УДК 004.056.55:004.932
DOI https://doi.org/10.32689/maup.it.2025.4.26

Ольга СУПРУН
кандидат фізико-математичних наук, доцент,
доцент кафедри теорії та технології програмування,
факультет комп'ютерних наук та кібернетики,
Київський національний університет імені Тараса Шевченка,
o.n.suprun@gmail.com
***ORCID:** 0000-0002-1196-5655*

Мар'яна МУСІЙОВСЬКА
кандидат технічних наук, доцент кафедри інформаційних технологій,
Львівський державний університет внутрішніх справ,
mysijovska@ukr.net
***ORCID:** 0009-0005-1063-5717*

Тетяна ЛАВРИК
кандидат педагогічних наук, доцент, старший викладач кафедри кібербезпеки, факультет електроніки та інформаційних технологій, Сумський державний університет,
t.lavryk@cs.sumdu.edu.ua
***ORCID:** 0000-0002-7144-7059*

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ ПРОТОКОЛІВ У ЗАХИСТІ ВІДЕОДАНИХ В УМОВАХ ІНФОРМАЦІЙНИХ АТАК

Анотація. *Актуальність дослідження зумовлено зростанням інтенсивності та складності інформаційних атак, у межах яких відеодані стають однією з найбільш уразливих категорій цифрової інформації. У сучасних умовах традиційні криптографічні засоби не забезпечують повного захисту від перехоплення, підміни та латентних маніпуляцій, що актуалізує потребу у використанні стеганографічних протоколів як додаткового рівня безпеки. Показано, що приховане вбудовування службових і контрольних даних у відеопотоки дозволяє зберігати цілісність та автентичність інформації навіть за високих навантажень і деструктивних впливів мережевого середовища.*

Метою статті *є формування науково вивіреної концепції підвищення захищеності відеоданих шляхом інтеграції стеганографічних механізмів у процеси їх передавання та оброблення в умовах ескалації інформаційних загроз, що передбачає створення багаторівневої моделі безпеки з урахуванням параметрів сигналу, специфіки компресії та режимів функціонування потокових систем.*

Методологія *дослідження ґрунтується на системному аналізі моделей стеганографічного приховування, порівняльному оцінюванні стійкості різних алгоритмів до перетворень, компресії та втрат пакетів, а також на методах структурного та спектрального аналізу відеосигналів. Використано підходи моделювання поведінки прихованих даних у потоках з адаптивним бітрейтом та методи оцінювання ефективності інтегрованих стего-криптографічних рішень.*

Наукова новизна *полягає в комплексному обґрунтуванні можливостей та обмежень стеганографічних протоколів у високонавантажених відеосистемах, а також у формуванні моделі їх адаптивної інтеграції з криптографічними засобами. Виявлено закономірності впливу параметрів відеосигналу, динаміки компресії та мережевих характеристик на збереження прихованих даних. Доведено, що поєднання стеганографічного та криптографічного підходів забезпечує синергетичний ефект підвищення безпеки.*

У висновках *установлено, що стеганографічні протоколи здатні ефективно підсилювати захист відеоданих завдяки прихованості каналу, стійкості до повторного кодування та збереження контрольних маркерів після мережевих спотворень. Виявлено науково-технічні та алгоритмічні проблеми впровадження таких рішень, пов'язані з деградацією вбудованих даних під час адаптивної компресії та високими вимогами до обчислювальних ресурсів. Сформульовано рекомендації щодо адаптації та оптимізації стеганографічних моделей з огляду на тип відеоданих і профіль потенційних атак.*

Ключові слова: *приховане кодування, автентичність, цілісність даних, криптографічні механізми, адаптивна компресія, мережеві загрози, потокова передача, вбудовані маркери.*

Olha SUPRUN, Mariana MUSIIOVSKA, Tetiana LAVRYK. USE OF STEGANOGRAPHIC PROTOCOLS IN VIDEO DATA PROTECTION UNDER INFORMATION ATTACKS

Abstract. *The relevance of this research is driven by the increasing intensity and complexity of information attacks, in which video data has become one of the most vulnerable categories of digital information. Under contemporary conditions, traditional cryptographic tools do not provide complete protection against interception, substitution, and latent manipulations,*

which necessitates the use of steganographic protocols as an additional security layer. It has been demonstrated that covert embedding of service and control data into video streams enables preservation of information integrity and authenticity even under high loads and destructive impacts within network environments.

