

**Нижник Андрій Олегович**

аспірант кафедри захисту інформації

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0009-0003-9094-0740

andrii.o.nyzhnyk@lpnu.ua

Ханін Денис Олегович

аспірант кафедри захисту інформації

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0009-0001-4009-0202

denys.o.khanin@lpnu.ua

**МЕТОД СЕЛЕКТИВНОГО РОЗКРИТТЯ ТА РЕДАГУВАННЯ ЧУТЛИВИХ ФРАГМЕНТІВ
АЕРОЗНІМКІВ ЗІ ЗБЕРЕЖЕННЯМ ПЕРЕВІРНОСТІ ПІДПISY**

Анотація. Аерознімки з безпілотних літальних апаратів, що документують руйнування цивільної інфраструктури, мають лишатися перевірними будь-якою стороною, а перед оприлюдненням із них потрібно вилучати ділянки, розголошення яких створює ризики; монолітний підпис файлу цього не дозволяє, бо руйнується будь-якою зміною пікселів. Запропоновано метод, який переносить відому конструкцію підпису з можливістю редагування на основі дерева Меркля на тайлований георозмічений растр: геоприв'язка входить до підписаного заголовка, прихована область подається мінімальним покриттям піддеревими, політики розширення навмисно збільшують приховану множину, щоб ускладнити визначення положення запитаної ділянки, а первинний підпис лишається чинним для відредагрованої версії без участі підписувача. Вимірювання виконано на синтетичних растрах вичерпним перебором розміщень на сітках від 8×8 до 64×64 тайлів. Для прямокутників 3×3 , 3×4 і 4×5 порядок Мортон дає менше вузлів покриття, ніж рядковий, у 100 % розміщень за медіани відношення 1,20–1,33; для ширини 2 і повернутих форм перевага непова. Для одиночного тайла на сітці 8×8 нормований структурний показник витоку за множиною сумісних положень знижується від 1,0 до 0,17 приховуванням піддерев за 48 % надлишкової площі і до 0,47 фіктивними областями за 12,5 % (для випадкових політик ці оцінки умовні щодо реалізованої процедури інверсії; ймовірнісний витік не оцінювали). Для прямокутника 2×3 квантування кількості тайлів із кроком $q \leq 8$ положення здебільшого не приховує (воно однозначне у 83–100 % пар «розміщення–секрет» на всіх 42 розміщеннях, за $q = 16$ у 17 %), а медіана 0,52 для вирівнювання блоками 4×4 і приховування піддерев рівнів 3 і 4 приховує найгірший випадок 0,81. Для 256 тайлів пакет дерева менший за підписаний список усіх гешів на 7894–8194 байти, а за список гешів лише прихованих тайлів тоді, коли на вузол покриття припадає в середньому понад приблизно 1,2 прихованого тайла, зокрема для всіх досліджених прямокутників шириною від трьох тайлів; для ізольованих тайлів він більший на 4–7 байтів на тайл. Усі 1589 екземплярів 26 класів валідаційних тестів дали передбачений результат; швидкодія не вимірювалася, перевірку на реальних знімках віднесено до подальших досліджень.

Ключові слова: цілісність даних; походження даних; дерево Меркля; підписи з можливістю редагування; селективне розкриття; знеособлення; БПЛА; аерознімки; геоінформаційні системи; C2PA.

ВСТУП

Постановка проблеми. Аерознімки з безпілотних літальних апаратів (БПЛА) використовують, зокрема, для оцінювання пошкоджень споруд [1]. Знімок, який документує руйнування цивільної інфраструктури, має лишатися перевірним будь-якою стороною, зокрема такою, що не довіряє ні знімальній організації, ні редакторів, а перед оприлюдненням із нього потрібно вилучити ділянки, розголошення яких створює ризики для людей чи об'єктів або розкриває персональні дані; настанови з



відкритих розслідувань [2] рекомендують оцінювати такі ризики заздалегідь. За монолітного підпису файлу ці вимоги несумісні: будь-яка зміна пікселів руйнує підпис, а повторне підписування відредагованої версії не доводить, що видимі пікселі походять з оригіналу.

Аналіз останніх досліджень і публікацій. Стандарти походження медіа охоплюють задачу лише частково. C2PA версії 2.4 [3] дозволяє вилучати твердження маніфесту, описувати просторові області та дії редагування в метаданих походження і застосовує дерева гешів до поблочного гешування BMFF-медіа, але, у нашому прочитанні, не визначає потайлового розкриття растра з перевіркою незмінених пікселів проти зобов'язання над оригіналом. ISO/IEC 23264-1 [4] визначає процеси, сторони та властивості безпеки редагування автентичних даних, а ISO/IEC 23264-2 [5] задає схеми підписів із можливістю редагування (redactable signatures) з перетворенням редагування за ключем редагування; у пропонованій схемі для редагування не потрібен ключ, пов'язаний із підписом або виданий підписувачем (секрет редагування, яким редактор керує випадковими політиками розширення, є лише його власним джерелом випадковості), а відповідність конкретному механізму стандарту не перевірялася.

Криптографічне ядро методу відоме: Johnson та ін. [6] запропонували підписи з можливістю редагування на дереві гешів Меркля [7] і дереві псевдовипадкових значень GGM [8], де власник підпису вилучає частини повідомлення без участі підписувача, а положення вилучених частин не приховується; Haber та ін. [9] мінімізували розмір підпису найменшим набором коренів піддерев; підписи з вилученням вмісту формалізовано в [10]; для деревоподібних даних приватність і прозорість підписів із можливістю редагування формалізовано в [11], витік структури усунуто в [12], довжину повідомлення і положення вилучень приховано в [13], а схему на дереві Меркля запропоновано в [14]. Для зображень Johnson, Walsh і Lamb [15] застосували дерева Меркля і GGM до фотографій зі стійкістю до обрізання та масштабування і відзначили, що порядок Мортон дає компактніший допоміжний матеріал, ніж рядковий. Жодна з цих робіт не розглядає георозмічений растр, у якому прихована ділянка лежить усередині кадру, а її положення є предметом захисту.

Другий напрям використовує доведення з нульовим розголошенням: PhotoProof [16] засвідчує дозволені перетворення зображення; у схемі Ко та ін. [17] вирізані ділянки обнуляються, тож їх розташування видиме, а автори відзначали компроміс між розміром блока і точністю вирізання; ZK-Disclosure [18] публікує проксі-зображення без візуального вмісту, а приховування окремих областей відкладає; Awan і Collomosse [19] приховують чутливі твердження маніфесту C2PA; VerITAS [20] і Trust Nobody [21] знижують вартість доведення і звітують час доведення, пам'ять і розмір доказу, а Trust Nobody описує й тайловий варіант із деревом Меркля. Ці роботи не оцінюють залишковий витік положення прихованої ділянки і площу, приховану понад запитане, а доведення потребують значних обчислень, тоді як криптографічне ядро гешової схеми обмежується гешуванням тайлів і одним підписом.

Політики розширення прихованої області та модель супротивника мають відповідники у приватності місцезнаходження: просторове маскування [22] збільшує область запиту до квадранта дерева квадрантів, а обізнаний супротивник інвертує це правило, що формалізовано разом із взаємністю маскування в [23]; фіктивні положення запропоновано в [24], а атаку перетином послідовних масок і захист запам'ятовуванням попереднього вибору описано в [25]. Розмір множини сумісних положень не враховує нерівних імовірностей кандидатів, а його логарифм є лише верхньою оцінкою залишкової невизначеності; для одного вгадування точнішою є мінімальна ентропія [26].

У проаналізованій літературі (станом на жовтень 2026 р.) не виявлено кількісного дослідження, яке для тайлового георозміченого растра одночасно оцінює витік положення запитаної області, частку надлишково прихованої площі та розмір пакета автентифікації. Внесок роботи полягає у просторовій семантиці відомої конструкції, політиках розширення, перенесених із приватності місцезнаходження на маски редагування, та кількісній оцінці компромісу між трьома названими величинами.

Мета статті. Метою статті є розробити та експериментально оцінити метод селективного розкриття фрагментів георозмічених аерознімків, за якого первинний підпис лишається перевіримим для відредагованої версії разом із доказом, і відповісти на три дослідницькі питання: як порядок лінеаризації тайлів впливає на розмір доказу (RQ1); який компроміс між витоком положення запитаної області, надлишково прихованою площею і розміром пакета дають політики розширення (RQ2); як розмір пакета співвідноситься з контрольними схемами (RQ3).

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Схема підписання, редагування та перевірки

Будову методу показано на рис. 1. Зображення розбивають сіткою на N тайлів, де N є степенем двійки (за потреби з доповненням нулями); канонічним поданням тайла є масив його відліків без стиснення, тому перевірність зберігається після перекодування контейнера без зміни відліків і полів

заголовка та руйнується після стиснення з втратами. Позицію тайла серед листків дерева задає порядок лінеаризації: рядковий або порядок Мортон, який переплітає біти координат.

