УДК 004.056

В. О. Супрунець

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ВІДЕОЗАПИСІВ У VSAAS-СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз методів забезпечення цілісності відеоданих у VSaaS-системах, зокрема криптографії на еліптичних кривих, блокчейн-реєстрів та пасивної форензики. Досліджено стійкість різних підходів до просторових і часових маніпуляцій, а також до легітимного перекодування відео в хмарних сховищах. Визначено переваги та обмеження кожного методу залежно від швидкості обробки даних та вимог до тривалості зберігання архівів..

Ключові слова: відеоспостереження як сервіс, хмарна безпека, цілісність, блокчейн, часові геші.

Abstract

The paper analyzes video integrity methods in VSaaS systems, specifically elliptic curve cryptography, blockchain ledgers, and passive forensics. It examines the resistance of various approaches to spatial and temporal manipulations, as well as to legitimate video transcoding in cloud storage. The study identifies the advantages and limitations of each method depending on data processing speed and archive storage duration requirements.

Keywords: Video Surveillance as a Service (VSaaS), cloud security, integrity, blockchain, temporal hashes

Вступ

У сучасну епоху цифрової трансформації послуги відеоспостереження як сервісу (VSaaS) стали невід'ємною частиною інфраструктури безпеки, що зумовлює критичну потребу в забезпеченні автентичності та цілісності відеоданих, які зберігаються у хмарних сховищах [1]. Розв’язання задачі перевірки автентичності відеоматеріалів виходить далеко за межі простої модифікації окремих пікселів усередині кадру, охоплюючи складні маніпуляції з послідовністю подій, такі як підміна цілих кадрів або фальсифікація часових міток, що може повністю змінити зміст доказової бази [2]. У зв’язку з комплексністю цієї задачі актуальним є проведення досліджень щодо захисту цілісності відеозаписів.

Метою дослідження є покращення захисту даних в системах відеоспостереження, що використовують VSaaS, шляхом проведення аналізу та порівняння методів забезпечення цілісності відеозаписів.

Для досягнення мети необхідно виконати такі завдання: проаналізувати принципи формування відеоданих; виконати порівняльний аналіз методів захисту цілісності, які можуть бути використаними для розв’язання задачі дослідження; розробка практичних рекомендацій щодо застосування методів захисту.

Результати дослідження

Забезпечення цілісності цифрових відеоданих у системах відеоспостереження вимагає всебічного розуміння природи атак, які зловмисники можуть застосовувати для модифікації контенту. Сучасні наукові дослідження поділяють методи виявлення втручань на дві великі категорії: активні та пасивні [3]. Водночас самі атаки класифікуються на просторові та часові маніпуляції [3]. Просторові атаки спрямовані на зміну візуального змісту конкретних кадрів без порушення загальної тривалості відео. Вони включають видалення об'єктів, вставку нових елементів або використання техніки копіювання та переміщення фрагментів (copy-move) у межах одного й того ж зображення для приховування реальних подій. З іншого боку, часові атаки передбачають маніпуляції з послідовністю кадрів у часі. Це може бути видалення цілих сегментів подій (наприклад, моменту скоєння злочину), вставка сторонніх відеозаписів у наявний потік або перестановка кадрів місцями для створення цілком хибної хронології [2]. Усі ці втручання порушують фундаментальні принципи безпеки даних, до яких належать конфіденційність, цілісність та доступність інформації, що є критично важливими для функціонування будь-якої системи відеоспостереження [1].

Для протидії зазначеним загрозам активно застосовуються криптографічні методи захисту, серед яких особливу увагу привертає метод забезпечення цілісності даних на основі рандомізованого гешування в поєднанні з криптографією на еліптичних кривих (ECC) [4]. У цьому технічному підході безперервний потік відеоданих із камери спостереження попередньо розбивається на сегменти визначеного розміру. Перед тим як застосувати стандартний алгоритм гешування, кожен такий сегмент рандомізується за допомогою унікального випадкового значення. Процес гешування використовує випадковий вектор ініціалізації, який динамічно генерується системою за допомогою секретного ключа [4]. Це унеможливлює використання зловмисниками попередньо обчислених таблиць (rainbow tables) для підробки гешу. Після генерації результату гешування ця сума разом із секретним ключем піддається процедурі асиметричного шифрування з використанням алгоритму ECC [4]. Вибір криптографії на еліптичних кривих зумовлений її надзвичайно високою обчислювальною ефективністю. Даний алгоритм забезпечує рівень криптографічної стійкості, який є зіставним із традиційним алгоритмом RSA, проте використовує значно менший розмір ключа. Це суттєво зменшує навантаження на процесори камер спостереження та знижує вимоги до пропускної здатності мережі, що робить метод ідеальним для VSaaS-систем, які функціонують у режимі реального часу [4]. Будь-яка, навіть найменша модифікація бітового потоку відео миттєво призведе до повної невідповідності дешифрованого гешу, що дозволить системі негайно зафіксувати факт втручання.

