Теоретичні основи розробки та експлуатації систем озброєння

УДК 681.3 DOI: 10.30748/soivt.2021.66.04

А.Е. Бекіров

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

ФОРМУЛЮВАННЯ ВИМОГ ДО АЛГОРИТМУ ПОШУКУ ЕЛЕМЕНТІВ ПРОСТОРОВОГО ПРЕДСТАВЛЕННЯ КОНТЕЙНЕРУ ДЛЯ СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ

У статті розглядається актуальне питання забезпечення стійкості стеганографічних методів на основі модифікації найменш значущих бітів в умовах застосування атак. Розглядаються особливості функціонування методів статистичного стеганографічного аналізу. Для забезпечення зниження рівня статистичних обурень в результаті вбудовування пропонується напрямок на основі застосування алгоритму пошуку елементів в контейнері. Формулюються вимоги до алгоритму пошуку, які передбачають врахування семантичних та синтаксичних особливостей контейнеру, забезпечують зменшення рівня візуальних спотворень в умовах заданого значення стеганографічної ємності та передбачають застосування адаптивного ключового правила.

Ключові слова: *стеганографічний аналіз, алгоритм пошуку, стеганографічна ємність.*

Вступ

Постановка проблеми. Велика кількість публікацій, пов'язаних з розробкою нових або покращенням характеристик вже існуючих методів стеганографічних перетворень, супроводжується створенням дієвих способів детектування скритного вбудовування в контейнерах. Враховуючи, що стеганографічна модифікація змінює статистичні характеристики елементів представлення вихідних контейнерів, велика кількість методів стеганографічного аналізу побудовано саме на розрахунку та оцінці метрик, які характеризують ступінь спорідненості міжелементних зв'язків у контейнері [1–4].

Складність застосування методів стеганографічного аналізу пов'язана з відсутністю апріорної інформації про метод вбудовування, довжину корисного повідомлення, області вбудовування (у разі попередньої селекції робочих областей). Для найбільш поширених методів стеганографічного аналізу результат оцінки наявності вбудовування уявляє собою ймовірнісне значення, наприклад: "вірогідність присутності вбудовування 56%" [3]. Тому рішення задачі детектування вбудовування передбачає використання у комплексів декількох, різних за принципом, методів стеганографічного аналізу [5–6].

Аналіз останніх досліджень і публікацій. Найбільш відомим методом стеганографічного вбудовування в зображення є метод заміни найменш значущого біту, принцип роботи якого засновано на заміні молодшого біту двійкового представлення елементів контейнеру. Поряд з простотою та великою стеганографічною ємністю даний метод є нестійким до статистичних алгоритмів стеганографічного аналізу, а саме методу "хи-квадрат" та RS-методу [7].

Подальший розвиток стеганографічних методів родини НЗБ, направлений на підвищення стійкості вбудовування до стеганографічного аналізу, пов'язаний з вибором елементів для вбудовування.

Так, метод псевдовипадкового інтервалу передбачає вбудовування бітів не в кожний елемент контейнеру, а через інтервали, які визначаються на основі псевдовипадкового закону. В даному випадку правило формування псевдовипадкової послідовності є додатковою ключовою інформацією, яка повинна бути відома на передавальній та приймальній стороні. Аналіз стійкості алгоритму до виявлення вбудовування на основі методу "хи-квадрат" показує значне зниження вірогідності встановлення факту наявності додаткової інформації. Але в той же час, метод псевдовипадкового інтервалу є нестійким до стеганографічного аналізу RS-методом [8].

Подальшим розвитком методу найменшого значущого біту є метод псевдовипадкового розподілу вбудованого повідомлення. Сутність методу полягає у вбудовуванні бітів, які розподілені на основі

псевдовипадкового правила. Композиція вихідного інформаційного повідомлення на приймальній стороні відбувається на основі ключового правила. Метод є стійким до атак, направлених на вилучення вбудованого повідомлення, але не впливає на зміни статичних характеристик контейнера [9–11].