Дерево будують за конструкцією Меркля з розділенням доменів, як у підписах із можливістю редагування [6], [9], [15]: листок, внутрішній вузол і аргумент підпису гешуються з різними одnobайтовими тегами:

$$L_i = H(0x01 \parallel i \parallel \text{geo}_i \parallel r_i \parallel T_i), \quad (1)$$

$$P = H(0x02 \parallel C_1 \parallel C_2), \quad S = \text{Sign}(H(0x03 \parallel \text{Hdr} \parallel R)). \quad (2)$$

Тут i є індексом тайла, geo_i його геометрією у режимі потайлової геоприв'язки, r_i сіллю, T_i вмістом, P значенням внутрішнього вузла з дочірніми вузлами C_1 і C_2 , R коренем дерева, а Hdr канонічним заголовком із фіксованим порядком серіалізації (додаток В), який містить версію схеми (вона фіксує алгоритм підпису Ed25519 за RFC 8032), параметри растра, сітки, геш-функції, порядку лінеаризації та режимів солі й геоприв'язки, специфікацію маски, 16-байтову прив'язку маніфесту, систему координат, афінне геоперетворення, час знімання та ідентифікатор пристрою. Солі виводяться функцією HKDF [27] з кореневого секрету солей і прив'язки маніфесту, тому сіль, розкрита в одному знімку, нічого не каже про інший; режими солі: без солі (S0), окрема сіль на тайл (S1), ієрархічна деривація за деревом GGM (S2); виміряно S0 і S1.

Редагування замінює вміст прихованих тайлів сталою маскою із заголовка і публікує пакет доказу, який замість значень листків прихованих тайлів містить мінімальне покриття прихованої області піддеревами: вузол входить до покриття, якщо всі його листки приховані, а серед листків батьківського вузла є видимий (за повного приховування покриттям є корінь); кількість вузлів покриття n_{subtrees} тим менша, чим повніші піддерева утворюють приховані тайли в порядку лінеаризації. Пакет містить також маніфест (заголовок, корінь, підпис), кодування прихованої множини та солі видимих тайлів (у режимі S1 по 20 байтів) і кодується детермінованим CBOR за базовими вимогами розд. 4.2.1 [28]; його розмір σ_{package} у байтах без растра є основною мірою накладних витрат. Відредаговану версію можна редагувати повторно без оригіналу, закритого ключа і кореневого секрету солей, причому прихована множина лише зростає. Перевірка відновлює корінь із видимих тайлів, їхніх солей і покриття, звіряє його з підписом і обов'язково перевіряє, що приховані тайли містять саме маску, інакше їх вміст можна було б підмінити без зміни кореня.

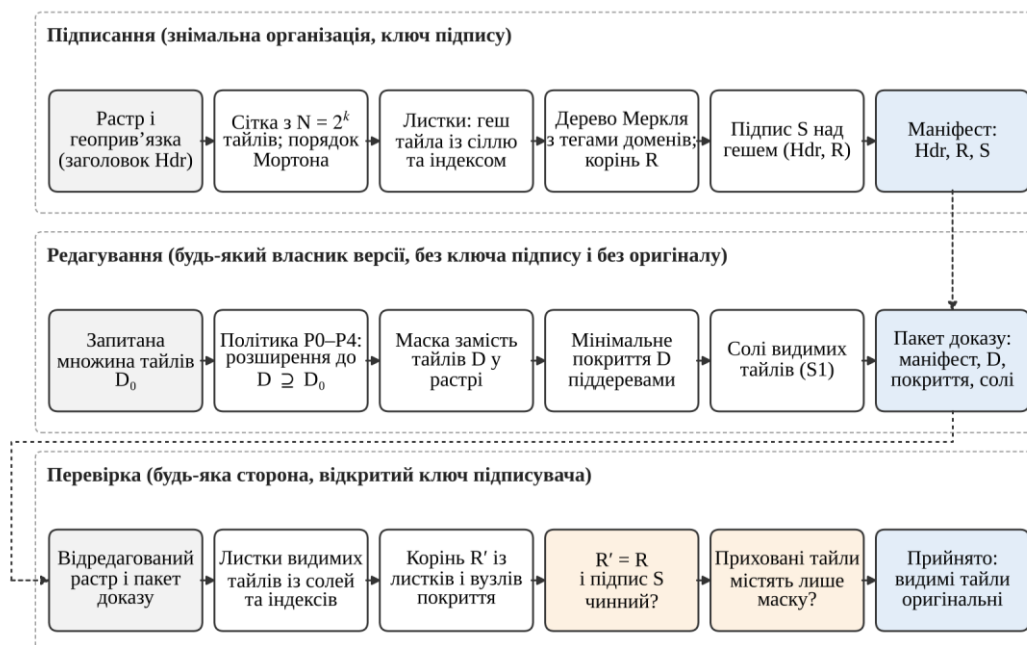


Рис. 1. Схема методу: підписання тайлового растра, редагування з розширенням прихованої множини та перевірка відредагованої версії за первинним підписом; штрихові стрілки позначають передавання маніфесту і пакета доказу між сторонами

**Політики розширення, супротивник і міри витоку**

Запитана множина прихованих тайлів D_0 може розширюватися до фактично прихованої $D \supseteq D_0$, щоб ускладнити визначення положення D_0 . Досліджено п'ять політик: без розширення (P0); вирівнювання до блоків $b \times b$ сітки, що перетинаються з D_0 (P1); додавання m фіктивних областей, конгруентних D_0 і відокремлених від неї та одна від одної щонайменше одним тайлом по горизонталі чи вертикалі, дотик по діагоналі допускається (P2); нарощування окол до кількості тайлів, кратної q (P3); приховування повних піддерев рівня l , що перетинаються з D_0 (P4). Випадкові рішення P2 і P3 визначає потік ChaCha20 у варіанті RFC 8439 (96-бітний попсе і 32-бітний лічильник блоків) з ключем, виведеним із секрету редагування і прив'язки маніфесту; повні правила наведено в додатку В. Лише P4 залежить від порядку лінеаризації: за порядку Мортон рівні $l = 2$ і 4 збігаються з блоками P1 при $b = 2$ і 4 , а рівні $l = 3$ і 5 дають вирівняні прямокутники 4×2 і 8×4 .

Супротивник знає метод, перелік політик і домени їхніх параметрів, опублікований пакет і відредаговане зображення, отже і множину D , але не знає D_0 та джерела випадковості; основна модель M2 додатково вважає відомими застосовану політику і параметр, довідкова M0 їх не знає. Форма області вважається відомою: сімейство кандидатів C_{shape} складається з усіх перенесень форми D_0 у межах сітки, а кількість кандидатів n_{cand} дорівнює числу положень, сумісних із опублікованою D за прийнятою моделлю, і обчислюється інверсією правила політики.

Вітік положення вимірюється в логарифмічній шкалі:

$$I_{\text{norm}} = 1 - \frac{\log_2 n_{\text{cand}}}{\log_2 |C_{\text{shape}}|}, \quad \lambda = \frac{|D \setminus D_0|}{N}. \quad (3)$$

Значення $I_{\text{norm}} = 0$ означає, що D сумісна з усіма положеннями, а $I_{\text{norm}} = 1$, що положення визначене однозначно; λ є часткою тайлів, прихованих понад запитане. Міра спирається на носій множини кандидатів (support), а не на ймовірності його елементів: для детермінованих політик за рівномірного апріорного розподілу всі сумісні положення рівноймовірні і міра точна; для випадкових P2 і P3 правдоподібність положень неоднакова, тому за рівномірного апріорного розподілу $\log_2 n_{\text{cand}}$ є верхньою оцінкою залишкової невизначеності, а I_{norm} нижньою оцінкою витоку [26]; для моделі M0 носій об'єднує кандидатів усіх політик без апріорних ваг і міра є лише структурною. Для одиночного запитаного тайла за P1, P3 і P4 усі приховані тайли є кандидатами, тому $I_{\text{norm}} = 1 - \log_2 |D| / \log_2 N$ і та сама політика дає різні значення на різних сітках (піддерево з 32 тайлів: 0,17 на сітці 8×8 і 0,58 на сітці 64×64).

Гарантії та їх межі

Якщо геш-функція стійка до колізій і другого прообразу, підпис стійкий до підробки, а заголовок серіалізується однозначно, то будь-яка версія, що проходить перевірку для фіксованих заголовка, підпису і оголошеної прихованої множини, містить оригінальні відліки на всіх видимих тайлах і маску на всіх прихованих: інший видимий вміст за того самого кореня дає колізію або другий прообраз на шляху до кореня, а інший заголовок чи корінь за того самого підпису дає підробку підпису; доведення в моделі з іграми не наводиться. Гарантія не вимагає довіри до редактора і стосується масивів відліків у межах профілю канонізації (додаток В), а не їх відображення: палітру, прозорість, колірний профіль та орієнтацію профіль поточної версії не засвідчує. Конфіденційність вмісту прихованих тайлів є окремою властивістю: у режимі S1 вона спирається на приховувальну властивість солоного гешу за секретної 16-байтової солі, а в режимі S0 здогад перевіряється простим гешуванням, і для вузла рівня l потрібно вгадати одночасно всі $2^l - n_{\text{known}}$ невідомих вмістів піддерева (властивість H7), що є кількістю невідомих листків, а не бітів стійкості.