***The aim** of this article is to develop a scientifically validated concept for enhancing video data security through integration of steganographic mechanisms into their transmission and processing under escalating information threats. This involves creating a multilevel security model that accounts for signal parameters, compression specifics, and operational modes of streaming systems.*

***The research** methodology is based on systematic analysis of steganographic concealment models, comparative evaluation of different algorithms' resilience to transformations, compression, and packet losses, as well as structural and spectral analysis methods for video signals. Approaches for modeling covert data behavior in adaptive bitrate streams and methods for evaluating the effectiveness of integrated stego-cryptographic solutions were employed.*

***The scientific novelty** lies in comprehensive substantiation of the capabilities and limitations of steganographic protocols in high-load video systems, as well as in formulating a model for their adaptive integration with cryptographic tools. Patterns of influence exerted by video signal parameters, compression dynamics, and network characteristics on covert data preservation have been identified. It has been proven that combining steganographic and cryptographic approaches provides a synergistic effect in security enhancement.*

***The conclusions** establish that steganographic protocols can effectively strengthen video data protection through channel concealment, resilience to re-encoding, and preservation of control markers after network distortions. Scientific, technical, and algorithmic challenges in implementing such solutions have been identified, related to embedded data degradation during adaptive compression and high computational resource requirements. Recommendations have been formulated for adaptation and optimization of steganographic models based on video data type and potential attack profile.*

***Key words:** covert encoding, authenticity, data integrity, cryptographic mechanisms, adaptive compression, network threats, streaming transmission, embedded markers.*

Вступ. Проблема захисту відеоданих в умовах інтенсивного зростання інформаційних атак набуває критичної ваги, оскільки сучасні цифрові середовища характеризуються високою вразливістю до несанкціонованого доступу, модифікації та прихованого перехоплення потокового контенту. Збільшення обсягів відеокомунікацій у сферах безпеки, телемедицини, інтелектуального відеоспостереження, дистанційної освіти та мультимедійних сервісів формує новий рівень наукової та практичної значущості проблеми забезпечення цілісності, автентичності та конфіденційності відеопотоків. Традиційні криптографічні методи не завжди гарантують стійкість до складних атак, орієнтованих на аналіз структур даних, латентні зміни та реконструкцію відеофайлів, що зумовлює потребу в пошуку додаткових захисних механізмів. Стеганографічні протоколи відкривають можливість багаторівневого приховування критично важливої інформації у відеопослідовностях, забезпечуючи прихованість каналу передачі та підвищуючи стійкість систем до маніпулятивних впливів. Наукова проблема полягає у визначенні оптимальних моделей інтеграції стеганографічних методів у процеси захисту відеоданих з огляду на технічні, алгоритмічні та мережеві обмеження. Практичне завдання полягає у формуванні ефективних рішень, здатних протидіяти сучасним деструктивним впливам, гарантувати безпечну передачу інформації та підтримати надійність критичних інфраструктур, що функціонують у режимі реального часу.

Аналіз останніх досліджень і публікацій. Огляд сучасних досліджень дає змогу виокремити чотири взаємопов'язані наукові напрями. Перший із них охоплює концептуальні та архітектурні засади формування багаторівневого захисту відео на основі поєднання криптографічних і стеганографічних механізмів. Зокрема, у дослідженні Ю. Горбенко (Y. Horbenko) сформовано принципи zero trust-взаємодії, які закладають методологічну основу для застосування прихованих каналів у клієнтських середовищах [10]. Доцільність застосування гібридних схем криптостеганографії для захисту відеоданих від перехоплення та маніпуляцій обґрунтовують Р. Ф. Хасан (R. F. Hasan), Н. Н. Махді (N. N. Mahdi) та А. А. Р. Рашід (A. A. R. Rasheed) [2].

Зі свого боку, С. Лью (S. Liu) та співавтори демонструють можливості інтеграції HEVC-стеганографії з блокчейном, що забезпечує верифікацію операцій та прихованість самого факту передавання приватних даних [12]. Класифікацію методів приховування в просторовому та частотному доменах узагальнюють М. Далал (M. Dalal) та співавтори, підкреслюючи їхню чутливість до перекодування і компресії [6].