Для забезпечення стійкості методів модифікації елементів просторового представлення до статистичного стеганографічного аналізу пропонується на прикладі методу найменш значущого біту розробити алгоритм вибору елементів контейнера для приховуваного вбудовування.

Мета статті – формулювання вимог до алгоритму пошуку елементів контейнеру для приховуваного вбудовування даних на основі методу найменш значущого біту.

Виклад основного матеріалу

Враховуючи особливості функціонування методів стеганографічного вбудовування, при розробці алгоритму пошуку робочих елементів необхідно забезпечення низки вимог, які характеризують алгоритм з позицій зменшення спотворень контейнеру одночасно з забезпеченням заданого значення стеганографічної ємності методу вбудовування.

З позиції зменшення статистичних характеристик вихідного зображення, результати роботи алгоритму пошуку елементів для різних контейнерів в однакових умовах повинні бути різними. Дана вимога обумовлена необхідністю врахування семантичної та синтаксичної складової контейнеру при виділенні елементів для вбудовування. Іншими словами, для двох різних контейнерів, при однакових умовах роботи алгоритму, положення елементів для вбудовування будуть різними. Для оцінки відповідності алгоритму пошуку щодо сформульованої вимоги пропонується використовувати метрику Ψ, величина якої характеризує ступінь відмінності між результатами роботи алгоритму для двох різних контейнерів:

$$\Psi = \phi(S_{sel}^{(1)}, S_{sel}^{(2)}), \qquad (1)$$

де $\phi(\bullet)$ – функціонал для здійснення операції порівняння;

$S_{sel}^{(1)}$ та $S_{sel}^{(2)}$ – множини позицій вбудовування для двох різних контейнерів.

В ідеальному випадку величина Ψ буде приймати максимальне значення: $\Psi \to \infty$.

Для забезпечення стійкості атаки на основі відомого вбудованого повідомлення, позиції елементів для вбудовування, визначених на основі алгоритму пошуку, для однакового контейнеру при різних умовах роботи будуть приймати різні значення. Іншими словами, здійснення пошуку елементів з різним ключовим правилом k для контейнеру буде супроводжуватись різними значеннями позицій елементів для вбудовування:

$$S_{sel}^{(1,k_1)} = f(S_1, k_1) \neq S_{sel}^{(1,k_2)} = f(S_1, k_2), \qquad (2)$$

де $f(\bullet)$ – оператор роботи алгоритму пошуку елементів для вбудовування;

$S_{sel}^{(1,k_1)}$ та $S_{sel}^{(1,k_2)}$ – множини позицій вбудовування для контейнеру S_1 при використанні ключових правил k_1 та k_2.

В даному випадку метрика $\Psi = \phi(S_{sel}^{(1,k_1)}, S_{sel}^{(1,k_1)})$ також буде примати максимальне значення: $\Psi \to \infty$.

Також для алгоритму пошуку елементів вбудовування повинна бути можливість адаптивної зміни ключового правила k з метою приведення кількості $q_{S_{sel}}$ обраних елементів до кількості q_B бітів, яка міститься у інформаційному повідомлені B. Для відповідності алгоритму пошуку даній вимозі ключове правило поряд з статичними коефіцієнтами $\{k_{n,m}\}$ визначення позиції елементів, буде містити адаптивний поріг M_{edg}. Відношення елементів контейнерів до множини S_{sel} здійснюватиметься шляхом порівняння результатів значень елементів з пороговим значенням M_{edg}. Тоді визначення елементів для вбудовування буде містити три етапи:

– етап застосування ключового правила k до вихідного зображення з метою отримання позицій потенційних елементів для вбудовування:

$$S_{sel} = f(S, k); \qquad (3)$$

– порівняння елементу $s_{i,j}$ множини S_{sel} виділених елементів з пороговим значенням M_{edg}. Якщо кількість $q_{S_{sel}}$ елементів є недостатньою для вбудовування повідомлення B, то в даному випадку значення порогу M_{edg} зменшується: $q_{S_{sel}} < q_B \to M_{edg} \downarrow$, і навпаки, якщо кількість виявлених елементів більша ніж потрібно для вбудовування повідомлення B, значення величини M_{edg} збільшується:

$$q_{S_{sel}} > q_B \to M_{edg} \uparrow. \qquad (4)$$

У випадку, коли не висуваються вимоги до довжини інформаційного повідомлення B, значення порогу M_{edg} може бути обрано постійним $M_{edg} = const$.