Схема не має прозорості в сенсі робіт [11], [13]: кількість і розташування прихованих тайлів видимі, приховується лише положення D_0 усередині D . Аналіз витоку передбачає, що редактор чесно виконує політику зі свіжим секретом редагування для кожної нової запитаної множини, а повторний запит на ту саму D_0 обслуговує тією самою версією або тим самим збереженим секретом (запам'ятовування попереднього вибору в сенсі [25]); доказ не засвідчує ані дотримання політики, ані санкціонованості редагування, і будь-який власник версії може приховати ще частину тайлів. Повторне редагування не відкликає вже розкритого: оприлюднені тайл, сіль або значення вузла слід вважати відомими назавжди, а оцінки H7 та I_{norm} стосуються одного опублікованого доказу. Кілька незалежних версій для тієї самої D_0 з різними фіктивними областями вразливі до атаки перетином: спільними для всіх версій лишаються лише D_0 і випадково збіжні фіктивні області, тому перетин може звузити носій аж до D_0 (кількість потрібних для цього версій тут не оцінювалася); детерміновані P1 і P4 за незмінних параметрів і маніфесту до неї стійкі, бо та сама D_0 завжди дає ту саму D , а в ланцюгу повторних редагувань версії вкладені, хоча це не виключає витоку через інші метадані або раніше розкриті тайли й солі. Підписаний заголовок є публічним: час знімання, ідентифікатор пристрою та геоприв'язка не приховуються і до оцінки витоку не входять; геоприв'язка захищена лише в обсязі полів заголовка, а інші метадані контейнера, зокрема теги TIFF, world-файли чи коефіцієнти RPC, не засвідчуються і мають вважатися недовіреними. Схема гарантує не



істинність геоприв'язки чи сцени, а лише їх незмінність після підписання; ланцюг зберігання поза криптографічним зобов'язанням і юридична допустимість матеріалу лежать поза нею.

МЕТОДИКА ДОСЛІДЖЕННЯ

Матеріали, реалізація та протокол

Вимірювання виконано на синтетичних триканальних растрах 128×128 пікселів по 8 біт на канал, згенерованих детерміновано з початкового значення 42, з глобальною геоприв'язкою; вибір допустимий для структурних і розмірних величин, які від значень пікселів не залежать (валідаційні тести реалізації залежать від поведінки кодеків). Прототип реалізовано мовою Python 3 з бібліотеками cryptography, numpy і Pillow (версію Pillow у знімку середовища не зафіксовано) і покрито 100 автоматизованими тестами; часові характеристики не вимірювалися. Ключ підпису, кореневий секрет солей, майстер-секрет, з якого функцією HKDF виведено чотири секрети редагування, і прив'язка маніфесту в прогоні є детермінованими тестовими значеннями; у застосуванні їх має породжувати криптографічно стійкий генератор.

Детерміновані величини отримано вичерпним перебором усіх унікальних розміщень форми в сітці, тому результат описує повну скінченну сукупність і довірчі інтервали не застосовуються; для випадкових політик вісь секретів зафіксована чотирма ідентифікаторами, а зведення виконується спершу всередині розміщення медіаною за секретами, потім за розміщеннями. Пороги, рівні параметрів і вирішальні правила гіпотез H1 і H5 зафіксовано до вимірювань у конфігураційному артефакті, геш SHA-256 якого записано в кожен рядок сирих даних; оракули валідаційних тестів і властивості H7 та H8 визначено кодом прототипу (геші файлів у додатку Г). Зовнішньої реєстрації артефакта з міткою часу не було, тому фіксація засвідчує сталість конфігурації під час прогону, а не момент її ухвалення; нумерація гіпотез успадкована від специфікації, у якій H2, H3 і H6 належать до пізніших хвиль.

Дослідницьким питанням відповідають такі гіпотези та експерименти. RQ1 перевіряє E1 (сітки $8 \times 8 \dots 64 \times 64$, прямокутники 2×3 , 3×3 , 3×4 і 4×5 , усі розміщення) з гіпотезою H1: для кожного зв'язного невіривняного прямокутника медіана відношення n_{subtrees} за рядковим порядком до n_{subtrees} за порядком Мортонна перевищує 1, а частка розміщень із відношенням понад 1 перевищує 0,60; вердикт: у загальному формулюванні не підтверджено. RQ2 перевіряє E5 (сітка 8×8 , режим S1, порядок Мортонна, політики P0–P4, одиночний тайл і прямокутник 2×3 , усі розміщення, для P2 і P3 чотири секрети) з гіпотезою H5 лише для пакета за фіктивних областей: $\Delta\sigma(1) > 0$ і $c(1) > c(2) > c(4) > c(8)$, де $\Delta\sigma(m)$ є медіанним приростом пакета за m областей відносно P0, а $c(m) = \Delta\sigma(m) / m$, тоді як для I_{norm} і λ оцінка описова; вердикт: підтверджено для одиночного тайла як властивість формату, для прямокутника незастосовна. RQ3 перевіряє E6 (сітка 16×16 , режими S0 і S1, приховані множини як префікси індексів тайлів, $|D| = 0 \dots 128$, схеми B1 і B3' аналітично) з питанням H8, чи існує в дослідженому діапазоні $|D|$ точка перетину розміру пакета дерева Меркля і підписаного списку гешів B3; відповідь: проти B3 перетину немає за побудовою, проти B3' дерево менше, коли на вузол покриття припадає в середньому понад приблизно 1,2 прихованого тайла. Перевірку реалізації виконує E4 (26 класів тестів з оракулом і описовий клас NT14-R) з гіпотезою H4, за якою кожен клас дає результат, передбачений оракулом, без неочікуваних прийнять і відмов, і властивістю H7, за якою в режимі S0 підтвердження вузла рівня 1 потребує всіх $2^1 - n_{\text{known}}$ невідомих вмістів; вердикт: H4 і H7 підтверджено.

Усюди використано SHA-256, порядок Мортонна як базовий, режими S0 і S1 та глобальну геоприв'язку, а в E1 і E5 запитана область не перевищує чверті сітки. Відхилення від специфікації: реалізацію виконано мовою Python замість Rust із провізornoю версією протоколу; в E5 запитана множина зафіксована на найменшому дозволеному розмірі, тому двійковий квадрат зі стороною 1 збігається з одиночним тайлом і різних геометрій дві; нездійсненні комірки P2 виключено для кожного розміщення окремо; первісне правило H5 не передбачало вердикту «незастосовна», тому після виявлення нездійсненності $m = 8$ для прямокутника його застосовано лише до одиночного тайла, а для прямокутника наведено описовий аналіз на спільних розміщеннях.

Схеми зважування M0 і M2, аналіз непомічаності для кожного розміщення окремо та орієнтаційний аналіз E1 є апостеріорними аналізами над незмінними сирими даними або детермінованими обчисленнями.

Основний прогін w1-1787603877 виконано із замороженим артефактом (SHA-256 58f0bde9...939c92) на macOS 26.6.2 (arm64, CPython 3.9.6, numpy 2.0.2, cryptography 50.0.0); той самий код і артефакт автори виконали також у Linux 6.8 (CPython 3.10.12, numpy 2.2.6, cryptography 50.0.0); прогін w1-1787600395), і за порівнянням авторів сирі вимірювання, таблиці та висновки збіглися побайтово, крім ідентифікатора прогону та позначок часу. Повні таблиці (додаток А), скрипти переобчислення (додаток Б), профіль формату й політик (додаток В), артефакти прогону (додаток Г) і додаткові рисунки (додаток Д) надаються за запитом разом із сирими даними і кодом (див. заяву про доступність даних і коду).



РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

RQ1. Порядок лінеаризації і розмір доказу

Для кожної форми й сітки від 8×8 до 64×64 перебрано всі розміщення чотирьох прямокутників (19 556) й обчислено n_{subtrees} за рядковим порядком і порядком Мортон; пошукові класи (одиначний тайл, двійкові квадрати зі сторонами 1, 2, 4 і 8, розсіяні тайли і кластери як перенесення одного зафіксованого шаблону) додають 34 131 розміщення (додаток А; у сирих даних по 59 127 записів для кожної з метрик n_{subtrees} і σ_{cover} на кожен порядок, бо квадрат зі стороною 1 повторює 5440 розміщень одиначного тайла). Форми задано як ширина $\times$ висота; молодший біт переплетення Мортон належить горизонтальній координаті. Для прямокутників 3×3 , 3×4 і 4×5 порядок Мортон дає менше вузлів у 100 % розміщень за медіани відношення 1,20, 1,33 і 1,25 (окремі відношення від 1,14 до 1,67); від сітки не залежать медіана, частка і множина значень, змінюються лише частоти окремих значень. Для прямокутника 2×3 медіана відношення дорівнює 1,5, але перевага є лише у 0,571, 0,533, 0,516 і 0,508 розміщень на сітках від 8×8 до 64×64 , нижче зафіксованого порога 0,60: за парної горизонтальної координати початку три пари тайлів шириною 2 зливаються у два вузли проти трьох, за непарної обидва порядки дають по шість листків, а частка парних координат прямує до 0,5, тому для ширини 2 критерій не виконується за побудовою. Отже, Н1 у загальному формулюванні не підтверджена. Сам ефект відзначено ще в [15], де для підматриці $h \times w$ показано, що рядковий порядок у найгіршому випадку потребує $\Omega(h \log w)$ значень дерева GGM, а варіант порядку Мортон не більше $4(h + w)$ неперетинних вирівняних областей; тут його виміряно вичерпно за формами й орієнтаціями.

Результат залежить від орієнтації: для повернутого прямокутника 4×3 порядок Мортон кращий у 60–74 % розміщень і ніколи не гірший, для 5×4 кращий у 75–77 %, але гірший у 23–25 % з найменшим відношенням 0,89, а для квадратів 4×4 і 8×8 рядковий порядок кращий у 7–16 % (аналітичне обчислення для тих самих розміщень, додаток А). Порядок Гільберта [29] у стандартному ітеративному варіанті з обертанням квадрантів (орієнтація першого кроку залежить від парності $\log_2$ сторони сітки: вертикальна для 8×8 і 32×32 , горизонтальна для 16×16 і 64×64 ; додаток Б) відносно рядкового порядку кращий у 50–85 % розміщень, але для повернутих форм 3×2 , 4×3 і 5×4 гірший у 24–34 %; відносно порядку Мортон за окремими розміщеннями він кращий у 21–45 % і гірший у 23–46 %, а на сітках 32×32 і 64×64 його медіана покриття для жодної з форм не менша, ніж у порядку Мортон; це не суперечить кластеризації кривої Гільберта [29], де критерієм є кількість неперервних відрізків кривої, а не вирівняних двійкових піддерев. Отже, висновок про 100 % стосується зазначених орієнтацій і перевірених форм, а не довільних геометрій. Для зазначених орієнтацій серіалізоване покриття σ_{cover} (записи вузлів по 37–39 байтів для сіток до 64×64) змінює рішення лише для ширини 2: частка розміщень 2×3 із більшим σ_{cover} за рядкового порядку становить 0,667, 0,571, 0,613 і 0,538.

Перевірка реалізації

Експеримент Е4 виконує на сітках 16×16 (класи NT13 і NT19 на 8×8) 26 класів валідаційних тестів з оракулом, зафіксованим у коді (1589 екземплярів: 814 з очікуваною відмовою, 171 з очікуваним прийняттям, 604 структурні перевірки), і описовий клас NT14-R без оракула (20 екземплярів). Усі 1589 екземплярів дали передбачений результат: H4_W1 підтверджена на 24 класах першої хвилі (1486 екземплярів), повна H4 на 26 класах (перелік у додатку А). Клас NT14-R показав, що два редагування одного маніфесту за тієї самої політики P2 мають у середньому частку спільних фіктивних областей 0,263, бо послідовність кандидатів визначає пара «секрет, прив'язка маніфесту»; звідси вимога свіжого секрету для кожної нової запитаної множини. Клас NT21 підтвердив залежність P4 від порядку лінеаризації (різні множини у 74 з 80 пар), а властивість H7 перевірено на сітці 16×16 : у режимі S0 для одиначного прихованого тайла підтвердився лише істинний з чотирьох здогадів, у режимі S1 той самий здогад без солі не підтвердився, а для вузла рівня 4 підтвердження вдалося лише за всіх 16 відомих вмістів і не вдалося за жодного з 16 варіантів з одним заміненим. Генератор, верифікатор, канонізатор і оракули належать одному прототипу, тому Е4 перевіряє одну реалізацію, а не відповідність незалежній специфікації; внутрішня перевірка також показала, що прототип не відхиляє палітрові зображення (два PNG з однаковими індексами і різними палітрами проходять перевірку з тим самим доказом, бо засвідчуються індекси, а не кольори).

RQ2. Компроміс політик розширення

Для кожної політики, параметра та геометрії на сітці 8×8 (режим S1, порядок Мортон) перебрано всі розміщення, для P2 і P3 з чотирма секретами кожне: 6600 пакетних спостережень (по 21 рядку сирих даних на кожне), з яких 4040 різних, бо одиначний тайл записано також як двійковий квадрат зі стороною 1; разом 31 конфігурація (16 для одиначного тайла, 15 для прямокутника 2×3). Для прямокутника в табл. 1 зведено 34 спільні розміщення, на яких здійсненні всі порівнювані конфігурації (P2 з $m = 4$ нездійсненна для 8 центральних розміщень, з $m = 8$ для всіх 42); значення для P2 і P3 описують чотири зафіксовані



секрети редагування, а не розподіл випадкової політики.

Розмір пакета в режимі S1 визначають передусім солі видимих тайлів: без політики пакет для одиночного тайла займає 1570 байтів, з яких 1269 (81 %) припадає на 63 солі (по 20 байтів і 9 службових), а решта (маніфест 251 байт, кодування прихованої множини, покриття, обгортка) становить 301 байт (304 для P1 і P4); для прямокутника частка солей становить від 42 % (P2 з $m = 4$) до 77 %, крім повного приховування. Тому для вирівнювання і приховування підтерів скорочення солей переважає витрати покриття і пакет зменшується аж до 311 байтів при прихованні всієї сітки, тоді як для одиночного тайла з фіктивними областями зростає (з 1570 до 1714 байтів за $m = 8$), і вісь σ_{package} здебільшого повторює вісь λ . Фіктивна область для одиночного тайла додає запис покриття і вилучає сіль, тому $\Delta\sigma(m) \approx 17,5 \cdot m + 4$ байти, амортизована вартість 21,50, 19,50, 18,50 і 18,06 байта спадає здебільшого через одноразовий приріст кодування прихованої множини, і H5 підтверджена для одиночного тайла як властивість формату. Для прямокутника 2×3 фіктивна область вилучає шість солей (120 байтів) за покриття з 2 або 6 вузлів залежно від парності її горизонтальної координати, тому приріст від однієї області дорівнює -46 або -45 байтів у 98 із 168 спостережень і додатний у решті; медіани на 34 спільних розміщеннях становлять 28,75, $-14,5$ і 42,75 байта для $m = 1, 2, 4$, і H5 для прямокутника не застосовна.

Таблиця 1

Компроміс політик розширення на сітці 8×8 (E5; N = 64; режим S1; порядок Мортон)

Політика, параметр	Одиночний тайл, $ D_0 = 1, C_{\text{shape}} = 64$					Прямокутник 2×3 , $ D_0 = 6, C_{\text{shape}} = 42$				
	$ D $	σ_{package} , Б	λ	I_{norm}	межа	$ D $	σ_{package} , Б	λ	I_{norm}	межа
P0	1	1570 [1569–1570]	0,000	1,00	• 1,00	6	1511 [1510–1664]	0,000	1,00	• 1,00
P1, b = 2	4	1513	0,047	0,67	• 1,00	8 [8–16]	1470 [1273–1470]	0,031	0,81	• 0,76
P1, b = 4	16	1273	0,234	0,33	• 1,00	16 [16–64]	1273 [311–1273]	0,156	0,52 (0,81)	• 0,82
P1, b = 8	64	311	0,984	0,00	• 1,00	64	311	0,906	0,00	• 1,00
P2, m = 1	2	1591,5 [1590,5–1591,5]	0,016	0,83	0,36	12	1613,5 [1464–1766]	0,094	0,81	0,65
P2, m = 2	3	1609 [1608–1609,5]	0,031	0,74	• 1,00	18	1571,25 [1419–1724,5]	0,188	0,71	0,15
P2, m = 4	5	1644 [1643–1645]	0,062	0,61	• 1,00	30	1629,25 [1477–1707]	0,375	0,57	0,18
P2, m = 8	9	1714 [1712,5–1716,5]	0,125	0,47	• 1,00	нездійснення для всіх 42 розміщень				
P3, q = 2	2	1590 [1571,5–1592]	0,016	0,83	• 0,67	6	1511 [1510–1664]	0,000	1,00	• 1,00
P3, q = 4	4	1589,25 [1513–1609]	0,047	0,67	0,02	8	1546,5 [1508–1698,5]	0,031	1,00	0,26
P3, q = 8	8	1585,5 [1544–1642]	0,109	0,50	0,00	8	1546,5 [1508–1698,5]	0,031	1,00	0,26
P3, q = 16	16	1581,25 [1500,5–1653]	0,234	0,33	0,00	16	1582 [1459,5–1666]	0,156	0,79 (1,00)	0,12
P4, l = 2	4	1513	0,047	0,67	• 1,00	8 [8–16]	1470 [1273–1470]	0,031	0,81	• 0,76
P4, l = 3	8	1433	0,109	0,50	• 1,00	16 [16–32]	1273 [953–1310]	0,156	0,52 (0,81)	• 0,88
P4, l = 4	16	1273	0,234	0,33	• 1,00	16 [16–64]	1273 [311–1273]	0,156	0,52 (0,81)	• 0,82
P4, l = 5	32	953	0,484	0,17	• 1,00	32 [32–64]	953 [311–953]	0,406	0,29	• 0,82

Примітка. Медіани за розміщеннями, для P2 і P3 після медіани за чотирма секретами; у дужках діапазон за розміщеннями для $|D|$ і σ_{package} та найгірше значення для I_{norm} (за всіма розміщеннями, для P2 і P3 за всіма окремими реалізаціями секрету), якщо воно відрізняється від медіани; одиночний тайл на всіх 64 розміщеннях, прямокутник 2×3 на 34 спільних розміщеннях, здійснених для всіх порівнюваних



конфігурацій; • точка межі Парето агрегованих медіан за $(I_{\text{norm}}, \sigma_{\text{package}}, \lambda)$, число є часткою розміщень, у яких конфігурація не домінована.