Незважаючи на високу ефективність традиційних криптографічних підходів, вони стикаються зі значними проблемами при довгостроковому зберіганні відео в архівах. Криптографічні геші є надчутливими до будь-якої зміни бітів, що робить їх несумісними з процесами легітимного перекодування відео (format shifting), яке архіви змушені проводити для забезпечення сумісності файлів із новими стандартами відтворення у майбутньому. Вирішення цієї проблеми пропонується в системі ARCHANGEL, яка розроблена для забезпечення незмінності цифрових відеоархівів за допомогою часових гешів контенту (Temporal Content Hashes, TCH) та інтеграції з технологією блокчейн [5]. Система ARCHANGEL використовує архітектуру глибоких нейронних мереж для обчислення компактних часових гешів контенту з аудіовізуальних потоків, які можуть тривати хвилини або навіть години [5]. Ключовою технічною особливістю цих гешів є те, що вони інваріантні до кодеку, який використовується для ущільнення відео, але при цьому залишаються надзвичайно чутливими до будь-якої випадкової або зловмисної модифікації самого візуального змісту. Згенеровані часові геші контенту, а також моделі нейронних мереж, використані для їх створення, фіксуються та захищаються в розподіленому реєстрі на основі блокчейну з консенсусом Proof-of-Authority (доказ повноважень) [5]. Цей блокчейн розподілений між кількома незалежними організаціями. Ефективність ARCHANGEL була практично доведена під час масштабного пробного розгортання, у якому взяли участь національні урядові архіви Сполученого Королівства, Естонії та Норвегії, що підтверджує придатність методу для систем глобального рівня [5].

У випадках, коли відео завантажується до хмарної системи зі сторонніх джерел і не має вбудованих активних засобів захисту, єдиним способом перевірки його автентичності залишаються пасивні методи виявлення підробок [2]. Суть пасивних методів полягає у виявленні слідів втручання через аналіз внутрішньої статистики медіафайлу без використання водяних знаків чи цифрових підписів. Найважливішим напрямком пасивного аналізу є дослідження структури груп зображень (Group of Pictures, GOP) в ущільненому відеопотоці. Цифрове відео ущільнюється шляхом експлуатації просторової та часової надлишковості, розділяючи послідовність на I-кадри (внутрішньо кодовані), P-кадри (прогнозовані) та B-кадри (двонаправлено прогнозовані) [2]. I-кадри кодуються за схемою, подібною до стандарту JPEG, де обробляється лише просторова інформація окремого зображення. Перший кадр будь-якого відеофайлу завжди є I-кадром. P-кадри розраховують свої значення на основі попередніх опорних I- або P-кадрів, що дозволяє суттєво зменшити обсяг даних. B-кадри забезпечують найбільший рівень ущільнення, оскільки вони прогнозують рух пікселів одночасно з попередніх та наступних кадрів [2]. Оскільки прогнозувати тривалі сцени динамічного фону лише за одним першим кадром технічно неможливо, I-кадри регулярно вставляються в потік, формуючи жорстку періодичну структуру GOP. Будь-яка маніпуляція з часовою шкалою відео, така як видалення або вставка кадру, неминуче руйнує цю регулярну послідовність. Більше того, для збереження відредагованого файлу зловмисник змушений перекодувати відео, що призводить до подвійного ущільнення. Таке повторне збереження залишає чіткі математичні артефакти та помилки квантування, які експерти з форензики можуть виявити за допомогою спеціалізованих алгоритмів [2].

Ще одним високоефективним методом пасивного аналізу є перевірка цілісності відео шляхом дослідження характеристик його контейнера [6]. Хоча більшість криміналістичних методів аналізують безпосередньо потік пікселів, такий підхід стає неефективним при дослідженні відео з високим рівнем ущільнення або низькою роздільною здатністю, які часто зустрічаються в соціальних мережах та хмарних сервісах. Водночас структура відеоконтейнера зберігає значний обсяг метаданих, які можуть розкрити історію походження файлу. Запропонований дослідниками метод дозволяє ідентифікувати програмне забезпечення, використане для створення або маніпуляції з відео, а також операційну систему пристрою-джерела [6]. Це досягається завдяки використанню класифікатора на основі дерева рішень, який аналізує спеціально сформоване векторне представлення деревоподібної структури контейнера. Метод пройшов ретельну валідацію на масивному наборі даних, що складався з 7000 відеофайлів. Цей набір містив відео, модифіковані за допомогою найпопулярнішого програмного забезпечення (ffmpeg, Exiftool, Adobe Premiere, Avidemux, Kdenlive), а також відео, завантажені з платформ соціальних мереж, таких як Facebook, TikTok, Weibo та YouTube [6]. Аналіз контейнерів працює значно швидше за попіксельний аналіз і може бути автоматизований для миттєвої фільтрації підозрілого контенту на етапі його завантаження у VSaaS-сховище. Також варто враховувати, що комплексний захист інфраструктури вимагає дотримання правил кібергігієни та запобігання несанкціонованому доступу на рівні мережевих протоколів [1].Порівняння основних методів забезпечення цілісності, описаних у джерелах, наведено в таблиці нижче.

