УДК 004.056.5

С. О. Кормщикова

ПІДВИЩЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ СИСТЕМ БЕЗПЕКИ НА ОСНОВІ СТРУКТУРНОГО СТЕГАНОГРАФІЧНОГО КОДУВАННЯ

Вінницький національний технічний університет

Анотація

Запропоновано вдосконалення структурного стеганографічного кодування для підвіщення стійкості інформаційних ресурсів. Вдосконалення полягає у введенні в метод додаткових правил, що усувають проблеми вилучення даних і підвищують стійкість до атак.

Ключові слова: інформація, захист інформації, приховування даних, стеганографія.

Abstract

The report improved the structural steganographic coding for increasing the stability of information resources is proposed. The improvement is to introduce additional rules in the method that eliminate the problem of data extraction and increase the resistance to attacks.

Keywords: information, information security, data hiding, steganography.

Вступ

На сьогоднішній день суспільство характеризується суттєвим зростанням розуміння ролі та актуальності проблеми забезпечення безпеки в усіх сферах життєдіяльності. Особливо гостро дана проблема постає в забезпеченні саме інформаційної безпеки. Адже на сьогодні інформаціє є чи не найголовнішим стратегічним ресурсом як на державному рівні, так і на особистому. Основу будь-якої діяльності суспільства складає інформаційне забезпечення. Інформація є одним з основних засобів вирішення проблем та задач держави, політичних діячів, комерційних структур та окремих людей.

Захист інформації був актуальним завжди та залишається таким й сьогодні. Одним з найпопулярніших та найперспективніших напрямів інформаційної безпеки – є стеганографія. Адже на відміну від криптографіїї вона приховує сам факт наявності секретної інформації.

З розвитком обчислювальної техніки змінюються і засоби та методи захисту інформації, її викрадення. Поява комп'ютерної стеганографії сприяла поширенню її методів у різні сфери життя. Вона дозволяє не лише приховувати передачу даних, але й вирішувати проблеми автентифікації, захищати інформацію від несанкціонованих копіювання та модифікації.

Функціонування систем безпеки в сучасному світі визначає потребу забезпечення необхідного рівня безпеки інформаційних ресурсів. Це важливо, оскільки такі системи мають особливу значимість для інформаційної підтримки функціонування систем критичного призначення. Тому підвищення безпеки інформаційних ресурсів в інфокомунікаційних системах є актуальною науково-прикладною задачею.

Для вирішення сформульованої задачі необхідно розробити нові шляхи забезпечення безпеки інформаційних ресурсів. Одним з напрямків є використання стеганографічних методів вбудовування інформації в зображення-контейнер.

Серед методів стеганографічних перетворень найбільш опрацьованими і популярними на практиці є методи безпосереднього вбудовування інформації в зображення-контейнер. Вони характеризуються простотою реалізації вбудовування, великим значенням стеганографічної ємності та невеликими значеннями тимчасових витрат на реалізацію прямого і зворотного стеганографічних перетворень.

В процесі використання існуючих стеганографічних систем для прихованої передачі спеціальної інформації виникає протиріччя, яке полягає в тому, що існуючі технології стеганографічних перетворень не забезпечують повною мірою системних вимог в критичних умовах з активним протистоянням противнику.

Результати дослідження

Стеганографічним кодуванням називається процес при якому вбудовування інформації та побудова коду-контейнеру відбуваються одночасно. Значення коду-контейнера, яке містить приховану інформацію, є стеганокодом.

В структурному методі прихований текст формується шляхом здійснення послідовних модифікацій частин зображення.

В даних методах виділяють наступні етапи перетворень:

1. Перетворення приховуваного секретного повідомлення M у цифрову форму Dm, тобто текст шифрується з усіма відповідними атрибутами.
2. Перетворення послідовності чисел Dm в графічну структуру Gm, яку можно формально описати.
3. Перетворення графічної структури Gm у візуальне інформаційне середовище Vm.
4. Використання методів та процедур для створення сюжету візуальних образів з вбудованими прихованими повідомленнями.

На рисунку 1 зображена схема формування базису динамічних діапазонів для контейнера-зображення A.