Тоді для кожного контейнера S_z, $z = \overline{1; Z}$, кількість $q_{S_{sel}^{(z)}}$ обраних елементів для вбудовування може бути різною:

$$q_{S_{sel}^{(1)}} \neq q_{S_{sel}^{(z)}} \neq q_{S_{sel}^{(Z)}}, z = \overline{1; Z}. \quad (5)$$

Для відповідності умовам оперативності обміну повідомленнями необхідно забезпечити можливість розрахунку статичних коефіцієнтів $\{k_{n,m}\}$ ключового правила k визначення елементів вбудовування з врахуванням особливостей синтаксичного представлення контейнеру. У випадку забезпечення даної вимоги відсутня необхідність створення додаткового каналу передачі даних для відправлення отримувачу ключового правила. Іншим варіантом вирішення проблематики створення додаткового каналу передачі ключів є заздалегідь підготовлені набори коефіцієнтів $\{k_{n,m}\}$, які відомі на передавальній та приймальній стороні.

Умови взаємооднозначності прямого і зворотного алгоритму передбачає, що внесення спотворень в результаті стеганографічного перетворення не повинно впливати на результати роботи алгоритму пошуку елементів для вилучення інформаційної послідовності на приймальній стороні. Дана вимога передбачає, що значення S'_{sel} множини для вилучення вбудованої інформації, яке отримано в результаті зворотного алгоритму $f^{(-1)}(\bullet)$ пошуку елементів та значення S_{sel} будуть ідентичними:

$$S'_{sel} = f^{(-1)}(G, k_1) = S_{sel}, \quad (6)$$

де G – стеганограмма, отримана на приймальній стороні.

В даному випадку величина $\mu(B, B')$, яка характеризує ступінь відмінності між вихідним B та вилученим B' інформаційним повідомленням буде мінімальною:

$$\mu(B, B') = 0. \quad (7)$$

Також важливою умовою є можливість врахування при пошуку елементів семантичних особливостей контейнера та системи людського ока. Для методу вбудовування з використанням алгоритму пошуку елементів характерним буде зниження стеганографічною ємності. Враховуючи, що множина S_{sel} містить менше елементів ніж вихідний контейнер S, кількість q_B бітів вбудованого інформаційного повідомлення у контейнер S буде більшою ніж кількість $q_B^{(sel)}$ вбудованих біт в множину елементів S_{sel}:

$$q_B > q_B^{(sel)}. \quad (8)$$

Максимальна кількість інформації, що вбудовується контейнер є важливою характеристикою стеганографічного методу. Тому, одним із напрямків забезпечення умови $q_B \approx q_B^{(sel)}$ внесення більшого ступеня спотворень в елементи множини S_{sel} шляхом заміни двох і більше найменш значущих біта. Для зниження рівня візуальних спотворень в елементи контейнера, для алгоритму пошуку є важливим забезпечення селекції елементів з врахуванням особливостей системи людського ока.

Так, з одного боку, умови візуальної атаки характеризуються низькою чутливістю атакуючого до низькочастотного шуму та високою чутливістю до високочастотних спотворень. Також важливу роль для атакуючого відіграє чутливість до адаптивної зміни яскравості в залежності від діапазону.

З іншого боку, семантична складова кожного окремого контейнеру є особливою, що значно ускладнює завдання підбору коефіцієнтів $\{k_{n,m}\}$ для алгоритму пошуку. Можливим варіантом розв'язання проблеми врахування семантичної складової є класифікація контейнерів по визначеним ознакам, наприклад: аерофотознімок земної поверхні, зображення будівель, ландшафту і т.д.

Сформульовані вимоги до алгоритму пошуку елементів для вбудовування в просторову область зображень охоплюють особливості роботи методів стеганографічного перетворення особливості синтаксичної побудови контейнерів. Серед обмежень сформульованої системи вимог можна відзначити відсутність врахування змісту інформаційного повідомлення, яке вбудовується.

