УДК 004

Катерина БАТЬКІВСЬКА, Сергій КУЛИНА

Західноукраїнський національний університет

МЕТОДИ ВИЯВЛЕННЯ ПІДРОБЛЕНИХ АБО ЗМІНЕНИХ ЗОБРАЖЕНЬ ІЗ ЗАСТОСУВАННЯМ КРИПТОГРАФІЧНИХ ХЕШ-ФУНКЦІЙ

Вступ. У цифрову епоху зображення стали одним із ключових носіїв інформації, що використовуються в медіа, освіті, електронній комерції, державних установах та правовій системі. З розвитком технологій редагування та створення візуального контенту (зокрема DeepFake, GAN) значно зросла кількість підроблених зображень, які можуть бути використані для дезінформації, фальсифікації доказів або маніпуляції громадською думкою [1]. Це зумовлює необхідність створення надійних методів перевірки автентичності цифрових файлів. Одним із найефективніших і водночас простих інструментів є криптографічні хеш-функції, які забезпечують контроль цілісності та виявлення будь-яких змін у зображенні [2].

Мета: дослідження методів виявлення підроблених або змінених зображень із застосуванням криптографічних хеш-функцій.

1. Принципи роботи криптографічні хеш-функції

Криптографічна хеш-функція перетворює будь-яку кількість даних на короткий, унікальний ідентифікатор - хеш-код. Якщо змінити навіть один піксель, колір або метадані (EXIF) у файлі, нове хеш-значення буде повністю відрізнятися від оригіналу. Ця властивість, відома як ефект лавини, дозволяє надійно виявляти навіть незначні підробки.

Основні вимоги до безпечної хеш-функції:

- односторонність - неможливо відновити вихідні дані з хешу;
- стійкість до колізій - важко знайти два різні файли з однаковим хешем;
- висока продуктивність - швидке обчислення хешів для великої кількості зображень.

Серед сучасних алгоритмів найпоширенішими є MD5, SHA-1, SHA-256 та SHA-3 [3]. Однак, MD5 та SHA-1 більше не вважаються безпечними через доведені колізії. На противагу їм алгоритми сімейства SHA-2 (зокрема SHA-256) забезпечують високу стійкість до атак, а SHA-3 забезпечує ще вищий рівень безпеки завдяки принципу губчастої конструкції.

2. Практичні аспекти виявлення змінених зображень

Для перевірки автентичності зображення використовується наступний алгоритм дій:

- обчислення хешу оригінального файлу (SHA-256 або SHA-3);
- збереження цього хешу в безпечному сховищі або базі даних;
- під час повторної перевірки, обчислення нового хешу та порівняння його з оригіналом;
- якщо хеші не збігаються, зображення було змінено або пошкоджено.

Графічно алгоритм зображено на рисунку 1.

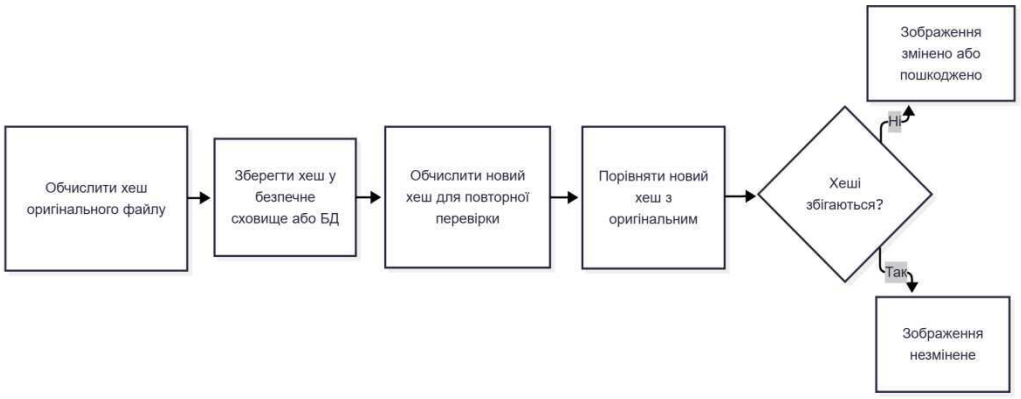

Рисунок 1 - Алгоритм перевірки автентичності зображення

Алгоритм, представлений на рисунку 1, дозволяє легко виявити будь-які спроби несанкціонованого редагування, навіть якщо зміни невидимі для людського ока. Для підвищення рівня безпеки система може бути доповнена цифровими підписами (DSA або RSA), які гарантують автентичність автора, а також використанням стеганографічних водяних знаків, які приховують хеш безпосередньо в піксельних даних зображення [4].