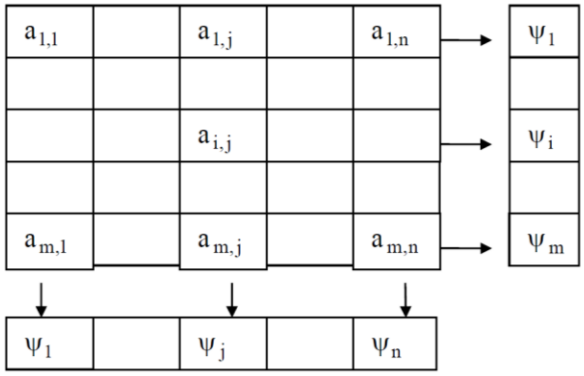

Рис. 1 – Схема формування базису динамічних діапазонів для зображення-контейнера A

Проектування стегосистеми здійснюється на основі кодоутворюючого функціоналу з врахуванням нерівноважного базису, адже саме він має властивість враховувати обмеження на динамічний діапазон в процесі представлення та кодування.

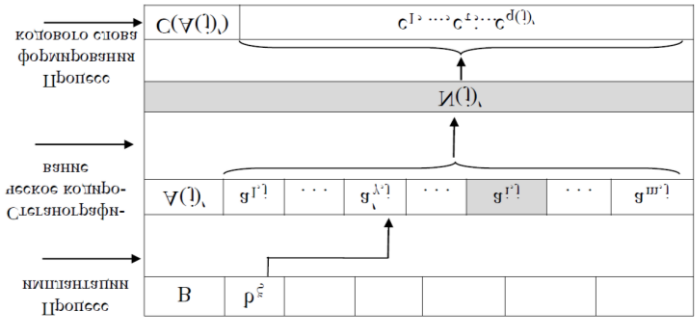

Рисунок 2 – Структурна схема побудови кодограми стеганокоду для числа $A(\mathrm{j})'$ з імплантацією

Перший крок являє собою обчислення стеганокоду $\mathrm{N(j)}'$, як суму величин $a_{i,j}V'_{i,j}$ та $\mathrm{a}'_{\gamma,j}V'_{\gamma,j}$. Кодограма $C(A(\mathrm{j}))'$ будується на другому кроці для значення $\mathrm{N(j)}'$:

$$C(A(\mathrm{j}))' = \{c_1, \dots c_\tau, \dots, c_{q(j)'}\},$$

де $q(j)'$ - довжина кодограми $C(A(\mathrm{j}))'$.

В результаті утворюються кодові комбінації, які складаються з двох частин: службової $\psi^{(1)}$ та інформаційної $\mathrm{N(j)}'$.

Структурний метод дозволяє не тільки модифікувати зображення, в якому буде приховано послання, але і створювати зображення по секретному повідомленням. Даний метод стійкий до атак.

Розроблений метод стеганографічного кодування дозволяє вбудовувати приховану інформацію в

цифрове зображення-контейнер на основі структурних особливостей контейнеру. Перед етапом стеганографічного кодування виконується вставка даних приховуваного повідомлення в старше нерівноважне позиційне число A (j) довжиною m. В процесі стеганографічного кодування для вбудованого числа A(j)′ формується стеганокод N′(j).

Основною характеристикою стеганографічного методу є об'єм інформації що можна вбудувати до контейнеру. Для оцінки буде використано відносна стеганографічна ємкість $w_{\text{відн}}^{(m)}$ системи.

Значення відносної стеганографічної ємності відображає відсоткове співвідношення об'єму інформації що вбудовується відносно розмірів контейнеру. Величина $w_{\text{відн}}^{(m)}$ відносної стеганографічної ємності системи обраховується за формулою:

$$w_{\text{відн}}^{(m)} = \frac{w_{\text{вбуд}}^{(m)}}{W_{\text{контейнеру}}} * 100\% = \frac{3 * z_{\text{стрічок}} * z_{\text{стовпців}}}{m * W_{\text{контейнеру}}} * 100\%,$$

де $z_{\text{стрічок}}$ $z_{\text{стовпців}}$ – розмір контейнеру у вигляді двомірної матриці.