Висновки

На основі аналізу особливостей функціонування методів статистичного стеганографічного аналізу алгоритмів вбудовування на основі модифікації найменш значущих бітів запропоновано напрямок для підвищення стеганографічної стійкості, який полягає у застосуванні алгоритму пошуку елементів для вбудовування.

Сформульовано систему вимог, яка відповідає особливостям функціонування методів стеганографічного вбудовування. Так, до важливих характеристик алгоритму пошуку елементів для вбудовування визначено наступні:

1. Результати роботи алгоритму пошуку елементів при однакових умовах функціонування для різних контейнерів приймають різні значення.

2. Застосування алгоритму пошуку з різним ключовим правилом для однакового контейнеру передбачає різні позиції елементів для вбудовування.

3. Стійкість алгоритму виявлення позицій елементів на приймальній стороні до спотворень контейнеру, які виникають в результаті вбудовування.

4. Адаптивна зміна коефіцієнтів ключового правила відповідно до довжини інформаційної послідовності.

5. Врахування семантичної складової контейнеру та системи людського ока при визначенні позицій елементів для вбудовування.

Подальшим напрямком дослідження визначено формування системи властивостей функціоналу для здійснення алгоритму пошуку, яка забезпечує виконання сформульованих у статті вимог.

Список літератури

1. Задирака В.К. Статистичний аналіз систем с цифровими водяними знаками / В.К. Задирака, Н.В. Кошкіна, Л.Л. Никитенко // Штучний інтелект. – 2008. – № 3. – С. 315-324.

2. Al-Shatnawi A.M. A new method in image steganography with improved image quality / A.M. Al-Shatnawi // Applied Mathematical Science. – 2012. – № 6(79). – P. 3907-3915.

3. Avinash K.G. A high capacity secured image steganography method with five pixel pair differencing and LSB substitution / K.G. Avinash, S.J. Madhuri // Graphics and Signal Processing. – 2015. – № 5. – P. 66-74.

4. Юдін О.К. Захист інформації в мережах передачі даних: підручник / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко. – К.: ТОВ НВП "ІНТЕРСЕРВІС", 2009. – 714 с.

5. Danik Yu. Synergistic effects of information and cybernetic interaction in civil aviation / Yu. Danik, R. Hryschuk, S. Gnatyuk // Aviation. – 2016. – № 3(20). – P. 137-144.

6. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатов. – К.: Юниор, 2003. – 501с.

7. Ravi Shankar Reddy M. A novel method for steganography in spatial domain / M. Ravi Shankar Reddy, Sri J. Swami Naik // International Journal of Advanced Research in Computer Science and Software Engineering. – 2013. – № 3(10). – P. 1117-1122.

8. Бекіров А.Е. Технологія селекції областей аерофотознімку з різною насиченістю для стеганографічного перетворення / А.Е. Бекіров, В.Ж. Ященок, О.М. Крейдун // Сучасні інформаційні технології у сфері безпеки та оборони. – 2019. – № 1(34). – С. 55-60. https://doi.org/1.33099/2311-7249/2019-34-1-115-120.

9. Jassim F.A. Five modulus method for Image compression / F.A. Jasim // Signal and Image Processing. – 2012. – № 5(3). – P. 26-34.

10. Бекіров А.Е. Стеганографічний метод на основі безпосереднього та непрямого вбудовування даних для областей зображення з різною насиченістю / А.Е. Бекіров, В.Ж. Ященок, О.М. Крейдун // Сучасні інформаційні технології у сфері безпеки та оборони. – 2020. – № 1(37). – С. 115-120. https://doi.org/10.33099/2311-7249/2020-37-1-55-60.

11. Cox I.J. Digital watermarking and steganography / I.J. Cox, J.A. Bloom, T. Fridrick. – Burlington: Morgan Kaufman Publishers. – 591 p.

12. Fufang L. Text steganography based on ci-poetry generation using Markov chain model / Li Fufang, Yubo Luo, Yongfeng Huang, Chinchen Chang // KSII Transactions on Information and Systems. – 2016. – № 10(9). – P. 4568-4584.

Надійшла до редколегії 16.04.2021
Схвалена до друку 12.05.2021

Відомості про автора:

Бекіров Алі Енверович
кандидат технічних наук старший викладач
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-6155-0597

Information about the author:

Ali Bekirov
Candidate of Technical Sciences Senior Instructor
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-6155-0597

ФОРМУЛИРОВАНИЕ ТРЕБОВАНИЙ К АЛГОРИТМУ ПОИСКА ЭЛЕМЕНТОВ ПРОСТРАНСТВЕННОГО ПРЕДСТАВЛЕНИЯ КОНТЕЙНЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ

А.Э. Бекиров

В статье рассматривается актуальный вопрос повышения стойкости стеганографических методов к статистическим стеганографическим атакам. С позиции изменений статистических свойств в результате встраивания наиболее слабыми являются методы встраивания в наименее значимые биты. На основе анализа функционирования методов статистического стеганографического анализа предложен подход в виде использования алгоритма поиска оптимальных элементов контейнера для встраивания данных. Сформулированы требования, которые должны удовлетворяться в процессе разработки алгоритма встраивания. Применения единого ключевого правила алгоритма поиска для разных по семантическому и синтаксическому содержанию контейнеров должно сопровождаться разными позициями элементов для встраивания. Устойчивость метода встраивания с учетом разработанного алгоритма поиска к атакам с известным встроенным сообщением должна обеспечиваться за счет разных результатов позиций элементов для единого контейнера в условиях применения разных ключевых правил. Условие взаимно-однозначности прямого и обратного алгоритма поиска обеспечивается за счет удовлетворения требования стойкости алгоритма к модификациям значений элементов в результате стеганографического встраивания. Изменение длины встраиваемого сообщения сопровождается изменением количества выделенных элементов за счет адаптивного изменения порога выявления. Стойкость к визуальным атакам злоумышленника обеспечивается за счет работы алгоритма поиска с учетом семантической составляющей контейнера и особенностей системы человеческого глаза.

Ключевые слова: *стеганографический анализ, алгоритм поиска, стеганографическая емкость.*

FORMULATION OF REQUIREMENTS TO THE ALGORITHM FOR SEARCHING THE ELEMENTS OF THE SPATIAL REPRESENTATION OF A CONTAINER FOR STEGANOGRAPHIC EMBEDDING

A. Bekirov

The article discusses the topical issue of increasing the resistance of steganographic methods to statistical steganographic attacks. From the point of view of changes in statistical properties as a result of embedding, the methods of embedding in the least significant bits are the weakest. Based on the analysis of the functioning of statistical steganographic analysis methods, an approach in the form of using an algorithm for finding the optimal container elements for embedding data is proposed. Requirements that must be satisfied in the process of developing an embedding algorithm are formulated. The application of a single key rule of the search algorithm for containers with different semantic and syntactic content should be accompanied by different positions of elements for embedding. The stability of the embedding method, taking into account the developed search algorithm, against attacks with a known embedded message should be ensured due to different results of the positions of elements for a single container under the conditions of applying different key rules. The one-to-one condition of the forward and reverse search algorithms is ensured by satisfying the requirement of the algorithm's resistance to modifications of element values as a result of steganographic embedding. In this case, on the receiving side, the presence of element distortions does not affect the correct positioning of the elements of the container with embedded information. A change in the length of an embedded message is accompanied by a change in the number of selected elements due to an adaptive change in the detection threshold. This condition also potentially reduces the level of introduced distortion. It is also possible to use a static threshold value by decomposing the inline element into blocks. Resistance to visual attacks by an intruder is ensured by robots of the search algorithm, taking into account the semantic component of the container and the features of the human eye system. The need to satisfy this requirement also arises from the condition of ensuring a predetermined level of steganographic capacity by increasing the degree of distortion of the container elements identified on the basis of the developed search algorithm.

Keywords*: steganographic analysis, search algorithm, steganographic capacity.*