Другий науковий напрям пов'язаний з розробленням алгоритмічних рішень, спрямованих на підвищення стійкості стеганографічних методів до інформаційних атак. Наприклад, С. Дебнатх (S. Debnath) та співавтори розробили модель coverless-video стеганографії, яка усуває потребу в прямій модифікації контейнера та мінімізує ознаки виявлення [8]. Розширений огляд сучасних методів відеостеганографії здійснюють Дж. Кунхот (J. Kunhoth) та співавтори, акцентуючи на ролі глибинного навчання в оптимізації вбудовування та стійкості до стегоаналізу [11]. Модель прихованого вбудовування в метадані, що дозволяє забезпечити сумісність зі стандартними форматами відео й уникнути деформації кадрів, пропонують Д. Дарвіс (D. Darwis) із колегами [7]. У дослідженні Р. Аді (R. Adee) та

співавторів обґрунтовано гібридну модель безпеки для хмарних середовищ, в якій стеганографія виступає адаптивним механізмом маскування даних у нестабільних мережевих умовах [1].

Третій напрям досліджень стосується використання відео як універсального транспортного середовища для прихованого передавання інших типів медіаданих у хмарних та мережевих системах. Зокрема, Г. Шідагханті (G. Shidaganti) та співавтори демонструють підвищення безпеки шляхом комбінування криптографії і стеганографії в медіаконтейнерах, що може бути масштабовано на відеопотоки [14]. Схему багаторівневого хаотичного шифрування в поєднанні зі стеганографією у відео, де контейнером виступають відеофайли для прихованого транспортування чутливих зображень, запропоновано С. Альрекабі (S. Alrekaby) та співавторами [3]. Безпечне вбудовування ідентифікаційних маркерів у відеоспостереження досліджують М. Модіґа (M. Modiga) з колегами, підкреслюючи потенціал таких рішень для судової верифікації та протидії підробленню відео [13]. Схему LSB-приховування аудіо у відео реалізують С. Срінідхі (S. Srinidhi) та співавтори, аналізуючи компроміси між якістю зображення і стійкістю до атак перекодування [15].

Четвертий напрям наукових праць присвячено виявленню вразливостей стеганографічних схем і протидії стегоаналізу та змагальним атакам. Зокрема, методи, орієнтовані на протидію статистичним стегоаналітичним підходам, дозволяють визначати стійкі моделі приховування. Ці методи систематизують Р. Апау (R. Apau) та співавтори [4]. Вразливості прихованих каналів, наприклад, ризик їх використання зловмисниками, досліджують Й. Ґуанья-Моя (J. Guaña-Moya) та колеги, акцентуючи, що це створює потребу у формалізованих політиках контролю [9]. Вплив змагальних атак на алгоритми стеганографії кількісно аналізують М. Бокхарі (M. Bokhari) та співавтори, доводячи, що навіть високоточні методи можуть утрачати ефективність під дією модифікованих вхідних даних [5].

Попередні дослідження не пояснюють поведінку стеганографічних вставок у реальних потокових умовах зі змінним бітрейтом, перекодуванням і мережевими втратами. Недостатньо вивчено комбіновані стего-криптографічні моделі, а також відсутні стандартизовані методики оцінювання їх стійкості. Немає узагальнених рекомендацій щодо адаптації протоколів під різні типи відеоконтенту. У пропонованій роботі змодельовано стійкість прихованих даних у динамічних відеопотоках, оцінено ефективність інтегрованих стего-криптографічних рішень і сформовано практичні підходи до адаптації алгоритмів під конкретні режими передавання та профілі атак, що дозволяє усунути ключові прогалини та розширити наявні наукові уявлення.

Метою статті є розроблення науково обґрунтованого підходу до підвищення захищеності відеоданих шляхом інтеграції стеганографічних протоколів у процеси передавання та оброблення інформації в умовах зростання інтенсивності інформаційних атак.