Витік положення для одиночного тайла знижується від 1,0 без політики до 0,17 при прихованні піддерева рівня 5 ($\lambda = 0,48$) і до 0,47 за восьми фіктивних областей ($\lambda = 0,125$). Для прямокутника 2×3 квантування кількості тайлів (P_3) за $q \leq 8$ положення здебільшого не приховує: за $q = 2$ не приховує зовсім, бо 6 кратне 2, а за $q = 4$ і 8 прихована множина з 8 тайлів сумісна лише з одним розміщенням у 115 із 136 спостережень (34 спільні розміщення $\times 4$ секрети); за $q = 16$ медіана I_{norm} знижується до 0,79, але у 26 із 136 спостережень положення однозначне, а найбільший носій має шість кандидатів; на всіх 42 розміщеннях (168 пар) частки однозначного положення становлять 100 %, 83 % і 17 % за того самого найбільшого носія (додаток А). P_2 дає рівно $m + 1$ кандидатів, а P_4 рівня 5 знижує I_{norm} до 0,29. Медіана приховує найгірший випадок: для прямокутника P_1 з $b = 4$ і P_4 з $l = 3$ або 4 мають медіану 0,52, але 0,81 у розміщеннях, де область перетинає межу блоків, а для P_3 найгірша реалізація дорівнює 1,00 за всіх q (табл. 1, у дужках). Моделі знань M_0 і M_2 дають однакові медіани в усіх 31 конфігураціях і розходяться лише для прямокутника за P_1 і P_4 у 66 із 294 комірок цих політик (22,4 %; 4,0 % від 1646 унікальних комірок матриці) з найбільшою різницею 4,39 біта.

Межа Парето за $(I_{\text{norm}}, \sigma_{\text{package}}, \lambda)$ на медіанах конфігурацій для одиночного тайла містить P_0 , P_3 з $q = 2$, P_2 з $m = 2, 4, 8$, P_1 з $b = 2, 4, 8$ та P_4 з $l = 3$ і 5, а для прямокутника лише P_0 (з якою збігається P_3 з $q = 2$), P_1 з $b = 2, 4, 8$ та P_4 з $l = 3$ і 5 (P_4 з $l = 2$ і 4 збігаються з P_1 з $b = 2$ і 4); домінованість P_2 з $m = 1$ для одиночного тайла визначає різниця в 1,5 байта з P_3 при $q = 2$, порівняння з коливанням довжини запису, тому вона не змістовна. Перевірка не домінованості для кожного розміщення окремо (частки в табл. 1) узгоджується з агрегованою межею для одиночного тайла, але не для прямокутника: P_2 з $m = 1$ не домінована у 65 % розміщень, а за окремими реалізаціями секрету в усіх 34, бо одна фіктивна область там частіше зменшує пакет, ніж збільшує. Отже, твердження про перевагу однієї політики над іншою справедливі лише для одиночного тайла: там за порівнянного витоку вирівнювання і приховування піддерев дають менший пакет, ніж фіктивні області, а квантування з $q = 4, 8$ і 16 збігається за витоком і площею з вирівнюванням або приховуванням піддерев того самого розміру ($b = 2, l = 3, b = 4$) і відрізняється лише більшим пакетом. Значення для P_2 і P_3 стосуються однієї оприлюдненої версії для кожної D_0 і є структурними оцінками, умовними щодо реалізованої в прототипі процедури інверсії; ймовірний витік для них не оцінювався.

RQ3. Порівняння з контрольними схемами

Контрольна схема B_3 підписує вектор значень усіх N листків і публікує його цілком, як підписані списки солоних гешів на кшталт SD-JWT [30]; вона повторює формулу листка, режим солі, канонізацію і обгортку маніфесту і відрізняється лише складовою агрегації. Оскільки верифікатор може обчислити значення видимих листків сам, додатково розглянуто сильніший варіант B_3' , який публікує лише геші прихованих тайлів (аналітично, з тих самих складових). B_3 є контрольною схемою лише для розміру пакета, а не еквівалентом за приватністю, бо поелементні зобов'язання і покриття піддеревами мають різну гранулярність, що впливає на підтвердження здогаду, особливо в режимі S_0 . Схема з підписом на кожен тайл (B_1) оцінена аналітично як маніфест і N пар «підпис, геш», тобто $251 + 96 \cdot N$ байтів (24 827 байтів для $N = 256$). Вимірювання на сітці 16×16 для прихованих множин, які є префіксами індексів тайлів у рядковій нумерації, зведено в табл. 2.

Таблиця 2

Розмір пакета дерева Меркля проти контрольних схем (Е6; сітка 16×16 , $N = 256$, порядок Мортон; приховані множини є префіксами індексів тайлів у рядковій нумерації; B_3 публікує геші всіх 256 листків (8195 Б), B_3' лише геші прихованих тайлів (аналітично); $\Delta\sigma = \sigma(\text{контрольна}) - \sigma(\text{Меркля})$ однакова в обох режимах солі)

D	n_{subtrees}	Покриття, Б	Геші B_3' , Б	$\sigma(\text{Меркля}), S_0$, Б	$\sigma(\text{Меркля}), S_1$, Б	$\Delta\sigma(B_3)$, Б	$\Delta\sigma(B_3')$, Б
0	0	1	1	262	5 388	8 194	0
1	1	38	34	303	5 409	8 157	-4
2	1	38	66	307	5 393	8 157	28
4	2	75	130	344	5 390	8 120	55
8	4	149	259	418	5 384	8 046	110
16	8	301	515	570	5 376	7 894	214
32	4	149	1 027	418	4 904	8 046	878
64	2	75	2 051	344	4 190	8 120	1 976
128	1	38	4 099	307	2 873	8 157	4 061



Покриття дерева займає від 1 до 301 байта, а вектор В3 завжди 8195 байтів, тому дерево дає менший пакет для всіх дев'яти значень $|D|$ в обох режимах солі: різниця становить від 7894 до 8194 байтів, найменша при $|D| = 16$, коли префікс у порядку Мортон розпадається на вісім пар. Точки перетину з В3 немає за побудовою: вузол покриття рівня 0 має видимий сусідній листок, а вузол вищого рівня покриває щонайменше два приховані листки, тому вузлів покриття не більше $N / 2$, а оскільки запис вузла в досліджуваному форматі не довший за 41 байт (додаток В), покриття не перевищує $41 \cdot N / 2$ байтів плюс заголовок масиву проти $32 \cdot N$ байтів вектора. Проти В3' запис вузла на 5–7 байтів довший за геш, тому для префіксів вигода дерева з'являється від $|D| = 2$, а для розсіяних множин, у яких кожен прихований тайл утворює окремий вузол, В3' завжди менший (4099 проти 4854 байтів для 128 тайлів); точна умова порівнює заголовок масиву і суму довжин записів покриття з довжиною рядка з $32 \cdot |D|$ байтів, а наближено дерево виграє, коли $n_{\text{subtrees}} \cdot (32 + \delta) < 32 \cdot |D|$, де δ є накладними байтами запису вузла, тобто коли на вузол покриття припадає в середньому понад $(32 + \delta) / 32 \approx 1,2$ прихованого тайла; за перебором усіх розміщень на сітках від 8×8 до 64×64 (додаток А) це виконується в усіх розміщеннях досліджених прямокутників шириною від трьох тайлів (медіанний виграш від 76 байтів для 3×2 до 1427 для 8×8), для ширини 2 лише за парної горизонтальної координати (51–57 % розміщень), а для одиночного тайла і вертикальної пари ніколи (програш 4–13 байтів). Це і є відповіддю на Н8. У режимі S0 пакет дерева (262–570 байтів) перевищує пакет монолітного підпису В0 (252 байти) не більш як у 2,3 раза; у режимі S1 домінує розкриття солей (95 % пакета за $|D| = 0$), тому пакет здебільшого зменшується зі зростанням $|D|$, хоча не монотонно (5388 байтів за $|D| = 0$ і 5409 за $|D| = 1$). Розкриття солей у режимі S1 зростає лінійно з кількістю видимих тайлів (20 байтів на тайл, близько 82 кілобайт для сітки 64×64); у режимі S2 замість солей розкриваються насінини піддерев GGM за кількістю вузлів мінімального покриття видимої множини, а запис насінини за форматом вузла покриття займає 37 байтів за малих індексів: для одиночного прихованого тайла на сітці 8×8 це 6 насінин (приблизно 222–224 байти записів без обгортки) замість 63 солей, тоді як за чергування видимих і прихованих тайлів кожен видимий тайл потребує окремої насінини, дорожчої за сіль. Отже, S2 вигідніший тоді, коли видима множина стискається в небагато піддерев; його повна оцінка лишається перспективною.

