УДК 004.056.5

Борисенко І.І., Дідик Є.Ю.

Національний університет «Одеська політехніка»

СТЕГАНОГРАФІЧНА СИСТЕМА КОНТРОЛЮ РОЗМІЩЕННЯ ПОВІДОМЛЕННЯ В КОНТЕЙНЕРІ

Вступ. У сучасному світі теорія графів є однією з актуальних та ефективних, серед математичних технологій, бо сфера її застосування охоплює різні області діяльності людства, зокрема у інформаційній та кібернетичній безпеці. Аналіз наукової літератури [1] свідчить про наявність глибокої зацікавленості вчених до проблеми використання графових технологій у кібербезпеці. Сформувалися наступні напрями застосування теорії графів в інформаційній та кібернетичній безпеці: в інформаційній системі та у програмуванні; моделювання, аналіз та застосування графів атак; криптографічні перетворення за допомогою теорії графів; побудова дерева рішень у задачах прийняття рішень в умовах ризику і невизначеності. Теорія графів знайшла своє застосування і в стеганографії, оскільки завдяки графам можна представити структуру контейнера, повідомлення, яке вбудовується, та вирішити безліч задач.

Мета: Модифікація стеганографічного алгоритму засобами теорії графів.

Основна частина.

Розглянемо як можна застосувати розвинуту в стеганографії теорію графів до алгоритмів, які вже мають практичне застосування, тобто як і надалі можна розвивати практичну теорію графів.

В роботі [1] пропонується новий стеганографічний алгоритм просторової області вбудовування в цифрове зображення. Основним принципом розробки є мінімізація впливів вбудованого повідомлення на контейнер. В основу алгоритму покладено порівняння бітових послідовностей контейнера та повідомлення, модифікація елементів контейнера виконується тільки у випадку, коли виявлено неспівпадіння відповідних бітів. Алгоритм дозволяє зменшити викривлення контейнера, зберегти статистики першого порядку та забезпечити стійкість до найбільш відомих статистичних атак.

Повідомлення і пікселі контейнера розбиваються на підпослідовності. Початок підпослідовностей, в які вбудовується повідомлення фіксуються в ключі K. Але саме цю задачу можна вирішити за допомогою графа. Що ефективніше використовувати ключ чи граф, це окрема задача. Зараз розглянемо, саме яким чином можна фіксувати, за допомогою графа, підпослідовності контейнера, в які вбудована інформація, яку треба передати адресату. Окрім цього, пропонується дублювати інформацію, яку треба переслати. За рахунок клонування відліків інформації, що вбудовується, алгоритм підвищить свою стійкість не тільки до статистичних але і до інших видів атак таких як, наприклад, зашумлення стегоконтейнера, а в окремих випадках до геометричних атак, таких як поворот та обрізання.

Вузли графа – це початки підпослідовностей контейнера, в які вбудоване повідомлення, ребра – показують, з якої вершини графа потрібно переміститись в

іншу, а саме ту вершину, щоб одержати зв'язне повідомлення.

Оскільки є клони кожного відліку повідомлення, то граф буде представляти собою не ланцюг, а дерево (рисунок 1).

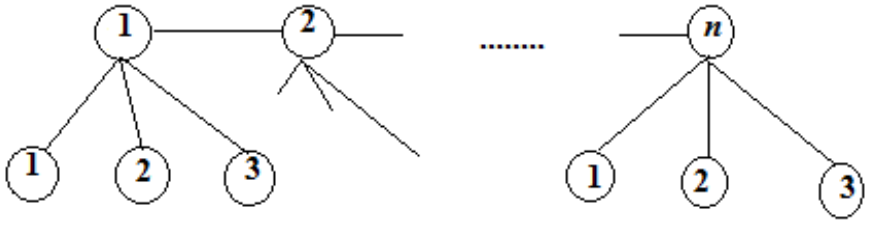

Рисунок 1. – Граф-дерево розміщення повідомлення

При декодуванні повідомлення, якщо ланцюг графа 1-2…n не дає зв'язного тексту (шум в каналі зв'язку або навмисно накладений шум як атака на стегоконтейнер, інші види атак), то є можливість використати листи графа 11, 12 або 13 і так далі n1, n2, n3. Дублювання окремих блоків інформації дещо перевантажує контейнер, але дає можливість протистояти атакам, які вносять невеликі збурення в контейнер,наприклад, накладання шуму, який непомітний або ледь помітний оку. Характеристики алгоритмів, що оперують із графами, зазвичай дуже чутливі до способу їх представлення.

Відомі схеми представлення графів [1]. Однією з найбільш простих схем зберігання графа є таблиця зв'язків - двовимірний масив, який має n рядків і m стовпців, де m - максимальна степінь вершин в G=(X,E). Список суміжності i-го вузла зберігається в i-ому рядку.

Дана схема зберігання надзвичайно проста при реалізації, доступ до списку суміжності чергового вузла - доступ до відповідного рядка матриці, модифікація графа приводить до зміни елементів відповідних рядків матриці без порушення загальної структури (якщо при модифікації не змінюється m). Однак ця схема може бути надзвичайно неефективна, якщо велика кількість вузлів графа має степінь, меншу (значно), ніж максимальна, оскільки її вимоги до пам'яті визначаються як mn «збережених» елементів.Найбільш зручною з погляду можливостей проведення модифікацій графа є схема, що використовує поле зв'язків.

Дана схема містить три одновимірні масиви A, A_s, A_{ind}, перші два з яких мають довжини 2|E|, останній - |X|. Значенням покажчика $A_{ind}(i)$ є початок списку суміжності i-го вузла в масиві A. Якщо A(k)- це черговий сусід i-го вузла, то $A_s(k)$ - покажчик розташування наступного його сусіда в масиві A^A. Від'ємне значення $A_s(k)$ говорить про закінчення списку суміжності вузла, що розглядається.

Загальна довжина масивів при такому способі представлення графа – 4|E|+|X|, що значно більше, ніж у першій схемі. Однак модифікація графа вимагає лише незначних змін у вже сформованій частині масивів.

Перелік використаних джерел

1. Борисенко І.І. Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень. Сучасна спеціальна техніка. Київ, 2014. №2. С. 110-115.

2. Нікольський Ю.В, Пасічник В.В, Щербина Ю.М. Дискретна математика. – К.: Видавнича група BHV, 2007. – 368 с.