Завдання статті:

1) дослідити структурні та функціональні властивості сучасних стеганографічних протоколів і визначити вплив параметрів відеосигналу, компресії та мережі на їх ефективність;

2) оцінити можливості комбінованих стего-криптографічних моделей та ідентифікувати науково-технічні й алгоритмічні обмеження їх застосування у високонавантажених відеосистемах;

3) сформувати науково обґрунтовані рекомендації щодо адаптації й оптимізації стеганографічних рішень відповідно до типів відеоданих та профілів інформаційних атак.

Виклад основного матеріалу. Дослідження сутності, структурних характеристик та функціональних можливостей сучасних стеганографічних протоколів у контексті захисту відеопотоків ґрунтується на аналізі алгоритмів прихованого вбудовування інформації у відеопослідовності, здатних забезпечувати додатковий шар інформаційної безпеки без помітної деградації якості передавання. Наукова актуальність дослідження зумовлена тим, що відеодані залишаються одним із найбільш уразливих типів мультимедійного контенту, оскільки вони характеризуються високою щільністю інформації, чутливістю до модифікацій та широким використанням стиснення. У таких умовах стеганографічні протоколи, орієнтовані на непомітність, стійкість і пропускну здатність, формують перспективний інструментарій для прихованого кодування службових повідомлень, маркерів автентифікації або елементів контролю цілісності (табл. 1).

Практичне застосування стеганографічних протоколів у сучасних відеосистемах базується на здатності алгоритмів непомітно змінювати структуру відеокадру або його перетворених компонентів так, щоб приховані дані залишалися стійкими до типових впливів, властивих реальним каналам передавання. У практиці інтелектуального відеоспостереження такі протоколи використовуються для непомітного маркування потоків ідентифікаторами джерела, що уможливлює відстеження підміни або модифікації контенту під час кібератак на мережеві відеореєстратори. В аналітичних платформах дистанційного моніторингу стеганографічні вставки дають змогу переносити службові сигнали синхронізації або контрольні хеші, які забезпечують коректність автоматичного аналізу навіть у разі

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

повторного перекодування відео у форматах H.264 чи H.265 [6, p. 5835]. У потокових мультимедійних сервісах приховані повідомлення часто інтегруються в частотні компоненти кадру, що дозволяє створювати невидимі канали для передачі автентифікаційних токенів без ризику їх перехоплення у відкритій мережі [12]. Стійкість таких рішень проявляється в здатності відновлювати вбудовані дані після масштабування, фільтрації, додавання шуму або зниження бітрейту, що робить стеганографічні протоколи дієвим інструментом зміцнення безпеки відеоданих у складних, динамічно змінюваних середовищах.

Ефективність стеганографічного приховування у відеоданих визначається складною взаємодією параметрів відеосигналу, алгоритмів компресії та мережевих характеристик, які формують умови збереження непомітності та стійкості вбудованих даних. Властивості сцени, ступінь руху, текстурна насиченість, інтенсивність квантування та варіації бітрейту під час передавання безпосередньо впливають на структуру кадрів і глибину змін, які можуть бути внесені без ризику виявлення або втрати прихованої інформації (табл. 2).

У практичних умовах приховування реалізується за допомогою адаптивного вибору областей відеокадру, які залишаються відносно стабільними навіть після інтенсивного стиснення або мережевих спотворень.

У системах відеоспостереження це дає змогу маркувати потоки контрольними хешами, що зберігаються після повторного перекодування в H.264 та H.265. У потокових сервісах приховані дані розподіляються між кількома блоками кадру, що забезпечує відновлення повідомлень після втрат пакетів під час переходу між профілями якості. У високоточних телемедичних системах стеганографічні протоколи інтегруються в низькоквантизовані області, завдяки чому службові маркери залишаються придатними для декодування навіть у разі зниження бітрейту [11, p. 41963]. Комплексне використання цих принципів забезпечує надійну роботу стеганографічних схем у реальних мережевих і обчислювальних середовищах.