Обговорення, обмеження і загрози валідності

Внутрішню валідність обмежує випадковість P2 і P3: чотири секрети дають грубу дискретність медіани і не описують хвостів розподілу, а інверсію для них звірено з прямим перебором лише односторонньо, за однієї реалізації випадковості (для детермінованих політик перевірено рівність); контрприкладу неправильного n_{cand} не знайдено, але повної валідації носія не виконано, і значення слід вважати умовними. Найсуттєвіша загроза зовнішній валідності: задача сформульована для аерознімків з БПЛА, а всі вимірювання виконано на синтетичних растрах і малих сітках (компроміс політик на сітці 8×8 для двох геометрій, порівняння з контрольними схемами на сітці 16×16 для однієї сім'ї множин); реальний георозмічений файл наскрізно не оброблявся. Профіль канонізації охоплює лише беззнакові цілі відліки 8 і 16 біт у режимі декодера; семантика каналів, орієнтація та палітра не засвідчуються, тому палітрові режими слід відхиляти або канонізувати до RGB, чого прототип не робить, а відліки з плаваючою комою, NoData і канонічна форма системи координат лишаються поза профілем; режим S2, незв'язні геометрії, інші геш-функції, потайлова геоприв'язка та часові вимірювання лишаються поза межами статті. Щодо конструктивної валідності: λ зважає тайли за кількістю, а не за інформативністю; I_{norm} є нижньою оцінкою витоку, а $\log_2 n_{\text{cand}}$ верхньою оцінкою невизначеності для відомої форми області без зовнішньої інформації, тоді як контекст сцени, карти чи попередні знімки можуть звузити носій і збільшити витік, зокрема відкинути неправдоподібні фіктивні області; у режимі S1 вісь σ_{package} вимірює насамперед кількість видимих тайлів, і для S0 та S2 форма компромісу буде іншою. Щодо валідності висновку: вичерпно перебрані величини описують повну скінченну сукупність, залежні від секрету стосуються чотирьох зафіксованих секретів, а твердження про безпеку спираються на криптографічні припущення.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропоновано метод селективного розкриття та редагування чутливих фрагментів георозмічених аерознімків, який переносить відому конструкцію підпису з можливістю редагування на основі дерева Меркла [6], [9] на тайлований растр: геоприв'язка входить до підписаного заголовка, прихована область подається канонічним покриттям піддеревками, а первинний підпис лишається перевіримим для відредагованої версії разом із доказом без участі підписувача. Наукова новизна полягає в такому. По-перше, для тайлового растра визначено політики розширення запитаної області та модель витоку її положення за носієм з інверсією політик, яка переносить ідеї просторового маскування і фіктивних положень із приватності місцезнаходження на маски редагування. По-друге, компроміс між витоком, надлишковою прихованою площею і розміром пакета оцінено кількісно для чотирьох політик вичерпним



перебором розміщень: для одиночного тайла на сітці 8×8 структурний показник витоку за носієм знижується до 0,47 фіктивними областями за надлишку 12,5 % площі і до 0,17 приховуванням піддерев за надлишку 48 %, тоді як для прямокутника 2×3 квантування кількості тайлів за $q \leq 8$ положення здебільшого не приховує (воно однозначне у 83–100 % пар «розміщення–секрет» на всіх 42 розміщеннях, за $q = 16$ у 17 %), а фіктивні області на сітці 8×8 для прямокутника часто нездійсненні ($m = 4$ для 8 із 42 розміщень, $m = 8$ для всіх); медіана 0,52 для вирівнювання блоками 4×4 і приховування піддерев рівнів 3 і 4 приховує найгірший випадок 0,81; для випадкових політик P2 і P3 ці значення умовні щодо реалізованої процедури інверсії, а ймовірнісний витік не оцінювався. По-третє, кількісно уточнено структурні чинники розміру доказу: відомий ефект порядку Мортонна [15] для прямокутників 3×3 , 3×4 і 4×5 у зазначеній орієнтації зменшує покриття у 100 % розміщень за медіани відношення від 1,20 до 1,33, а для ширини 2, повернутих форм і квадратів перевага неповна; пакет дерева менший за пакет контрольної схеми з повним вектором гешів на 7894–8194 байти, а проти варіанта з гешами лише прихованих тайлів виграє тоді, коли на вузол покриття припадає в середньому понад приблизно 1,2 прихованого тайла, зокрема в усіх розміщеннях досліджених прямокутників шириною від трьох тайлів, і програє для ізольованих тайлів.

Практичне значення полягає в технічній основі для оприлюднення аерознімків із прихованими ділянками зі збереженням перевірності канонічних відліків видимих тайлів у заданому профілі і для передавання матеріалу ланцюгом організацій без ключа підпису; криптографічне ядро редагування і перевірки зводиться до гешування тайлів і одного підпису без доведень з нульовим розголошенням, хоча пошук фіктивних областей, канонізація і серіалізація додають обчислення, яких не вимірювали. Застосовність до реальних георозмічених файлів потребує окремої перевірки, оцінка витоку передбачає чесне виконання політики та одну оприлюднену версію для кожної запитаної області, а повторне редагування не відкликає вже оприлюднених тайлів. Подальша робота охоплює деривацію потоку політики з довгострокового секрету, прив'язки маніфесту, політики, параметра і канонічного кодування запитаної області, щоб повторний запит давав ту саму маску (запропонований, ще не реалізований механізм), профіль канонізації із закритим переліком режимів зображення, компактний формат пакета без надлишкових індексів, оцінку режиму S2, повну валідацію інверсії випадкових політик, інші форми й орієнтації та перевірку на реальному георозміченому знімку.

ДЕКЛАРАЦІЇ

Конфлікт інтересів. Автори заявляють про відсутність конфлікту інтересів.

Фінансування. Дослідження виконано без зовнішнього фінансування.

Доступність даних і коду. Додатки А–Д (повні таблиці, скрипти переобчислення і збирання, профіль формату, артефакти прогону, додаткові рисунки), сирі вимірювання прогону (375 243 рядки) і код прототипу з набором тестів надаються за обґрунтованим запитом до авторів.

Декларація про використання штучного інтелекту. Під час підготовки дослідження і рукопису автори використовували моделі сімейства Claude 5 (Anthropic), а саме `claude-opus-5-5` і `claude-fable-5-1`, у застосунку Claude та в інструменті Claude Code; моделі GPT 5.5 SOL і ChatGPT-6 Astra (OpenAI) у вебзастосунку ChatGPT. Мета й обсяг використання: (1) допомога в розробленні методу і написанні специфікації експерименту, а також написання коду прототипу (модулі схеми, набір тестів і скрипти прогону) в інструменті Claude Code; (2) написання скриптів агрегування сирих вимірювань прогону `w1-1787603877` для формування таблиць і рисунків, а також скриптів апостеріорних детермінованих обчислень (орієнтаційний аналіз E1 і порядок Гільберта, розклад розміру пакета, найгірший випадок витоку, контрольна схема B3' і порівняння з нею, частки однозначного положення для P3 на всіх розміщеннях); (3) редагування, повне переписування за авторським планом статті, скорочення та переформулювання тексту рукопису, зокрема анотацій і викладу висновків, виправлення мовних помилок і неточностей, побудова схеми методу (рис. 1), технічне оформлення та збирання файлу рукопису; (4) попереднє критичне оцінювання рукопису цими моделями у кількох раундах перед поданням; (5) допомога в перевірці бібліографічних записів за первинними джерелами. Інструменти штучного інтелекту не використовувалися для проведення вимірювань. Постановку задачі, остаточні рішення щодо конструкції методу і параметрів експерименту та наукові висновки сформульовано авторами; виклад висновків і решти тексту підготовлено за допомогою штучного інтелекту за авторським планом. Спосіб перевірки: код прототипу автори перевірили контрольними векторами з артефактів прогону, зокрема вектором RFC 8439 для ChaCha20, валідаційними тестами експерименту E4 з оракулом, зафіксованим у коді, і побайтовим відтворенням прогону на macOS і Linux; експериментальні результати звірили із сирими вимірюваннями прогону, результати апостеріорних детермінованих обчислень відтворили скриптами з пакета додатків, схему методу (рис. 1) звірили з описом методу в розділі теоретичних основ, бібліографічні відомості перевірили за DOI та сторінками видавців, а відповідність цитованих джерел твердженням рукопису



перевірили за змістом цих джерел; зауваження попереднього критичного оцінювання автори розглянули та прийняли або відхилили самостійно. Автори несуть повну відповідальність за зміст статті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yang, Z., Xu, Y., Song, H., & Yu, K. (2025). Data-driven structural damage monitoring and assessment based on unmanned aerial vehicle images: A survey. *International Journal of Digital Earth*, 18(1), 2528617. <https://doi.org/10.1080/17538947.2025.2528617>
2. Office of the High Commissioner for Human Rights, & Human Rights Center, UC Berkeley School of Law. (2022). *Berkeley Protocol on digital open source investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law* (HR/PUB/20/2). United Nations. ISBN 978-92-1-154233-2
3. Coalition for Content Provenance and Authenticity. (2026). *Content Credentials: C2PA technical specification* (Version 2.4). https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html
4. ISO/IEC. (2021). *Information security — Redaction of authentic data — Part 1: General* (ISO/IEC 23264-1:2021). <https://www.iso.org/standard/78341.html>
5. ISO/IEC. (2024). *Information security — Redaction of authentic data — Part 2: Redactable signature schemes based on asymmetric mechanisms* (ISO/IEC 23264-2:2024). <https://www.iso.org/standard/78342.html>
6. Johnson, R., Molnar, D., Song, D., & Wagner, D. (2002). Homomorphic signature schemes. In *Topics in Cryptology — CT-RSA 2002* (LNCS, Vol. 2271, pp. 244–262). Springer. https://doi.org/10.1007/3-540-45760-7_17
7. Merkle, R. C. (1988). A digital signature based on a conventional encryption function. In *Advances in Cryptology — CRYPTO '87* (LNCS, Vol. 293, pp. 369–378). Springer. https://doi.org/10.1007/3-540-48184-2_32
8. Goldreich, O., Goldwasser, S., & Micali, S. (1986). How to construct random functions. *Journal of the ACM*, 33(4), 792–807. <https://doi.org/10.1145/6490.6503>
9. Haber, S., Hatano, Y., Honda, Y., Horne, W., Miyazaki, K., Sander, T., Tezoku, S., & Yao, D. (2008). Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS '08)* (pp. 353–362). ACM. <https://doi.org/10.1145/1368310.1368362>
10. Steinfeld, R., Bull, L., & Zheng, Y. (2002). Content extraction signatures. In *Information Security and Cryptology — ICISC 2001* (LNCS, Vol. 2288, pp. 285–304). Springer. https://doi.org/10.1007/3-540-45861-1_22
11. Brzuska, C., Busch, H., Dagdelen, Ö., Fischlin, M., Franz, M., Katzenbeisser, S., Manulis, M., Onete, C., Peter, A., Poettering, B., & Schröder, D. (2010). Redactable signatures for tree-structured data: Definitions and constructions. In *Applied Cryptography and Network Security (ACNS 2010)* (LNCS, Vol. 6123, pp. 87–104). Springer. https://doi.org/10.1007/978-3-642-13708-2_6
12. Kundu, A., Atallah, M. J., & Bertino, E. (2012). Leakage-free redactable signatures. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy (CODASPY '12)* (pp. 307–316). ACM. <https://doi.org/10.1145/2133601.2133639>
13. Derler, D., Pöhls, H. C., Samelin, K., & Slamanig, D. (2016). A general framework for redactable signatures and new constructions. In *Information Security and Cryptology — ICISC 2015* (LNCS, Vol. 9558, pp. 3–19). Springer. https://doi.org/10.1007/978-3-319-30840-1_1
14. Hirose, S., & Kuwakado, H. (2013). Redactable signature scheme for tree-structured data based on Merkle tree. In *Proceedings of the 10th International Conference on Security and Cryptography (SECRYPT 2013)* (pp. 313–320). SciTePress. <https://doi.org/10.5220/0004507003130320>
15. Johnson, R., Walsh, L., & Lamb, M. (2012). Homomorphic signatures for digital photographs. In *Financial Cryptography and Data Security (FC 2011)* (LNCS, Vol. 7035, pp. 141–157). Springer. https://doi.org/10.1007/978-3-642-27576-0_12
16. Naveh, A., & Tromer, E. (2016). PhotoProof: Cryptographic image authentication for any set of permissible transformations. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 255–271). IEEE. <https://doi.org/10.1109/SP.2016.23>
17. Ko, H., Lee, I., Lee, S., Kim, J., & Oh, H. (2021). Efficient verifiable image redacting based on zk-SNARKs. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (ASIA CCS '21)* (pp. 213–226). ACM. <https://doi.org/10.1145/3433210.3453110>
18. Marinho, J., Schiller, E., Debaugé, A., & Foukia, N. (2025). ZK-Disclosure: Privacy-preserving



- information disclosure for digital evidence with C2PA and zk-SNARKs. In *2025 Annual Computer Security Applications Conference Workshops (ACSAC Workshops)* (pp. 309–315). IEEE. <https://doi.org/10.1109/ACSACW69556.2025.00040>
19. Awan, M., & Collomosse, J. (2026). *Soft redaction of image provenance via zero-knowledge proofs* (arXiv:2608.07063). arXiv. <https://arxiv.org/abs/2608.07063>
 20. Datta, T., Chen, B., & Boneh, D. (2025). VerITAS: Verifying image transformations at scale. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 4606–4623). IEEE. <https://doi.org/10.1109/SP61157.2025.00097>
 21. Della Monica, P., Visconti, I., Vitaletti, A., & Zecchini, M. (2025). Trust Nobody: Privacy-preserving proofs for edited photos with your laptop. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 4624–4642). IEEE. <https://doi.org/10.1109/SP61157.2025.00014>
 22. Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys 2003)* (pp. 31–42). ACM. <https://doi.org/10.1145/1066116.1189037>
 23. Kalnis, P., Ghinita, G., Mouratidis, K., & Papadias, D. (2007). Preventing location-based identity inference in anonymous spatial queries. *IEEE Transactions on Knowledge and Data Engineering*, 19(12), 1719–1733. <https://doi.org/10.1109/TKDE.2007.190662>
 24. Kido, H., Yanagisawa, Y., & Satoh, T. (2005). An anonymous communication technique using dummies for location-based services. In *Proceedings of the International Conference on Pervasive Services (ICPS '05)* (pp. 88–97). IEEE. <https://doi.org/10.1109/PERSER.2005.1506394>
 25. Chow, C.-Y., & Mokbel, M. F. (2007). Enabling private continuous queries for revealed user locations. In *Advances in Spatial and Temporal Databases (SSTD 2007)* (LNCS, Vol. 4605, pp. 258–275). Springer. https://doi.org/10.1007/978-3-540-73540-3_15
 26. Smith, G. (2009). On the foundations of quantitative information flow. In *Foundations of Software Science and Computational Structures (FoSSaCS 2009)* (LNCS, Vol. 5504, pp. 288–302). Springer. https://doi.org/10.1007/978-3-642-00596-1_21
 27. Krawczyk, H., & Eronen, P. (2010). *HMAC-based extract-and-expand key derivation function (HKDF)* (RFC 5869). IETF. <https://doi.org/10.17487/RFC5869>
 28. Bormann, C., & Hoffman, P. (2020). *Concise binary object representation (CBOR)* (RFC 8949). IETF. <https://doi.org/10.17487/RFC8949>
 29. Moon, B., Jagadish, H. V., Faloutsos, C., & Saltz, J. H. (2001). Analysis of the clustering properties of the Hilbert space-filling curve. *IEEE Transactions on Knowledge and Data Engineering*, 13(1), 124–141. <https://doi.org/10.1109/69.908985>
 30. Fett, D., Yasuda, K., & Campbell, B. (2025). *Selective disclosure for JSON Web Tokens* (RFC 9901). IETF. <https://doi.org/10.17487/RFC9901>

**Andrii Nyzhnyk**

Postgraduate student, Department of Information Protection

Lviv Polytechnic National University, Lviv, Ukraine

ORCID: 0009-0003-9094-0740

andrii.o.nyzhnyk@lpnu.ua

Denys Khanin

Postgraduate student, Department of Information Protection

Lviv Polytechnic National University, Lviv, Ukraine

ORCID: 0009-0001-4009-0202

denys.o.khanin@lpnu.ua

A METHOD FOR SELECTIVE DISCLOSURE AND REDACTION OF SENSITIVE REGIONS IN AERIAL IMAGERY WHILE PRESERVING SIGNATURE VERIFIABILITY

Abstract. UAV imagery documenting damage to civilian infrastructure must remain verifiable by any party, yet regions whose disclosure creates risks must be removed before publication; a monolithic file signature does not allow this, because any pixel change breaks it. The proposed method transfers the known Merkle-tree redactable-signature construction to a tiled georeferenced raster: the georeference is part of the signed header, the hidden region is represented by a minimal subtree cover, expansion policies deliberately enlarge the hidden set to make the position of the requested region harder to determine, and the original signature remains valid for the redacted version without the signer's involvement. Measurements used synthetic rasters and exhaustive enumeration of placements on grids from 8×8 to 64×64 tiles. For 3×3, 3×4 and 4×5 rectangles the Morton order yields fewer cover nodes than row-major order in 100 % of placements with a median ratio of 1.20–1.33; for width 2 and for rotated shapes the advantage is incomplete. For a single tile on an 8×8 grid the normalised structural leakage indicator over the set of compatible positions decreases from 1.0 to 0.17 with subtree hiding at 48 % excess area and to 0.47 with decoy regions at 12.5 % (for the randomised policies these values are conditional on the implemented inversion procedure; probabilistic leakage was not assessed). For a 2×3 rectangle, quantising the number of tiles with step $q \leq 8$ mostly does not hide the position (it is unique in 83–100 % of placement–secret pairs over all 42 placements, with $q = 16$ in 17 %), and the median of 0.52 for 4×4 block alignment and subtree hiding at levels 3 and 4 conceals a worst case of 0.81. For 256 tiles the tree package is smaller than a signed list of all hashes by 7894–8194 bytes, and smaller than a list of the hidden tiles' hashes only when a cover node holds on average more than about 1.2 hidden tiles, e.g. for all studied rectangles at least three tiles wide; for isolated tiles it is larger by 4–7 bytes per tile. All 1589 instances of 26 validation test classes gave the predicted result; throughput was not measured, and validation on real imagery is left for further research.