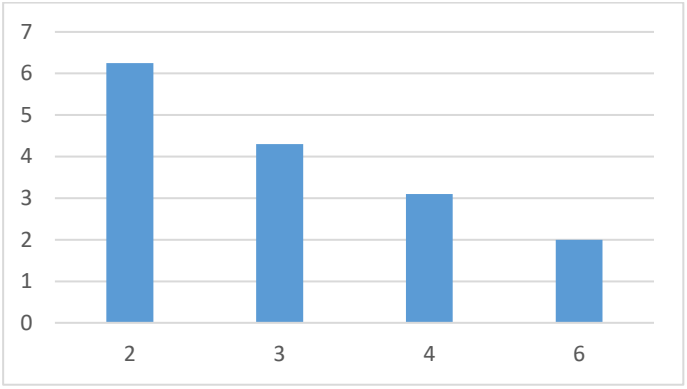

Рисунок 3 – залежність значення $w_{\text{відн}}^{(m)}$ від довжини m НПЧ

З аналізу рисунку 2.3 можна зробити висновок, що в випадку формування НПЧ довжиною m = 2, відносна стеганографічна ємність системи становить 6,25%, а при m=6 ємність системи становить 2%.

При перевірці стійкості до атак зловмисника, доцільно розглядати атаки до руйнування вбудованого повідомлення. Для оцінки будуть використані наступні атаки:

– виконання прямого та зворотного дискретного косинусного перетворення з округленням до цілих значень

– пряме та зворотне квантування з різними факторами втрати якості.

Для атак будуть обрані три зображення з різною насиченістю. Також для аналізу будуть використані:

– набір нерівноважних позиційних чисел m = 2;3;4;6;

– формуваннння НПЧ буде проведено до 3 кольорових компонент

– коефіцієнт квантування обирається з набору q = 1;2;5;10.

В таблиці 2.1 представлені отримані при тестуванні значення безпомилково отриманих біт відносно кількості вбудованих біт в умовах атак.

Таблиця 1 – кількість безпомилкових отриманих біт

	Кількість безпомилково отриманих біт, %			
	m=2	m=3	m=4	m=6
Без атаки	100	100	100	100
ДКП	98.3	99.3	99.7	99.9
Q=1	80.4	91.9	96.8	99.4
Q=2	78.5	91	96.4	99.3
Q=5	75.6	90	95.9	99.3
Q=10	74.1	89.1	95.4	99.2

Провівши аналіз значень з таблиці 2.1 можна зробити висновки, що:

– даний стеганографічний кодування в умовах без проведення активних атак має 100% безпомилковість видобування повідомлення незалежно від нерівноважного позиційного числа

– в умовах атаки ДКП и квантування з кроком 10 найменший відсоток правильно видобутих біт повідомлення при НПЧ довжиною 2

– найбільший відсоток правильно отриманих біт при атаці ДКП та квантуванні з кроком 10 при НПЧ довжиною 6.

Проаналізувавши отримані дані можна зробити висновок, що для різних коефіцієнтів квантування кількість правильно отриманих біт повідомлення в середньому складає 90%. Також було виконано реалізацію програмного додатку на основі вдосконаленого методу, а саме розроблено програму для вбудовування інформації у зображення.

Висновки

Проаналізовано можливості вдосконалення стійкості інформаційних ресурсів в системах безпеки. Удосконалено структурного стеганографічного кодування, а саме підвищено стійкість до активних стеганографічних атак. Розроблено алгоритм та програмний засіб для реалізації вдосконаленого методу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аграновски А.В. Стеганография, цифровые водяные знаки и стегоанализ [Тест]: учеб. пособие для вузов / А.В. Аграновски, А.В. Балакин,В.Г. Грибунин. – М.:Вузовская книга, 2009. – 220 с.

2. Баранник Д.В. Концепция структурного стеганографического кодирования с маскированием / Д.В. Баранник, А.Е. Бекиров // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 4 - 11.

3. Баранник В.В. Технология неравновесного позиционного кодирования для функционального преобразования чисел со встроенной информаций / В.В. Баранник, Ю.Н. Рябуха, А.Э. Бекиров // Радиоэлектронные и компьютерные системы. – 2014. - №4. - С. 32 - 39

Кормщикова Світлана Олексіївна – студент групи УБ-17м, факультет менеджменту, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: owl.svetik@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – канд.техн.наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця

Kormshchykova Svitlana O. — – student of group UB-17m, Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia

Supervisor: **Karpinets Vasyl V**. — Ph. D. Assistant professor, management and security of information Systems department; Vinnitsa, Ukraine;