Таблиця 1 – Порівняльна характеристика методів забезпечення цілісності відео

Критерій	Рандомізоване гешування	Блокчейн та TCH	Контейнерний аналіз	Пасивний аналіз
Основна перевага	Висока безпека бітового рівня	Інваріантність до формату	Швидкість аналізу	Не потребує втручання
Стійкість до перекодування	Низька	Висока	Відсутня	Середня
Складність впровадження	Середня	Висока	Низька	Середня
Об'єкт перевірки	Бітовий потік	Візуальний контент	Метадані контейнера	Статистика ущільнення

На основі аналізу відомостей, наведених в табл. 1, рекомендується застосовувати гібридну архітектуру захисту для VSaaS-систем. Для оперативного моніторингу та виявлення миттєвих втручань найбільш доцільним є використання сегментованого рандомізованого гешування з математичним апаратом ECC [4], оскільки цей метод забезпечує математичну гарантію відповідності кожного кадру оригіналу. У той же час, для критично важливих об'єктів, де відео може зберігатися роками і проходити через етапи архівації та зміни форматів, необхідно впроваджувати часові геші контенту, зафіксовані в децентралізованих блокчейн-мережах [5]. Це нівелює ризики, пов'язані з централізованим керуванням хмарним сховищем, де адміністратор сервісу міг би теоретично видалити або змінити дані. Пасивні методи аналізу, зокрема характеристика контейнерів та аналіз артефактів ущільнення [6], повинні використовуватися як вторинний інструментарій для проведення пост-фактум експертиз, коли початкові криптографічні мітки відсутні або пошкоджені.

Висновки

Проведений аналіз свідчить, що оптимальним компромісом між безпекою та продуктивністю для сучасних VSaaS-систем є поєднання рандомізованого гешування на основі ECC для поточного захисту та блокчейн-технологій для довгострокової архівації. Рандомізоване гешування гарантує високу швидкість обробки та математичну точність виявлення змін [4], тоді як часові геші контенту забезпечують стійкість до процесів перекодування відео в хмарі [5]. Впровадження таких комплексних рішень дозволяє мінімізувати ризики успішного застосування як просторових, так і часових методів фальсифікації відеоданих у хмарному середовищі.

Подальші дослідження в цьому напрямі доцільно провадити в контексті експериментальних досліджень продуктивності, а також визначення обмежень та технічних вимог до захисту цілісності відеозаписів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Asghar A., Shifa A., Asghar M. N. Survey on Video Security: Examining Threats, Challenges, and Future Trends. Computers, Materials & Continua. 2024. Vol. 79. URL: https://file.techscience.com/files/cmc/2024/TSP_CMC-80-3/TSP_CMC_54654/TSP_CMC_54654.pdf (last accessed: 02.02.2026)

2. Sitara K., Mehtre B. M. Digital video tampering detection: An overview of passive techniques. Digital Investigation. 2016. Vol. 18. P. 8–22. URL: https://daneshyari.com/article/preview/457998.pdf (last accessed: 03.02.2026).

3. Habeeb R., Manikandan L. C. A Review: Video Tampering Attacks and Detection Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2019. Vol. 5, Iss. 5. P. 158–168. URL: https://www.researchgate.net/publication/336494795_A_Review_Video_Tampering_Attacks_and_Detection_Techniques (last accessed: 04.02.2026).

4. Ghimire S., Lee B. A data integrity verification method for surveillance video system. Multimedia Tools and Applications. 2020. Vol. 79. P. 30163–30185. URL: https://www.researchgate.net/publication/343668378_A_data_integrity_verification_method_for_surveillance_video_system(last accessed: 05.02.2026).

5. ARCHANGEL: Tamper-proofing Video Archives using Temporal Content Hashes on the Blockchain / T. Bui et al. _CVPR Workshop paper_. 2019. 9 p. URL: https://openaccess.thecvf.com/content_CVPRW_2019/papers/BCMCVAI/Bui_ARCHANGEL_Tamper-Proofing_Video_Archives_Using_Temporal_Content_Hashes_on_the_CVPRW_2019_paper.pdf(last accessed: 06.02.2026).

6. Efficient video integrity analysis through container characterization / P. Yang et al. 2021. 12 p. URL: https://arxiv.org/pdf/2101.10795v1 (last accessed: 07.02.2026).

Супрунець Володимир Олександрович – студент групи 2БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vovasp100@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Volodymyr Suprunets – student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vovasp100@gmail.com

Supervisor: ***Yurii Baryshev*** – PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua.