУ В КАНАЛІ ЗАГАЛЬНОГО КОРИСТУВАННЯ

К.Р. Шерфедінов

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: k.sherfedinov@gmail.com

На основі стеганометоду Коха та Жао було побудовано стеганосистему для створення прихованого каналу зв'язку в мобільному каналі загального користування. Результатом роботи є android-додаток, який являє собою месенджер. В якості контейнера використовується цифрове зображення. Конфіденційною інформацією є текстові повідомлення користувачів. За допомогою android-додатку створюється прихований канал мобільного зв'язку в каналі загального користування. Клієнти обмінюються стеганоповідомленнями, які зберігаються на сервері. При цьому, власник серверу може мати повний доступ до файлів користувачів. Кожна клієнтська програма може вбудовувати конфіденційну інформацію у цифрове зображення та декодувати символьну послідовність із стеганоповідомлень. Ключем стеганосистеми є послідовність вбудови чергового біту додаткової інформації у контейнер. Кінцевий текст повідомлень буде правильно відображатися лише автентифікованим користувачам. Розроблений додаток підтримує обмін повідомленнями, які містять символи англійського алфавіту, числа та деякі розділові знаки. Максимальна довжина одного текстового повідомлення обмежена та складає 350 символів. Це обмеження було включено у додаток для того, щоб розроблену стеганосистему можна було використовувати на мобільних пристроях з невеликим обсягом оперативної пам'яті. Обчислювальна складність запропонованого алгоритму вбудови, декодування прихованої інформації становить $\underline{O}\left(n^2\right)$ операцій для $n \times n$-зображення, що робить його придатним для застосування в мобільних пристроях. Декодування прихованої інформації не потребує наявності незаповненого контейнеру. Запропонована система на сьогоднішній день не має аналогів. У майбутньому таку програму можна поєднати з клієнтами MySpace, Facebook, Twitter тощо.

Ключові слова: стеганографічний метод, цифрове зображення, канал зв'язку, дискретне косинусне перетворення, метод Коха та Жао, мобільна стеганосистема, android-додаток, безпека, чат

Вступ

В умовах активного розвитку мережевих технологій отримання доступу до інформації стало надзвичайно простим, все більша кількість інформації передається по мережі, та зростає кількість атак зловмисників з метою несанкціонованого доступу до неї. У зв'язку з цим виникає питання захищеної передачі даних в мережі.

З розвитком операційних систем iOS та Android мобільні додатки стали найпопулярнішим інструментом для обміну повідомленнями в Internet. Сучасна людина має в середньому 3-4 месенджера в своєму телефоні. Зазвичай це клієнтські програми таких соціальних мереж, як Facebook, Instagram, Telegram. Всі вони використовують шифрування та є добре захищеними від перехоплення повідомлень і атак ззовні. Але ці програми використовують сервери для зберігання даних користувачів, і тому якщо хтось отримає доступ до сервера, то він зможе отримати доступ і до повідомлень. Криптографічний захист інформації, де захищається лише сам зміст повідомлення, не усуває означену проблему повністю. Наявність шифрованого повідомлення сама по собі привертає увагу до нього, викликає підозру. До того ж в ряді країн, зокрема в

Україні, діють заборони чи обмеження на використання криптографічних засобів. З врахуванням цього, для захисту інформації, що передається за допомогою мобільного каналу зв'язку, від неавторізованого доступу *актуальним* є створення прихованого (стеганографічного) каналу всередині каналу загального користування, але на сьогодні не існує месенджерів, які використовують стеганографію для обміну конфедеційною інформацією.

На відміну від криптографії, яка приховує зміст таємного повідомлення, стеганографія приховує сам факт його існування [1,2]. У процесі стеганографування конфіденційна інформація (КІ) після попереднього кодування, результатом якого є додаткова інформація (ДІ), що, як правило, представляє бінарну послідовність, вбудовується в контейнер, чи основне повідомлення, яке не привертає уваги, результатом чого є стеганоповідомлення, яке відкрито пересилається по каналу зв'язку. Найбільш підходящими об'єктами-контейнерами, враховуючи специфіку сучасної стеганографії, що має «комп'ютерний» характер [1-3], є цифрові зображення (які використовуються далі в роботі), файли аудіо й відеоданих.

Стеганографічні методи для захисту інформації зазвичай використовують разом з методами криптографії, таким чином доповнюючи її. Сьогодні стеганографія переживає етап свого бурхливого розвитку, пов'язаний з багатьма об'єктивними і суб'єктивними причинами. Цей розвиток є важливим для вдосконалення системи захисту інформації, яка сьогодні носить комплексний характер [4], в цілому.

З урахуванням особливостей сучасної комунікації, невід'ємною частиною якої є передача інформації у форматах з втратами, одною з найважливіших вимог до стеганоалгоритмів, які використовуються при організації будь-якого прихованого каналу зв'язку, є вимога стійкості до атак проти вбудованого повідомлення – збурних дій, найпоширенішими з яких є стиск з втратами (з різними коефіцієнтами якості), накладання на зображення різноманітних шумів, фільтрів, афінні перетворення.

Стеганосистема, що будується в мобільному каналі загального користування, має свої особливості:

– Вона повинна мати малу обчислювальну складніть (не тільки у випадку потокового, а й фіксованого контейнеру). Як правило, мобільні пристрої мають менший об'єм оперативної пам'яті, ніж персональні комп'ютери, і тому працюють значно повільніше, виконуючи меншу кількість операцій в одиницю часу. Стеганоалгоритми, розроблені для комп'ютерів, можуть бути непридатними для застосування на смартфонах внаслідок великої обчислювальної складності, що, в свою чергу, трансформуєтья у значні вимоги до оперативної пам'яті.

– Операційна система Android оперує структурами даних для обробки зображень та їх збереження, схожими до своїх аналогів у MATLAB та Java (класична версія), але такими, що мають деякі відмінності [5]. Це обумовлено вбудованим у мобільні пристрої, працюючі на данній операційній системі, середовищем Android SDK. Якщо знехтувати цими умовами, то стеганоалгоритм може втратити свою ефективність або зовсім стати недієздатним.

– Стеганоалгоритм, який є основою відповідної стеганосистеми, обов'язково повинен бути стійким проти повторного стиску: переважна кількість серверів стискають зображення для більшої економії вільного місця на жорсткому диску; зазвичай стиск відбувається з коефіцієнтом якості QF 75-80.

При розробці стеганосистеми в мобільному каналі загального користування всі ці особливості повинні бути врахованими.

Метою роботи є забезпечення можливості прихованої передачі конфіденційної інформації загально використовуваним каналом мобільного зв'язку шляхом розробки відповідного android-додатку.

Створення прихованого каналу зв’язку відбувається за допомогою побудови стеганографічної системи, де в якості контейнерів використовуються цифрові зображення.

Для досягнення мети в роботі вирішуються такі *задачі*:

1. Обгрунтувати та здійснити вибір клієнтської програми з відкритим кодом для подальшої модифікації з врахуванням мети роботи.
2. Обгрунтувати та здійснити вибір стеганометоду, придатного для створення прихованого каналу зв’язку в мобільному каналі загального користування.
3. Для обраного стеганографічного методу вибрати значення параметрів, що визначають його алгоритмічну реалізацію, з урахуванням умов, в яких передбачається функціонування створюваного android-додатку.
4. Реалізувати обраний стеганографічний алгоритм в середовищі виконання для Android.
5. Інтегрувати розроблений алгоритм в клієнтську програму для обміну повідомленнями.

Основна частина

Математичні базиси при розробці сучасних стійких до збурних дій стеганоперетворень різні: лінійна алгебра, теорія ймовірності, математична статистика, теорія збурень [6]. Останнім часом почала розвиватися стеганографічна техніка, заснована на встановлених особливостях головного мозку людини, зокрема, нейромережевий підхід [7]. Для вбудовування ДІ в контейнер-зображення можуть використовуватися як просторова [1,2], так і область перетворення ЦЗ. В якості області перетворення може, зокрема, виступати частотна область ЦЗ, області різних розкладів матриці: сингулярного, спектрального [8-10].

Традиційно вважається, що для забезпечення стійкості стеганографічних методів і алгоритмів до збурних дій кращою для вбудови ДІ є область перетворення зображення, зокрема, частотна область. Це обумовлено тим, що в частотній області найпростіше задовольнити умовам забезпечення стійкості: достатньо виконувати вбудову додаткової інформації шляхом збурення низькочастотних коефіцієнтів цифрового зображення (блоків ЦЗ), виділення яких з усієї множини частотних коефіцієнтів є простою операцією. Враховуючи це, велика кількість розробок стійких стеганометодів і алгоритмів відповідає частотній області для проведення стеганоперетворення. Враховуючи те, що сучасні смартфони зберігають більшість файлів, зокрема зображення, у форматі з втратами, саме такі стеганографічні алгоритми доцільно використовувати при організації прихованого каналу мобільного зв’язку.

