УДК 004.056.5

В.М. Білоус
Д.С. Лавренюк

УДОСКОНАЛЕННЯ МЕТОДУ LSB-СТЕГАНОГРАФІЇ НА ОСНОВІ КОНТУРНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНОЇ МАРШРУТИЗАЦІЇ

Вінницький національний технічний університет

Анотація

У роботі досліджено проблему виявлення прихованих даних у класичних LSB-методах стеганографії та обґрунтовано необхідність підвищення їх стійкості до статистичного аналізу. Запропоновано гібридний крипто-стеганографічний алгоритм, що поєднує контурно-адаптивне вбудовування з псевдовипадковою маршрутизацією на основі криптографічного ключа. Реалізовано механізм стабілізації бітової площини та детермінованого відтворення координат. Проведене тестування підтвердило високу криптостійкість і непомітність методу, що робить його перспективним для захисту інформації.

Ключові слова: стеганографія, LSB-метод, стегоаналіз, криптографічна маршрутизація, контурно-адаптивне вбудовування.

Abstract

The paper investigates the problem of detecting hidden data in classical LSB steganography methods and justifies the need to increase their resistance to statistical analysis. A hybrid crypto-steganographic algorithm is proposed, combining contour-adaptive embedding with pseudo-random routing based on a cryptographic key. A mechanism for stabilizing the bit plane and deterministic coordinate reproduction is implemented. The testing confirmed the high crypto-resistance and invisibility of the method, which makes it promising for information protection.

Keywords: steganography, LSB method, stegoanalysis, cryptographic routing, contour-adaptive embedding.

Вступ

У сучасних умовах безпрецедентного зростання обсягів передачі цифрових даних та постійного вдосконалення методів мережевого перехоплення, забезпечення надійної конфіденційності інформації є одним із фундаментальних завдань кібербезпеки. Традиційні криптографічні системи, незважаючи на їхню математичну стійкість, мають суттєвий концептуальний недолік: зашифрований трафік або файл завжди привертає увагу зловмисників чи систем глибокого аналізу пакетів (DPI). Сам факт наявності незрозумілого набору байтів свідчить про високу цінність інформації, що провокує спроби криптоаналізу або застосування методів соціальної інженерії для отримання ключів доступу. Саме тому в арсеналі фахівців з інформаційної безпеки особливе місце займає стеганографія — наука про приховування самого факту існування таємного повідомлення [1]. Шляхом впровадження корисного навантаження у звичайні цифрові медіафайли (зображення, аудіо, відео), стеганографія дозволяє створити прихований канал зв'язку, який візуально не викликає жодних підозр у сторонніх спостерігачів. Найбільш розповсюдженим, завдяки своїй відносній алгоритмічній простоті та високій пропускній здатності, є метод заміни найменш значущого біта (Least Significant Bit, LSB). Цей підхід базується на особливостях фізіології людського зору, який фізично не здатний розрізнити мінімальні флуктуації кольорових відтінків, спричинені модифікацією останнього біта у байті кольору конкретного пікселя.

Проте, незважаючи на візуальну непомітність, класичний лінійний підхід LSB має критичну алгоритмічну вразливість до методів статистичного стегоаналізу. Традиційна реалізація алгоритму передбачає послідовний запис бітів секретного повідомлення у пікселі зображення-контейнера, починаючи з першого координатного значення і рухаючись рядок за рядком. Таке нелінійне втручання порушує природний статистичний розподіл нулів та одиниць у молодших бітових площинах зображення. Якщо запис здійснюється на великих однотонних ділянках (наприклад, чисте блакитне небо, гладка стіна, елементи комп'ютерної графіки), зміна бітів неминуче формує виражені структурні

аномалії. Сучасні автоматизовані системи та інструментальні засоби стегоаналізу, такі як аналіз гістограм, атака за критерієм χ^2 або метод RS-аналізу, здатні з високою ймовірністю не лише виявити факт наявності прихованих даних, але й точно визначити загальну довжину повідомлення та вилучити його, оскільки координати запису є тривіально передбачуваними. Таким чином, виникає гостра науково-практична потреба у розробці вдосконалених методів, які б забезпечували стійкість як до візуального, так і до глибокого статистичного виявлення.

Результати дослідження

Для подолання проблеми лінійного запису та статистичної передбачуваності в науковій літературі зазвичай пропонуються два окремі підходи. Першим напрямком є використання псевдовипадкового розподілу даних (Pseudo-Random Number Generator LSB, PRNG LSB). У цьому випадку пікселі для модифікації обираються не послідовно, а хаотично, на основі певної математичної послідовності. Це розпорошує дані по всьому контейнеру, суттєво ускладнюючи роботу алгоритмів статистичного аналізу. Другим популярним напрямком є адаптивна до контурів стеганографія (Edge-Adaptive Steganography) [2]. Суть цього підходу полягає у тому, що корисне навантаження приховується виключно у високочастотних ділянках зображення: на геометричних межах об'єктів, у складних текстурах матеріалів або дрібних деталях пейзажу. У таких зонах природний цифровий шум матриці фотокамери є найвищим, тому штучна зміна молодших бітів ідеально маскується під типові артефакти стиснення чи апаратні недоліки сенсора. Однак, ізольоване використання цих методів не гарантує абсолютного рівня захисту. Псевдовипадковий розподіл все одно може з певною ймовірністю потрапити на великі ділянки гладкого фону, де зміна бітів буде миттєво виявлена при аналізі нульової бітової площини. З іншого боку, чистий адаптивний метод залишається вразливим до атаки відтворення: зловмисник, знаючи загальний принцип роботи алгоритму (відповідно до криптографічного принципу Керкгоффса), може самостійно застосувати детектор контурів до аналізованого файлу, отримати масив використаних координат і лінійно зчитати приховані дані.

З метою комплексного усунення описаних недоліків, у даній роботі запропоновано та обґрунтовано модифікований крипто-стеганографічний гібридний алгоритм. Наукова новизна представленого рішення полягає в архітектурній інтеграції методів просторового контурного аналізу зображення з нелінійною динамічною маршрутизацією на основі користувацького криптографічного ключа. Базовим етапом роботи алгоритму є формування інваріантної маски високочастотних ділянок. Для детекції країв об'єктів використовується багатоетапний оператор Canny, який включає попереднє гаусове розмиття, обчислення градієнтів яскравості та придушення немаксимумів [3]. Критичною проблемою традиційної адаптивної стеганографії є те, що сам процес запису даних неминуче змінює значення пікселів на контурах, що може призвести до неможливості точного відтворення маски на стороні легітимного отримувача. Для вирішення цієї алгоритмічної колізії запропоновано метод попередньої стабілізації бітової площини. Перед застосуванням детектора алгоритм виконує побітове обнулення наймолодшого біта кожного пікселя. Це формує стабільну 7-бітну проєкцію зображення, яка є абсолютно стійкою до подальших цілеспрямованих LSB-модифікацій. Завдяки цій математичній операції декодер здатен згенерувати на сто відсотків ідентичну карту просторових координат для подальшого зчитування прихованої інформації.

Наступним етапом є підготовка корисного навантаження. Для забезпечення цілісності даних, стійкості до можливих пошкоджень та повної незалежності від таблиць кодування символів (що є особливо критичним при роботі з багатобайтовими стандартами, такими як UTF-8 для кириличних алфавітів), секретне повідомлення попередньо серіалізується та перетворюється у безпечний текстовий формат Base64. Після цього до отриманого рядка додається спеціальний термінальний маркер, що дозволяє системі динамічно визначати логічний кінець файлу під час операції екстракції. Проте головним вдосконаленням, що забезпечує безпрецедентний рівень захисту запропонованого методу, є запровадження глибокої криптографічної маршрутизації обраних пікселів. На відміну від класичних рішень, де послідовність запису є статичною та передбачуваною, у розробленому алгоритмі використовується динамічний генератор шляху на основі симетричного ключа доступу. Користувацький текстовий пароль хешується за допомогою надійного криптографічного алгоритму SHA-256 [4]. Отримане 256-бітне значення використовується як строго детермінований ініціалізаційний вектор (seed) для системного генератора псевдовипадкових чисел.

Маючи сформований масив координат пікселів, що належать до високочастотних ділянок (контурів), алгоритм застосовує операцію псевдовипадкового перемішування, суворо ініціалізовану отриманим криптографічним хешем [5]. В результаті цього процесу біти секретного повідомлення записуються не послідовно вздовж ліній виявлених контурів, а хаотично розподіляються по всій площі знайдених текстурних аномалій зображення. Такий підхід робить абсолютно неможливим вилучення інформації без знання точного пароля, оскільки будь-яка спроба лінійного або несанкціонованого зчитування контурів призведе до отримання повністю беззмістовного набору бітів. Практична апробація розробленого методу була успішно здійснена шляхом створення функціонального програмного прототипу мовою Python з використанням бібліотек комп'ютерного зору (OpenCV) та систем наукових обчислень (NumPy). Для об'єктивної оцінки криптостійкості та візуальної непомітності отриманих стегоконтейнерів було проведено комплексне тестування за допомогою спеціалізованих утиліт автоматизованого стегоаналізу, зокрема консольного інструменту zsteg, який детально перевіряє всі можливі лінійні комбінації бітових площин. Результати незалежного сканування підтвердили надвисоку ефективність розробленого алгоритму: спеціалізовані утиліти не змогли ідентифікувати наявність корисного навантаження, класифікувавши змінені біти виключно як рівномірний природний шум. Підсумовуючи результати дослідження, можна стверджувати, що інтеграція інваріантної 7-бітної маски контурів з криптографічною генерацією маршруту запису забезпечує надійний захист від несанкціонованого вилучення інформації, що робить розроблений підхід перспективним для впровадження у сучасні системи інформаційної безпеки.

Висновки

У результаті проведеного дослідження було підтверджено, що класичні методи LSB-стеганографії є вразливими до сучасних засобів статистичного стегоаналізу через передбачуваність процесу вбудовування даних. Запропонований гібридний підхід, що поєднує контурно-адаптивне приховування з криптографічно керованою псевдовипадковою маршрутизацією, дозволяє ефективно усунути ці недоліки. Використання інваріантної бітової маски забезпечує коректне відтворення координат, а застосування хеш-функції гарантує високий рівень захисту доступу. Експериментальні результати підтверджують підвищення стійкості до виявлення та вилучення даних, що свідчить про доцільність практичного застосування розробленого алгоритму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mayer J. (Ed.). Steganography: The Art of Hiding Information. London : IntechOpen, 2024. DOI: https://doi.org/10.5772/intechopen.1001493
2. Ismail S. M., AbuAladas F. E., Abu Helou M., Abu-ulbeh W. Edge-Adaptive High-Capacity Image Steganography Using Hybrid Edge Detection and MSB Embedding. Computers. 2026. DOI: https://doi.org/10.3390/computers15030141
3. Nashat D., Mamdouh L. A Least Significant Bit Steganographic Method Using Hough Transform Technique. Journal of Networking and Network Applications. 2023. DOI: https://doi.org/10.33969/J-NaNA.2023.030203
4. Katz, J., Lindell, Y., Introduction to Modern Cryptography. Chapman and Hall/CRC, 2020. DOI: https://doi.org/10.1201/9781351133036
5. Haider T., Blanco S. A., Hayat U. A novel pseudo-random number generator based on multivariable optimization for image-cryptographic applications. Expert Systems with Applications. 2024. DOI: https://doi.org/10.1016/j.eswa.2023.122446

Білоус Віталій Михайлович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: pydev@ukr.net

Лавренюк Дмитро Сергійович – студент групи 1БКС-24б, Факультет інформаційних технологій та комп`ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dims5688@gmail.com

Bilous Vitaliy M – assistant professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: pydev@ukr.net

Lavreniuk Dmytro S – student of group 1BKS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dims5688@gmail.com