- Для IoT і вбудованих рішень доцільно використовувати полегшені набори тестів або спеціалізовані фреймворки з підтримкою паралельного виконання, щоб врахувати обмежені ресурси.
- Загалом найкращий результат дає комбінований підхід, який поєднує статистичне та ентропійне тестування, оскільки вони виявляють різні типи слабких місць генераторів.

Отже, генератори псевдовипадкових чисел є критичними не лише для криптографії, але й для багатьох інших задач кібербезпеки. Їх якість визначає надійність результатів у тестуванні, пентесті, виявленні аномалій і ML-системах. Чинні стандарти (NIST та ISO) задають базові підходи до оцінювання, але повну картину забезпечує лише поєднання статистичних, ентропійних і ML-методів. Подальші дослідження мають бути спрямовані на створення адаптивних тестів для ресурсно-обмежених систем, уточнення критеріїв якості ГПВЧ для конкретних застосувань кібербезпеки та інтеграцію методів машинного навчання у стандартизовані процедури оцінювання.

1. Марія Хомік, Олег Гарасимчук. Застосування генераторів псевдовипадкових чисел та послідовностей в кібербезпеці, методи їх побудови та оцінки якості // Захист інформації. – 2023. – Т. 25, № 3. – С. 147–159. DOI: https://doi.org/10.18372/2410-7840.25.17940.
2. NIST SP 800-22 Rev. 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / Rukhin A., Soto J., Nechvatal J., et al. – Gaithersburg, MD: National Institute of Standards and Technology, 2010. – 127 p. – DOI: 10.6028/NIST.SP.800-22r1a.
3. NIST SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation / Bassham L. III, et al. – Gaithersburg, MD: National Institute of Standards and Technology, 2018. – 88 p. – DOI: 10.6028/NIST.SP.800-90B.

Розробка застосунку для забезпечення конфіденційності користувачів шляхом анонімізації метаданих у мультимедійних файлах

УДК 004.056.5

А.А. Гринько[1], Г.В. Шаповалов[2]

Національний університет «Одеська політехніка»
10252755@stud.op.edu.ua, shapovalov@op.edu.ua

Глобальна цифровізація та масове розповсюдження мультимедійного контенту актуалізували проблему захисту персональної інформації в інформаційному просторі. Кожен медіафайл супроводжується масивом метаданих стандартів EXIF, XMP та IPTC, які часто містять критично чутливі відомості: GPS-координати, серійні номери обладнання та часові маркери. Такі дані стають підґрунтям для деанонімізації особи та підготовки атак із використанням соціальної інженерії. Більшість загальнодоступних застосунків

проводять лише поверхневу обробку, ігноруючи глибоко вкладені теги, що створює ілюзію безпеки.

Метою роботи є розробка та програмна реалізація застосунку для ОС Windows, що забезпечує анонімізацію мультимедійних файлів шляхом модифікації заголовків без деградації якості контенту. Для досягнення мети проаналізовано специфікації медіаконтейнерів, змодельовано алгоритми деструкції метаданих EXIF, XMP та ID3, а також спроєктовано архітектуру системи з модулем логування на базі SQLite.

Архітектура застосунку базується на модульному патерні MVC, де рівень представлення на PyQt6 ізольований від логіки бінарного парсингу. Центральний контролер координує передачу дескрипторів файлів до сервісних модулів, які здійснюють пряму модифікацію заголовків медіаконтейнерів без перекодування. На низькому рівні взаємодія з файловою системою NTFS оптимізована шляхом буферизованого читання та використання атомарних операцій заміни файлів.

У результаті виконання роботи розроблено програмне забезпечення, яке дозволяє ефективно видаляти ідентифікаційні маркери без втрати якості медіафайлів. Використання асинхронної архітектури на базі Python дозволило досягти високої швидкодії при пакетній обробці даних. Реалізований підхід забезпечує надійний захист приватності в умовах масового розповсюдження контенту в мережі.

1. Information technology — Digital compression and coding of continuous-tone still images — Part 1: Requirements and guidelines : ISO/IEC 10918-1:1994 : standard. Revised 2021. URL: https://www.iso.org/standard/18902.html.
2. ExifTool by Phil Harvey : official website. URL: https://exiftool.org/.
3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.
4. Metadata Working Group. Guidelines For Handling Image Metadata : version 2.0. URL: https://s3.amazonaws.com/software.tagthatphoto.com/docs/mwg_guidance.pdf.

Комбінований метод захисту авторського права в зображеннях

УДК 004.056.5

Ірина Борисенко[1], Артем Грушевський[2]

Національний університет «Одеська політехніка»,
[1]borisenko.i.i@op.edu.ua, [2]10328113@stud.op.edu.ua

Традиційні методи захисту, такі як текстові метадані або видимі логотипи, виявилися малоефективними, оскільки вони легко видаляються або спотворюються зловмисниками. Це зумовлює гостру необхідність у розробці та впровадженні методів прихованого маркування на основі цифрових водяних знаків (ЦВЗ), які інтегруються безпосередньо в структуру графічного файлу на математичному рівні та демонструють високу стійкість до деструктивних впливів обробки сигналів.

Метою роботи є розробка комбінованого стеганографічного методу для захисту авторського права на цифрові зображення з застосуванням ЦВЗ, стійкого до стиснення.

В основі розробленого методу лежить комбінований підхід DWT-SVD як найбільш збалансований інструмент, що забезпечує одночасну візуальну невидимість (прозорість) вбудованого водяного знаку та його робастність (стійкість) до атак стиснення. Алгоритм вбудовування передбачає перехід зображення-контейнера в колірний простір YCbCr, де модифікації піддається лише канал яскравості (Y). До цього каналу застосовується дискретне вейвлет-перетворення на базі фільтра Хаара, що дозволяє виділити низькочастотну область апроксимації (LL), яка містить основну енергетичну складову зображення. Паралельно з цим, авторський водяний знак (логотип) піддається криптографічному скремблюванню за допомогою хаотичного перетворення Арнольда. Це перетворює впізнаваний підпис на візуальний шум, який неможливо відновити без знання секретного ключа. Математичне ядро системи реалізує модифікацію сингулярних чисел матриці LL-піддіапазону контейнера шляхом додавання до них сингулярних чисел зашифрованого знаку з певним коефіцієнтом інтенсивності α. Для реалізації «напівсліпої» схеми вилучення програма автоматично генерує та зберігає файл матричних ключів формату .npz. Це дозволяє проводити верифікацію авторства без наявності оригінального зображення, використовуючи лише захищене фото та збережені ортогональні матриці.

Експериментальні дані розробленого методу підтвердили його високу ефективність. PSNR = 41,8 дБ, що свідчить про ідеальну візуальну стійкість вбудованого ЦВЗ. Тестування на робастність продемонструвало, що водяний знак зберігає свою структуру та залишається впізнаваним після агресивного стиснення JPEG з фактором якості до 20%.

1. Мокін В. Б., Капшук О. В. Методи та засоби стеганографічного захисту інформації : монографія. Вінниця : ВНТУ, 2021. 180 с. URL: https://ir.lib.vntu.edu.ua/

Розробка безпечної системи таємного голосування

УДК 004.056.5

Володимир Гудиш [1], Валерій Трушевський [2]

Львівський національний університет імені Івана Франка, [1]volodymyr.hudysh@lnu.edu.ua, [2]valeriy.trushevsky@lnu.edu.ua

Голосування є ключовим механізмом народного волевиявлення в демократичному суспільстві. Проте сучасні виклики, зокрема пандемія COVID-19, повномасштабне збройне вторгнення Росії в Україну та вимушена міграція мільйонів громадян як всередині країни, так і за кордон, унеможливили або суттєво ускладнили участь у традиційному виборчому процесі. Ці обставини актуалізували запит на системи дистанційного електронного голосування як засіб забезпечення конституційного права на волевиявлення за будь-яких умов.