Спосіб стеганографічного захисту графічних даних на основі схеми відповідності бітів та аналізу візуальних властивостей контейнера

Радченко Є. О., Сулема Є.С.

Кафедра програмного забезпечення комп'ютерних систем,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Київ, Україна
radchenko.zh@gmail.com

Graphical Data Steganographic Protection Method Based on Bits Correspondence Scheme and Cover Visual Properties Analysis

Yevhen Radchenko, Yevgeniya Sulema
Computer Systems Software Department,
The National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine radchenko.zh@gmail.com

***Анотація*—Запропоновано вдосконалений спосіб захисту графічних даних на основі схеми відповідності бітів, в якому стеганографічне вбудовування даних, що підлягають захисту, виконується з врахуванням візуальних особливостей зображення, що виступає у ролі контейнера.**

***Abstract*—The advanced method of graphical data protection based on the bits correspondence scheme is proposed. In this method the steganographic embedding of data to be protected is fulfilled with consideration of visual specificity of the image used as a cover.**

Ключові слова—захист даних; стеганографія

Keywords—data protection; steganography

I.Вступ

Графічні дані є одними з найбільш поширених типів даних. Їх перевага полягає у легкості сприйняття людиною. Потужність обчислювальних засобів дозволяє зберігати, оброблювати та передавати все більше інформації саме в графічному вигляді. Зростання кількості графічних даних, доступних на різноманітних ресурсах у мережі, обумовлює нові вимоги щодо забезпечення безпеки зберігання та передавання цих даних. Оскільки при зберіганні зображень у відкритому доступі існує загроза їх несанкціонованого використання, захист графічних даних саме шляхом стеганографічного вбудовування одного зображення (що підлягає захисту) в інше зображення (яке виступає у ролі контейнера) є одним з найбільш ефективних шляхів захисту конфіденційних даних користувача. Стеганографічний захист даних забезпечує приховання самого факту їх наявності за рахунок використання певного маскуючого алгоритму, що модифікує масив відкритих даних, додаючи до них послідовність даних, що потребує захисту. Проте сам факт непомітності передачі даних ще не позбавляє можливості несанкціонованого доступу до цих даних – у разі стеганографічної атаки ці дані можуть бути виявлені і стати доступними сторонньому спостерігачу, якому для їх перегляду потрібно дізнатись використовуваний стеганографічний алгоритм. Тому на практиці стеганографічне вбудовування даних в контейнер відбувається в зашифрованому вигляді. Хоча на сьогодні існує велика кількість різноманітних підходів до стеганографічного захисту даних, потреба у розроблені нових методів захищеної передачі даних залишається через наявність значної кількості графічних форматів. Отже, значну увагу слід приділяти безпеці передачі цих даних з урахуванням особливостей стандартів кодування та форматів даних.

Графічні дані є набором значень, що визначають інтенсивність відтінку кольору у певній точці

зображення (пікселі). Для опису відтінку кольору кожного пікселя використовується 8 біт, що дозволяє відображувати 256 відтінків певного кольору. Кольорові цифрові зображення потребують 24-бітного представлення кольору – по 8 біт на кожен з 3 первинних кольорів. Найбільш поширені первинні кольори – це червоний, зелений та синій, що складають колірну модель RGB. Оскільки у такий спосіб можливо отримати 256 варіантів кожного базового кольору, в результаті маємо 16 мільйонів відтінків кольорів, що створює сприятливі умови для стеганографічного приховування даних у зображеннях.

II. Існуючі рішення

Існуючі стеганографічні методи поділяються на декілька груп [1-3] залежно від типу носія прихованих даних (контейнера) та способу приховування. Застосування зображень у ролі контейнера передбачає, що дані, які потребують захисту, приховуються у значеннях коду відтінку кольору. До способів вбудовування даних у зображення-контейнер відносяться наступні:

1. Модифікація наймолодших значущих бітів контейнера.
2. Модифікація коефіцієнтів дискретного косинусного перетворення (окремим випадком цього способу є застосування формату JPEG).
3. Модифікація коефіцієнтів вейвлет перетворення.
4. Модифікація бітових площин.

Для покращення ефективності методів стеганографії для зберігання даних графічного характеру доцільним є використання контейнеро-орієнтованої стегосистеми [4].

III. Опис методу

Модифікований спосіб захисту графічних даних, що пропонується, ґрунтується на базовому методі стеганографічного захисту на основі модифікації наймолодших значущих бітів контейнера та застосування схеми відповідності бітів [5], основою якого є певна схема перетворення бітів (рис. 1). Це схема виступає у ролі приватного ключа. Вона встановлює зв’язок між молодшими та старшими бітами послідовності, що кодує відтінок кольору чергового пікселя зображення. Відповідно до обраної схеми застосовується алгоритм перетворення бітів [6].

Процедура стеганографічного вбудовування даних, що підлягають захисту, у зображення-контейнер, яка є основою запропонованого способу стеганографічного захисту, включає наступні етапи:

1. Обирається булева функція, що гарантує відновлення зашифрованих даних [7].
2. Обрана функція (наприклад, виключна диз'юнкція) послідовно застосовується до всіх пар пов’язаних відповідно до обраної схеми відповідності бітів молодшого та старшого бітів даних, що приховується.

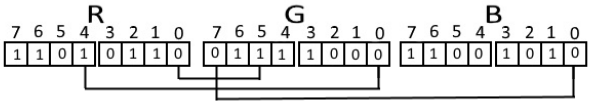

Рис. 1. Приклад схеми відповідності бітів

3. Зашифровані дані, отримані на попередньому етапі, вбудовуються у зображення-контейнер. Для цього кожен наступний «дозволений» молодший біт графічних даних контейнера заміщується черговим бітом зашифрованої послідовності. «Дозволеним» вважається молодший біт коду кольору пікселя, що не належить до однорідної зони зображення-контейнера – області на зображені, кожен піксель якої має однакове або близьке значення інтенсивності відтінку кольору порівняно з сусідніми пікселіми.

Головним фактором, що впливає на візуальне сприйняття зображення, є співвідношення кількості пікселів, що формують області зображення, де закономірності переходів і послідовностей значень пікселів породжують очікувані значення сусідніх пікселів, до загальної кількості пікселів. Особливо помітними є спотворення в областях зображення з однаковими характеристиками кольору та яскравості, де очікуваним фактом є те, сусідні пікселі будуть мати однаковий колір.

Отже, однорідною зоною будемо називати послідовність пікселів, що розташовані поруч та різниця компонент R, G та B яких не перевищує задану константу C (ціле додатне число). У такі зони дані вбудовуватись не будуть, щоб не знижувати стеганографічну стійкість контейнера. На рис. 2 представлений приклад зображення з виділеним прямокутником фрагментом однорідної зони. На рис. 3 проілюстровано внутрішнє подання графічних даних в однорідній зоні. Як можна побачити, таблиця значень яскравості кольору в однорідній зоні переважно містить однакові значення, що повторюються.

Рис. 2. Зображення з виділеним фрагментом однорідної зони

При змінні навіть однієї компоненти у пікселі, що знаходиться в однорідній зоні на одиницю, стегоаналітичні програми можуть розпізнати факт приховування даних у контейнері. Тому після вбудовування контейнер з прихованими даними знову перевіряється на наявність нових однорідних зон, що можуть з'явитись в результаті вбудовування даних у контейнер. У цьому випадку код відтінку кольору пікселів, що належать до нових однорідних зон, модифікуються таким чином, щоб мінімально змінити значення компонент цього пікселя не змінюючи останній біт, який є елементом послідовності даних, що приховується. Процес аналізу та модифікації однорідних зон продовжується, доки не буде оброблено всі нові зони.