3. Порівняльний аналіз алгоритмів хешування

MD5 та SHA-1 – це ранні криптографічні хеш-функції, але зараз вважаються застарілими через відомі вразливості до колізій. MD5 забезпечує високу швидкість, але низький рівень безпеки, і більше підходить для неформального контролю даних, ніж для захисту. SHA-1 дещо надійніший, але також більше не рекомендується для критично важливих застосувань.

На противагу цьому, SHA-256, який є частиною сімейства SHA-2, забезпечує значно вищу безпеку, зберігаючи при цьому хорошу продуктивність. Він широко використовується для перевірки цілісності файлів, цифрових підписів та в блокчейн-системах. Найновіша – SHA-3, яка базується на принципово іншій конструкції (Keccak). Вона демонструє дуже високу стійкість до атак і використовується в критично важливих інформаційних системах, зокрема для захисту цифрових доказів та в урядових криптографічних стандартах. На відміну від SHA-2, який використовує класичну схему Меркла-Дамгарда, SHA-3 реалізує губкоподібну (sponge) конструкцію, що дозволяє гнучко налаштовувати параметри безпеки та ефективно працювати в умовах обмежених ресурсів. Обидва алгоритми підтримуються сучасними криптографічними протоколами (TLS, PGP, S/MIME) і рекомендовані до використання такими організаціями, як NIST та ISO. В умовах зростаючих загроз цифровій безпеці вони забезпечують надійний фундамент для побудови систем автентифікації, верифікації цифрового контенту та зберігання доказів у юридичній практиці.

Алгоритми SHA-256 та SHA-3 вважаються сучасним стандартом криптографічного хешування завдяки їхній високій стійкості до криптоаналітичних атак, включаючи колізії та атаки на основі прообразів, що робить їх надійним інструментом для забезпечення цілісності файлів, автентифікації цифрових повідомлень, захисту електронних підписів, а також для використання в технологіях блокчейн та цифровій криміналістиці, де цілісність даних є критично важливою.

Таблиця 1 - Порівняльний аналіз алгоритмів хешування

Алгоритм	Довжина хешу (біт)	Рівень безпеки	Стійкість до колізій	Швидкодія	Застосування
MD5	128	Низький	Уразливий	Висока	Лише базова перевірка
SHA-1	160	Середній	Часткова	Висока	Обмежене використання
SHA-256	256	Високий	Висока	Середня	Перевірка цілісності файлів
SHA-3	256/512	Дуже високий	Дуже висока	Середня	Критичні системи, захист доказів

Як видно з таблиці 1, незважаючи на високу продуктивність алгоритм MD5 є повністю скомпрометованим алгоритмом, оскільки для нього вже давно виявлені колізії, що робить його непридатним для використання в системах безпеки. SHA-1, хоча й демонструє кращу стабільність, також не рекомендується для використання в сучасних рішеннях через часткові колізії, виявлені у 2017 році. Алгоритм SHA-256 забезпечує оптимальний баланс між продуктивністю та безпекою: він ефективно працює з великими зображеннями у форматах PNG та JPG, має високу стійкість до колізій та є фактичним стандартом для перевірки цілісності файлів у більшості операційних систем та мережевих протоколів [5].

SHA-3 характеризується підвищеною стійкістю до криптоаналітичних атак завдяки іншій структурі (модель губки). Доцільно використовувати його в системах, де довгострокова надійність є критично важливою, наприклад, у судових реєстрах, блокчейнах або при зберіганні цифрових доказів. Таким чином, SHA-256 можна вважати оптимальним рішенням для практичного контролю цілісності зображень, а SHA-3 – стратегічним вибором для майбутніх систем, орієнтованих на підвищення довіри та юридичної значущості цифрових даних[6].

Висновок. Аналіз підтверджує ефективність криптографічних хеш-функцій як універсального механізму виявлення підроблених або змінених зображень. Алгоритми SHA-256 та SHA-3 забезпечують оптимальне поєднання стійкості до колізій, продуктивності та захисту від сучасних атак. Їх інтеграція з цифровими підписами та технологіями блокчейн створює новий рівень безпеки для підтримки довіри до цифрових матеріалів у медіа, правовій та технічній сферах.

Перелік використаних джерел.

1. Verdoliva L. Media Forensics and DeepFakes: An Overview. IEEE Journal of Selected Topics in Signal Processing, 2020, Vol. 14, No. 5, pp. 910–932. DOI: 10.1109/JSTSP.2020.3002103

2. Столлінгс В. Криптографія та мережева безпека: принципи та практика. – Pearson, 2022.

3. Кучер В.І., Бондаренко І.В. Основи криптографії: підручник. – Київ: НАУ, 2020.

4 Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 2021.

5. Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. – Springer, 2020.

6. NIST. Secure Hash Standard (SHS): FIPS PUB 180-4. – National Institute of Standards and Technology, 2015.