Keywords: data integrity; provenance; Merkle tree; redactable signatures; selective disclosure; anonymisation; UAV; aerial imagery; geographic information systems; C2PA.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Yang, Z., Xu, Y., Song, H., & Yu, K. (2025). Data-driven structural damage monitoring and assessment based on unmanned aerial vehicle images: A survey. *International Journal of Digital Earth*, 18(1), 2528617. <https://doi.org/10.1080/17538947.2025.2528617>
2. Office of the High Commissioner for Human Rights, & Human Rights Center, UC Berkeley School of Law. (2022). *Berkeley Protocol on digital open source investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law* (HR/PUB/20/2). United Nations. ISBN 978-92-1-154233-2
3. Coalition for Content Provenance and Authenticity. (2026). *Content Credentials: C2PA technical specification* (Version 2.4). https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html
4. ISO/IEC. (2021). *Information security — Redaction of authentic data — Part 1: General* (ISO/IEC 23264-1:2021). <https://www.iso.org/standard/78341.html>
5. ISO/IEC. (2024). *Information security — Redaction of authentic data — Part 2: Redactable signature*



- schemes based on asymmetric mechanisms (ISO/IEC 23264-2:2024). <https://www.iso.org/standard/78342.html>
6. Johnson, R., Molnar, D., Song, D., & Wagner, D. (2002). Homomorphic signature schemes. In *Topics in Cryptology — CT-RSA 2002* (LNCS, Vol. 2271, pp. 244–262). Springer. https://doi.org/10.1007/3-540-45760-7_17
 7. Merkle, R. C. (1988). A digital signature based on a conventional encryption function. In *Advances in Cryptology — CRYPTO '87* (LNCS, Vol. 293, pp. 369–378). Springer. https://doi.org/10.1007/3-540-48184-2_32
 8. Goldreich, O., Goldwasser, S., & Micali, S. (1986). How to construct random functions. *Journal of the ACM*, 33(4), 792–807. <https://doi.org/10.1145/6490.6503>
 9. Haber, S., Hatano, Y., Honda, Y., Horne, W., Miyazaki, K., Sander, T., Tezoku, S., & Yao, D. (2008). Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS '08)* (pp. 353–362). ACM. <https://doi.org/10.1145/1368310.1368362>
 10. Steinfeld, R., Bull, L., & Zheng, Y. (2002). Content extraction signatures. In *Information Security and Cryptology — ICISC 2001* (LNCS, Vol. 2288, pp. 285–304). Springer. https://doi.org/10.1007/3-540-45861-1_22
 11. Brzuska, C., Busch, H., Dagdelen, Ö., Fischlin, M., Franz, M., Katzenbeisser, S., Manulis, M., Onete, C., Peter, A., Poettering, B., & Schröder, D. (2010). Redactable signatures for tree-structured data: Definitions and constructions. In *Applied Cryptography and Network Security (ACNS 2010)* (LNCS, Vol. 6123, pp. 87–104). Springer. https://doi.org/10.1007/978-3-642-13708-2_6
 12. Kundu, A., Atallah, M. J., & Bertino, E. (2012). Leakage-free redactable signatures. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy (CODASPY '12)* (pp. 307–316). ACM. <https://doi.org/10.1145/2133601.2133639>
 13. Derler, D., Pöhls, H. C., Samelin, K., & Slamanig, D. (2016). A general framework for redactable signatures and new constructions. In *Information Security and Cryptology — ICISC 2015* (LNCS, Vol. 9558, pp. 3–19). Springer. https://doi.org/10.1007/978-3-319-30840-1_1
 14. Hirose, S., & Kuwakado, H. (2013). Redactable signature scheme for tree-structured data based on Merkle tree. In *Proceedings of the 10th International Conference on Security and Cryptography (SECRYPT 2013)* (pp. 313–320). SciTePress. <https://doi.org/10.5220/0004507003130320>
 15. Johnson, R., Walsh, L., & Lamb, M. (2012). Homomorphic signatures for digital photographs. In *Financial Cryptography and Data Security (FC 2011)* (LNCS, Vol. 7035, pp. 141–157). Springer. https://doi.org/10.1007/978-3-642-27576-0_12
 16. Naveh, A., & Tromer, E. (2016). PhotoProof: Cryptographic image authentication for any set of permissible transformations. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 255–271). IEEE. <https://doi.org/10.1109/SP.2016.23>
 17. Ko, H., Lee, I., Lee, S., Kim, J., & Oh, H. (2021). Efficient verifiable image redacting based on zk-SNARKs. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (ASIA CCS '21)* (pp. 213–226). ACM. <https://doi.org/10.1145/3433210.3453110>
 18. Marinho, J., Schiller, E., Debaugé, A., & Foukia, N. (2025). ZK-Disclosure: Privacy-preserving information disclosure for digital evidence with C2PA and zk-SNARKs. In *2025 Annual Computer Security Applications Conference Workshops (ACSAC Workshops)* (pp. 309–315). IEEE. <https://doi.org/10.1109/ACSACW69556.2025.00040>
 19. Awan, M., & Collomosse, J. (2026). *Soft redaction of image provenance via zero-knowledge proofs* (arXiv:2608.07063). arXiv. <https://arxiv.org/abs/2608.07063>
 20. Datta, T., Chen, B., & Boneh, D. (2025). VerITAS: Verifying image transformations at scale. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 4606–4623). IEEE. <https://doi.org/10.1109/SP61157.2025.00097>
 21. Della Monica, P., Visconti, I., Vitaletti, A., & Zecchini, M. (2025). Trust Nobody: Privacy-preserving proofs for edited photos with your laptop. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 4624–4642). IEEE. <https://doi.org/10.1109/SP61157.2025.00014>
 22. Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys 2003)* (pp. 31–42). ACM. <https://doi.org/10.1145/1066116.1189037>
 23. Kalnis, P., Ghinita, G., Mouratidis, K., & Papadias, D. (2007). Preventing location-based identity inference in anonymous spatial queries. *IEEE Transactions on Knowledge and Data Engineering*, 19(12), 1719–1733. <https://doi.org/10.1109/TKDE.2007.190662>
 24. Kido, H., Yanagisawa, Y., & Satoh, T. (2005). An anonymous communication technique using dummies



- for location-based services. In *Proceedings of the International Conference on Pervasive Services (ICPS '05)* (pp. 88–97). IEEE. <https://doi.org/10.1109/PERSER.2005.1506394>
25. Chow, C.-Y., & Mokbel, M. F. (2007). Enabling private continuous queries for revealed user locations. In *Advances in Spatial and Temporal Databases (SSTD 2007)* (LNCS, Vol. 4605, pp. 258–275). Springer. https://doi.org/10.1007/978-3-540-73540-3_15
26. Smith, G. (2009). On the foundations of quantitative information flow. In *Foundations of Software Science and Computational Structures (FoSSaCS 2009)* (LNCS, Vol. 5504, pp. 288–302). Springer. https://doi.org/10.1007/978-3-642-00596-1_21
27. Krawczyk, H., & Eronen, P. (2010). *HMAC-based extract-and-expand key derivation function (HKDF)* (RFC 5869). IETF. <https://doi.org/10.17487/RFC5869>
28. Bormann, C., & Hoffman, P. (2020). *Concise binary object representation (CBOR)* (RFC 8949). IETF. <https://doi.org/10.17487/RFC8949>
29. Moon, B., Jagadish, H. V., Faloutsos, C., & Saltz, J. H. (2001). Analysis of the clustering properties of the Hilbert space-filling curve. *IEEE Transactions on Knowledge and Data Engineering*, 13(1), 124–141. <https://doi.org/10.1109/69.908985>
30. Fett, D., Yasuda, K., & Campbell, B. (2025). *Selective disclosure for JSON Web Tokens* (RFC 9901). IETF. <https://doi.org/10.17487/RFC9901>

Отримано редакцією журналу / Received: 28.08.26

Прорецензовано / Revised: 16.09.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.