235	235	235	235	235	235	235	235	235	235	235	235	235	235	235
233	233	233	233	233	233	233	233	233	233	233	233	233	233	233
235	235	235	235	235	235	235	235	235	235	235	235	235	235	235
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234
234	234	234	234	234	234	234	234	234	234	234	234	234	234	234

Рис. 3. Фрагмент таблиці значень яскравості кольору в однорідній зоні

IV. Аналіз методу

Оцінимо нижню межу оцінки ймовірність несанкціонованого доступу до прихованих даних. Ця ймовірність визначається як:

$$p_{loc} = \frac{N_{favourite}}{N_{all}}, \qquad (1)$$

Сприятливий випадок лише один – коли зловмисник знає стеганографічну схему, тобто $N_{favourite}$ = 1. Загальна кількість шансів для вгадування визначається запропонованою стеганографічною схемою:

$$N_{all} = C_{8-k}^{m} \cdot C_{3xy}^{q} = \frac{(8-k)!}{m!\cdot(8-k-m)!} \cdot \frac{(3xy)!}{q!\cdot(3xy-q)!}, \qquad (2)$$

де C_{8-k}^{m} визначає кількість можливих комбінацій старших та молодших бітів;

k – це кількість молодших бітів, що використовується для приховання даних;

m – це кількість старших бітів, що використовуються для перетворення даних, що підлягають приховуванню;

C_{3xy}^{q} визначає кількість можливих розміщень q біт даних, що приховуються у контейнері – зображені $x{\times}y$, представленому у кольорній моделі RGB, тобто для представлення відтінку кольору кожного пікселя використовуються 3 байти.

Тоді нижня межа оцінки ймовірності знаходження прихованих бітів у контейнері може бути оцінена як:

$$p_{loc} = \frac{q!\cdot(3xy-q)!\cdot m!\cdot(8-k-m)!}{(3xy)!\cdot(8-k)!}, \qquad (3)$$

Для визначення верхньої межі оцінки ймовірність несанкціонованого доступу до прихованих даних потрібно врахувати наявність та загальний розмір однорідних зон у контейнері, що залежить від обраного зображення.

Таким чином, можна зробити загальний висновок, що даний спосіб є стійким до несанкціонованого доступу до даних шляхом вгадування стеганографічної схеми.

V. Висновки

У даному дослідженні вирішувалась задача вдосконалення стеганографічного способу захисту інформації, що орієнтується на графічний тип даних та візуальні властивості контейнера. У процесі дослідження були проаналізовані існуючі способи стеганографічного захисту зображень, їх переваги і недоліки.

Аналіз стійкості запропонованого способу до несанкціонованого доступу до прихованих даних показав, що ймовірність вгадування стеганографічної схеми є низькою. Отже, запропонований спосіб може використовуватись у випадках, коли стеганографічний захист вважається більш доцільним, ніж криптографічний.

Література References

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", *Signal Processing*, 2010, vol. 90, issue 3, pp. 727-752.

[2] S. Bhattacharyya, I. Banerjee, G. Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", *Journal of Global Research in Computer Science*, 2011, Volume 2, No. 4, pp. 1-16.

[3] Ivan Dychka, Semen Shyrochyn, Yevgeniya Sulema, "Analysis of Parallel Computations Efficiency for User's Private Multimedia Data Protection in Clouds", *Research Bulletin of the National Technical University of Ukraine "Kyiv Polytechnic Institute"*, 2016, Issue 1, pp. 40-46.

[4] Yevgeniya Sulema, Semen Shyrochyn, "Criteria of Search of Optimal Placement of Stegodata Blocks in Container", *Proceedings of the International Conference "System Analysis and Information Technologies" (SAIT 2011)*, Kyiv, Ukraine, 2011, p.516.

[5] Zhengbing Hu, Ivan Dychka, Yevgeniya Sulema, Yevhen Radchenko, "Graphical Data Steganographic Protection Method Based on Bits Correspondence Scheme", *International Journal of Intelligent Systems and Applications (IJISA)*, vol. 9, issue 8, pp. 34-40, 2017, DOI: 10.5815/ijisa.2017.08.04.

[6] Yevgeniya Sulema, Yevhen Radchenko, "Algorithm of graphical data stegonagraphic protection based on bits difference transform", *Proceedings of the 8th Conference of young scientists "Applied Mathematics and Computing" (PMK-2016)*, Kyiv, Ukraine, 2016, pp. 254-258. (in Ukrainian).

[7] Yevgeniya Sulema, "Image Protection Method Based on Binary Operations", *Proceedings of the 23rd IEEE International Conference on Systems, Signals and Image Processing IWSSIP2016*, Bratislava, Slovakia, 2016, pp. 295-29