Розглянемо один з найпоширеніших на сьогодні методів приховування додаткової інформації в частотній області (області дискретного косінусного перетворення (ДКП)), який позиціонується як стійкий до стиску (з коефіцієнтами якості, що розглядаються в роботі), має низьку обчислювальну складність та просту реалізацію, - метод відносної заміни величин коефіцієнтів ДКП - Коха і Жао [3]. Для стеганоперетворення, з урахуванням необхідності збереження надійності сприйняття стеганоповідомлення, як правило, вибираються два ДКП-коефіцієнта K_1, K_2 середньої частини спектра блоку матриці ЦЗ-контейнера, отриманого після її попереднього стандартного розбиття [11]. Вбудовування ДІ відбувається за рахунок певної корекції їх значень з урахуванням значення сталої T, яка обирається за умов забезпечення найдійності сприйняття формованого стеганоповідомлення і стійкості відповідного стеганоалгоритму.

При організації прихованого каналу зв'язку часто використовується одна складова (з урахуванням особливостей людського зору - синя) кольорового ЦЗ. Тому,

не обмежуючи спільності міркувань, як формального представлення контейнера в роботі використовується одна $m \times n$ матриця F.

Як додаткова інформація розглядається випадково сформована бінарна послідовність $p_1,..., p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$.

Для емпіричного вибору коефіцієнтів K_1, K_2 ДКП блоку та сталої T, що фігурують у методі Коха і Жао, які доцільно задіювати в процесі стеганоперетворення (для забезпечення надійності сприйняття стеганоповідомлення та стійкості відповідного стеганоалгоритму до стиску), було проведено обчислювальний експеримент, в якому брали участь 100 ЦЗ розміром 3100*4200 пікселів. В ході експерименту сформована випадковим чином бітова послідовність, яка представляла з себе ДІ, вбудовувалась у ЦЗ-контейнер методом Коха і Жао з використанням різних K_1, K_2, T. Отримані стеганоповідомлення зберігалися в форматі Jpeg з коефіцієнтом якості QF=75, після чого вбудована послідовність вилучалась із цифрових зображень-стеганоповідомлень.

За результатами експерименту найпридатнішими для використання при вбудові ДІ були визнані коефіцієнти ДКП (4,5) та (5,4), оскільки саме вони забезпечували найбільшу кількість правильно відновленої інформації X (95.12%), яка обчислювалася за допомогою формули:

$$X = \frac{C_P}{C_O} \cdot 100\%, \qquad (1)$$

де C_P – кількість правильно декодованих бітів, C_O – кількість вбудованих бітів ДІ, X – кількість правильно відновленої ДІ.

Використання кожної з розглянутих пар коефіцієнтів ДКП ((4,5) та (5,4), (2,7) та (7,2), (1,7) та (2,8)) разом з емпірично встановленим значенням сталої $T = 25$ забезпечувало надійність сприйняття формованих стеганоповідомлень, яка встановлювалася за допомогою суб'єктивного ранжирування.

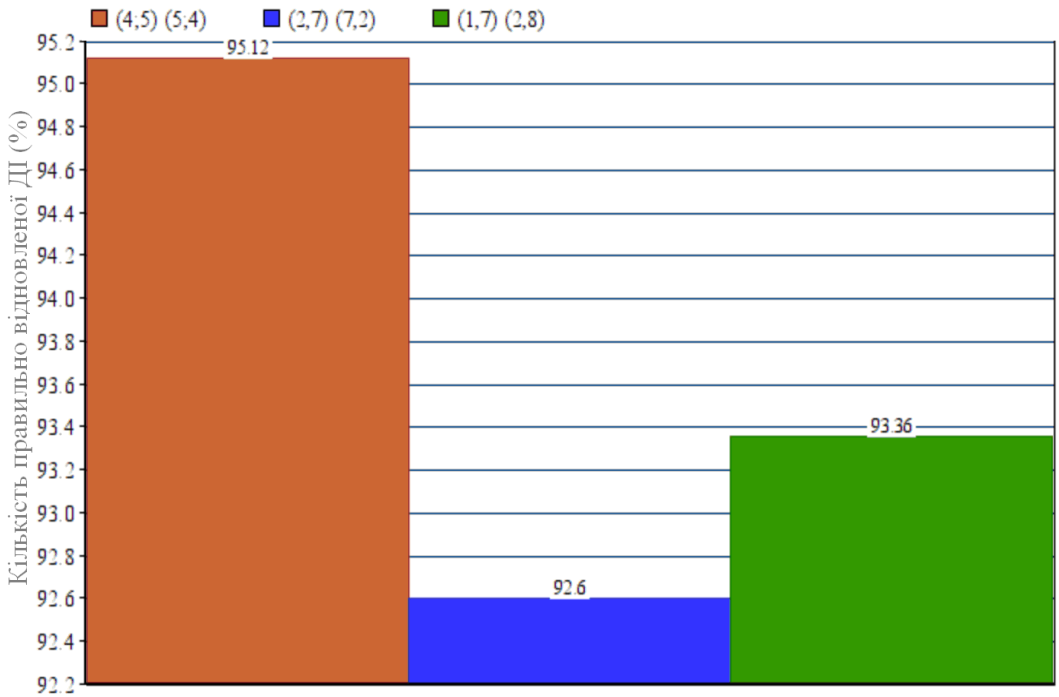

Рис. 1. Кількість правильно відновленої ДІ для різних пар коефіцієнтів ДКП блоків ЦЗ-контейнера, задіяних при стеганоперетворенні в методі Коха та Жао

Таким чином, в роботі використовується алгоритмічна реалізація методу Коха та Жао з наступними значеннями параметрів: $K_1 = (4,5)$, $K_2 = (5,4)$, $T = 25$ для процесу створення прихованого каналу мобільного зв'язку, основні кроки якого наступні.

Крок 1. Визначити кількість l символів повідомлення, що пересилається прихованим каналом мобільного зв'язку.

Крок 2. Матрицю F зображення-контейнера розбити стандартним чином на непересічні блоки розміром 8×8 пікселів. Визначити m - кількість отриманих блоків.

Крок 3. Визначити S - кількість блоків, що треба задіяти при стеганоперетворенні:

$$S = 3 + 3 \cdot 9 + 3 \cdot l \cdot 8.$$

Якщо $m < S$,

то попередження про неможливість відправлення повідомлення в запропонованому ЦЗ-контейнері. Перехід на крок 8.

Крок 4. Текстове повідомлення кодується в бінарну послідовність, результатом чого є ДІ: $p_1, ..., p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$. При перетворенні тексту (англійською мовою) до UTF-8 кожному символу ставиться у відповідність 8 бітів. Таким чином: $t = 8l$. Максимальна кількість символів у повідомленні, що приховано передається, незалежно від розміру ЦЗ-контейнера складає 350 символів. Ця величина є приємливою для більшості текстових повідомлень. Таке обмеження вводиться у зв'язку з тим, що оперативна пам'ять більшості смартфонів скаладає в середньому 1Гб.

Крок 5. В 3 блоки ЦЗ, місця розташування яких визначаються секретним ключом, за допомогою алгоритмічної реалізації методу Коха та Жао для визначення зображення як стеганоповідомлення вбудовуються значення: $k_1 = k_2 = k_3 = 1$

Крок 6. Кількість символів l повідомлення, що пересилається, переводиться в двійкову систему числення. Результат - l_B. Враховуючи те, що $l \le 350$, а двійкове представлення числа 350 має 9 розрядів, l_B представляється в дев'ятирозрядному вигляді: $l_B{}^{(1)} l_B{}^{(2)} ... l_B{}^{(9)}$.

Крок 7. У 27 блоків матриці зображення-контейнера, що використовуються в процесі стеганоперетворення, місця розташування та порядок яких визначається секретним ключом, за допомогою алгоритмічної реалізації методу Коха і Жао тричі вбудовується отримане двійкове представлення l_B (це необхідно для того, щоб при декодуванні була відома точна кількість блоків, які слід обробити для декодування інформації). В наступні блоки ЦЗ-контейнера, що задіюються в процесі стеганоперетворення (місця розташування та порядок яких визначається секретним ключом), вбудовуються послідовно біти $p_1, ..., p_{8l}$ ДІ за допомогою алгоритмічної реалізації методу Коха та Жао. Цей процес повторюється тричі. Результат – матриця ЦЗ-стеганоповідомлення F_S. Після стеганоперетворення ЦЗ зберігається в форматі Jpeg з коефіцієнтом якості QF, який дорівнює 75.

Крок 8. Закінчення обробки зображення.

Отримане стеганоповідомлення відправляється до серверу. Адресат, якому це повідомлення призначене, відкриває свій android-додаток та завантажує зображення з серверу до себе на смартфон. Після цього стартує процес декодування переданої інформації (рис.2).

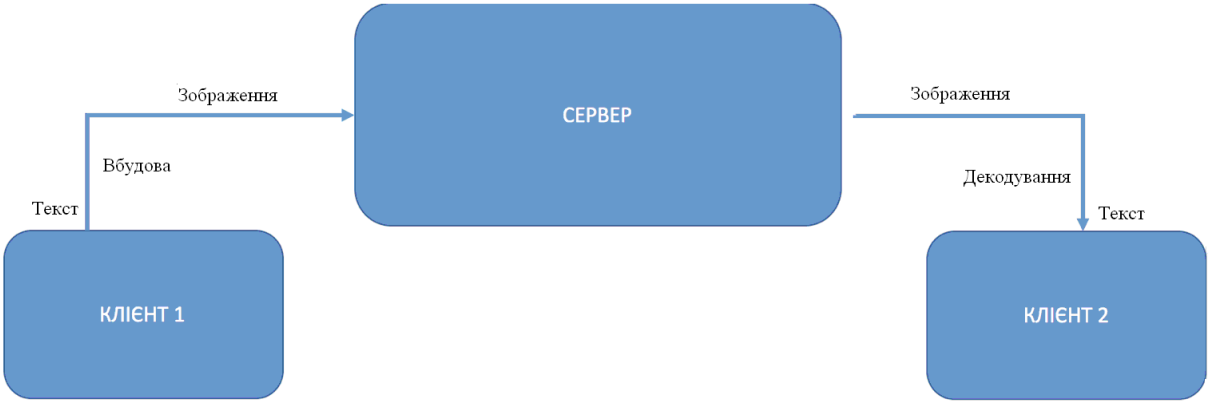

Рис.2. Схема роботи стеганомесенджера

Для кожного зображення алгоритм декодування ДІ має наступні кроки.

Крок 1. Отримане зображення з матрицею $\overline{F}_S$ розбивається стандартним чином на непересічні блоки розміром 8×8 пікселів.

Крок 2. За допомогою алгоритму Коха та Жао декодується інформація з 3 блоків ЦЗ, місця розташування яких визначаються секретним ключом (відповідно до кроку 5 при стеганоперетворенні ЦЗ): $\overline{k}_1, \overline{k}_2, \overline{k}_3$.

Якщо $\overline{k}_1 + \overline{k}_2 + \overline{k}_3 > 1,$

то перехід на крок 3,

інакше перехід на крок 6.

Крок 3. За допомогою алгоритму Коха та Жао декодуються наступні 27 бітів інформації з 27 чергових блоків ЦЗ-стеганоповідомлення (місця розташування та порядок яких визначається секретним ключом), задіяних в стеганоперетворенні, які розбиваються на 3 послідовні групи по 9 бітів: $\overline{a}_1, \overline{a}_2, ..., \overline{a}_9$, $\overline{b}_1, \overline{b}_2, ..., \overline{b}_9$, $\overline{c}_1, \overline{c}_2, ..., \overline{c}_9$.

Біти l_B відновлюються відповідно:

$$l_B^{(i)} = \begin{cases} 1, & якщо \quad \overline{a}_i + \overline{b}_i + \overline{c}_i > 1 \\ 0 & інакше \end{cases}, \quad i = \overline{1,9}.$$

Отримане значення l_B переводиться в десятичну систему числення. Результат - l (кількість символів повідомлення, що пересилається).

Крок 4. З блоків матриці $\overline{F}_S$, що були задіяні в процесі стеганоперетворення (місця розташування та порядок яких визначається секретним ключом), кількість яких становить $8 \cdot l \cdot 3$, за допомогою алгоритмічної реалізації методу Коха і Жао декодувати (можливо змінені) біти тричі вбудованої під час стеганоперетворення ДІ

$$p_1^{(1)}, ..., p_{8l}^{(1)}, p_1^{(2)}, ..., p_{8l}^{(2)}, p_1^{(3)}, ..., p_{8l}^{(3)}.$$

Остаточно біти $\overline{p}_1, ..., \overline{p}_{8l}$ ДІ відновлюються за формулою:

$$\overline{p}_i = \begin{cases} 1, & якщо \quad p_i^{(1)} + p_i^{(2)} + p_i^{(3)} > 1 \\ & \\ 0 & інакше \end{cases}, \quad i = \overline{1,8l}.$$

Крок 5. Отримана бітова послідовність ДІ $\overline{p}_1,...,\overline{p}_{8l}$ переводиться до ASCII вигляду. Результат записується у пам'ять смартфону.

Крок 6. Закінчення аналізу зображення.

Тестування розробленого стеганомесенджеру на 100 ЦЗ розміру 3100×4200 пікселів дали наступні результати. Порушення надійності сприйняття формованих стеганоповідомлень, яка встановлювалася за допомогою суб'єктивного ранжирування, зафіксовано не було. Як ілюстрація цього на рисунку 3 наведений типовий приклад застосування розробленого стеганододатку до одного з використаних в якості контейнера зображень.

а б

Рис. 3. Збереження надійності сприйняття стеганоповідомлення після вбудови в ЦЗ конфіденційної інформації розробленим android-додатком: а – ЦЗ-контейнер; б – стеганоповідомлення

Кількість правильно відновленої ДІ в середньому по експерименту становить 95.12%.

Кількість S правильно відновленої КІ (символів тексту) визначалася за формулою:

$$S = \frac{S_p \cdot 100}{S_o}, \qquad (2)$$

де S_p – кількість правильно декодованих символів, S_o – кількість вбудованих символів.

Треба зазначити, що величина (2) відрізняється (в бік зменшення) від (1). Це відбувається завдяки тому, що кожному символу ставилися у відповідність 8 бітів. Якщо серед цих бітів буде хоча б один, відновлений неправильно, то, теоретично, цей символ не буде знайдений у алфавіті та його буде замінено на спецсимвол "~" після декодування.

При проведенні обчислювального експерименту кількість правильно відновленої КІ склала в середньому 87.5%.

Як було зазначено, сьогодні не існує месенджерів, які використовують стеганографію для обміну конфедеційною інформацією. Тому розроблена

стеганосистема не має собі аналогів і поки що неможливо якісно оцінити її рівень ефективності порівняно з подібними стеганосистемами.

Обчислювальна складність запропонованого в роботі алгоритму визначається кількістю 8*8-блоків, на які розбивається матриця ЦЗ, а тому для зображення, матриця якого має розмір $n \times n$, становить $\left[\frac{n}{8}\right] \times \left[\frac{n}{8}\right] = \underline{O}\left(n^2\right)$ операцій, де $[\bullet]$ - ціла частина аргументу.

Висновки

В роботі вирішена важлива науково-практична задача забезпечення можливості прихованої передачі конфіденційної інформації загально використовуваним каналом мобільного зв'язку шляхом розробки android-додатку, результатом роботи якого є створювана стеганографічна система, побудована на основі алгоритмічної реалізації методу Коха і Жао, параметри якої обиралися емпірічно. В якості контейнера використовується цифрове зображення.

Обчислювальна складність запропонованого алгоритму вбудови, декодування прихованої інформації становить $\underline{O}\left(n^2\right)$ операцій для $n \times n$-зображення, що робить його придатним для застосування в мобільних пристроях. Декодування прихованої інформації не потребує наявності незаповненого контейнеру.

Тестування розробленого android-додатку показало його ефективність в умовах атаки проти вбудованого повідомлення (стиску стеганоповідомлення з втратами):

– суб'єктивним ранжируванням не було зафіксовано порушення надійності сприйняття стеганоповідомлень;

– при відновленні інформації, що пересилалася, кількість правильно відновленої бітової послідовності перевищив 95%, а правильно відновлених текстових символів повідомлення – 87.5%.

Запропонована система на сьогоднішній день не має аналогів. В майбутньому можуть бути розроблені аналогічні стеганомесенджері для соціальних мереж Facebook, WhatsApp тощо.

Список літератури

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
2. Аграновский, А.В. Стеганография, цифровые водяные знаки и стеганоанализ: [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
3. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
4. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008. —Т.2: Информационная безопасность. — 2008. — 344 с.
5. Android Programming: The Big Nerd Ranch Guide / Bill Phillips, Chris Stewart, and Kristin Marsicano // Indianapolis, IN 46240 USA.
6. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
7. Vafaei, M. A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability/ M. Vafaei, H. Mahdavi-Nasab // J. Basic. Appl. Sci. Res. — 2013. — 3 (4). — Pp. 577-587.
8. Bergman, C. Unitary Embedding for Data Hiding with the SVD / C. Bergman, J. Davidson // Proceedings of Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA, January 17, 2005. — Vol. 5681. — Pp. 619–630.

9. Fridrich, J. Steganography in Digital Media: Principles, Algoritms and Applications / J. Fridrich. — 2010. — 441 p.
10. Patra, J.C. Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication / J.C. Patra, A.K. Kishore, C. Bornand // In Proc. of 2011 IEEE International Conference on Systems, Man, and Cybernetics. — 2011. — Pp. 2940 – 2945.
11. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ОРГАНИЗАЦИИ СКРЫТОГО КАНАЛА СВЯЗИ В КАНАЛЕ ОБЩЕГО ПОЛЬЗОВАНИЯ

К.Р. Шерфединов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: k.sherfedinov@gmail.com

На основе стеганометода Коха и Жао была построена стеганосистема для создания скрытого канала связи в мобильном канале общего пользования. Результатом работы является android-приложение, которое представляет собой мессенджер. В качестве контейнера используется цифровое изображение. Конфиденциальной информацией являются текстовые сообщения. С помощью android-приложения создается скрытый канал мобильной связи в канале общего пользования. Клиенты обмениваются стеганосообщениями, которые хранятся на сервере. При этом владелец сервера может иметь полный доступ к файлам пользователей. Каждая клиентская программа может встраивать конфиденциальную информацию в цифровое изображение и декодировать символьную последовательность из стеганосообщений. Ключом стеганосистемы является последовательность встраивания очередного бита дополнительной информации в контейнер. Конечный текст сообщений будет правильно отображаться лишь для аутентифицированных пользователей. Разработанное приложение поддерживает обмен сообщениями, которые содержат символы английского алфавита, числа и некоторые знаки препинания. Максимальная длина текстового сообщения ограничена и составляет 350 символов. Это ограничение было встроено в приложение для того, чтобы разработанную стеганосистему можно было использовать на мобильном устройстве с небольшим объемом оперативной памяти. Вычислительная сложность предложенного алгоритма составляет $\underline{O}\left(n^2\right)$, что делает его пригодным для применения на мобильных устройствах. Декодирование скрытой информации не требует наличия незаполненного контейнера. Предложенная система на сегодняшний день не имеет аналогов. В будущего такую программу можно совместить с клиентами MySpace, Facebook, Twitter и т.п.

Ключевые слова: стеганографической метод, цифровое изображение, канал связи, дискретное косинусное преобразование, метод Коха и Жао, мобильная стеганосистема, android-приложение, безопасность, чат

MOBILE APPLICATION DEVELOPMENT FOR ORGANIZING A HIDDEN COMMUNICATION CHANNEL IN A PUBLIC CHANNEL

K.R. Sherfedinov

Odesa National Polytechnic University,
1, Shevchenko Str., Odesa, 65044, Ukraine; e-mail: k.sherfedinov@gmail.com

Based on the steganomethod Koch and Zhao, a steganosystem was constructed to create a hidden communication channel in a mobile public channel. The result of the work is the android-application, which is an instant messenger. The container is a digital image. Confidential information is text messages. With the help of the android application, a hidden mobile channel is created in the public channel. Clients exchange stegan messages, which are stored on the server. In this case, the server owner can have full access to user files. Each client program can embed confidential information into a digital image and decode the character sequence from steganesses. The key of the steganosystem is the sequence of embedding the next bit of additional information into the container. The final message text will be displayed correctly only for authenticated users. The developed application supports the exchange of messages, which contain the symbols of the English alphabet, numbers and some punctuation marks. The maximum length of a text message is limited to 350 characters. This restriction was built into the application so that the developed steganosystem could be used on a mobile device with a small amount of RAM. The computational complexity of the proposed algorithm is, which makes it suitable for use on mobile devices. Decoding of hidden information does not require the presence of an empty container. The proposed system to date has no analogues. In the future, such a program can be combined with clients MySpace, Facebook, Twitter, etc.

Keywords: steganographic method, digital image, communication channel, discrete cosine transformation, Koch and Zhao method, mobile steganosystem, android-application, security, chat