Оцінювання потенціалу комбінованих моделей, що інтегрують стеганографічні та криптографічні механізми, базується на тому, що кожен із цих підходів забезпечує різні рівні захисту відеоданих і функціонує за відмінними принципами. Криптографія гарантує математичну стійкість і недоступність змісту, тоді як стеганографія забезпечує прихованість самого факту передавання службової або конфіденційної інформації. Їх взаємодоповнюваність створює можливості формування

Таблиця 1

Основні характеристики сучасних стеганографічних протоколів для відеоданих

Ознака протоколу	Характеристика	Очікуваний ефект
Рівень вбудовування	Піксельний, блочний, трансформний	Можливість адаптивного приховування залежно від типу відео та ступеня стиснення
Тип загортання інформації	Просте вбудовування, мінімальна модифікація, розподілене кодування	Зниження ризику виявлення стеганографічного каналу
Стійкість до атак	Атаки на перетворення, повторне кодування, шум, фільтрацію	Підвищення надійності каналу в умовах зовнішніх впливів
Пропускна здатність	Низька, середня, висока	Можливість передавання службових даних у режимі реального часу
Сумісність із кодеками	H.264/AVC, H.265/HEVC, AV1	Забезпечення працездатності в сучасних потокових системах

Джерело: сформовано на підставі [6, p. 5835–5836; 11, p. 41950; 8; 12].

Таблиця 2

Фактори впливу на ефективність стеганографічного приховування у відеоданих

Категорія факторів	Конкретний параметр	Характер впливу	Наслідок для стеганографії
Параметри відеосигналу	Текстурна насиченість і рух	Ускладнення статистичного аналізу	Підвищення непомітності та місткості
Алгоритми компресії	Квантування та перетворення	Усунення дрібних деталей	Зниження стійкості прихованих даних
Мережеві характеристики	Втрата пакетів, джиттер	Порушення міжкадрових залежностей	Ризик часткової втрати повідомлення
Адаптивний стримінг	Зміна профілю бітрейту	Перекодування на льоту	Необхідність дублювання даних
Тип кодека	Ступінь міжкадрового прогнозування	Залежність кадрів від попередніх	Посилення впливу дрібних змін

Джерело: сформовано на підставі [6, p. 5840–5841; 11, p. 41963; 2, p. 1745; 12].

багатошарових систем відеозахисту, в яких дешифрування не дає зловмиснику повної картини, якщо прихований канал залишається невиявленим. Комбіновані моделі дозволяють зменшити вразливість до атак на окремі компоненти безпеки та забезпечити надійну роботу захисних механізмів у динамічних мультимедійних середовищах (табл. 3).

Таблиця 3

Характеристики комбінованих стего-криптографічних моделей для відеоданих

Компонент системи	Функціональна роль	Перевага інтегрованого підходу
Криптографічний модуль	Шифрування відеофрагментів або службових даних	Гарантування недоступності змісту навіть у разі перехоплення
Стеганографічний канал	Приховане вбудовування зашифрованих блоків	Маскування факту існування захищеної інформації
Керування ключами	Розподіл ключових матеріалів між компонентами	Зниження ризиків компрометації шляхом розмежування функцій
Аналіз цілісності	Додаткові приховані контрольні коди	Виявлення модифікацій, непомітних для традиційних методів
Адаптивність моделі	Підбір областей кадру для вбудовування	Стійкість до динамічних змін у кодеках та мережевих умовах

Джерело: сформовано на підставі [1; 2, p. 1747–1748; 3; 7, p. 27080–27082; 8].

Отже, комбіновані моделі функціонують як двошарові системи, в яких спочатку формується криптографічно стійкий фрагмент даних, а потім він розміщується в малопомітних або стійких до трансформацій областях відеокадру. У сервісах потокового відео це дає змогу передавати зашифровані маркери доступу або контрольні вектори без ризику їх перехоплення у відкритих мережах, оскільки зловмисник не може визначити місце їх розташування. У системах дистанційної аналітики зашифровані ділянки вбудовуються у блоки, які зберігають структуру після транскодування, що забезпечує коректність вилучення навіть під час роботи адаптивних стримінгових алгоритмів [8]. У відеоаналітичних комплексах безпеки комбіновані моделі дозволяють створювати приховані механізми контролю автентичності, які залишаються непомітними після маскування шумом, зміни масштабів кадру або застосування фільтрів стабілізації. Завдяки синергетичному використанню криптографії та стеганографії такі системи забезпечують підвищений рівень захисту в сценаріях, де традиційні методи не гарантують повної стійкості до перехоплення, модифікації або підміни відеоданих.

Упровадження стеганографічних протоколів у високонавантажені системи відеооброблення та передавання ускладнюється комплексом взаємопов'язаних науково-технічних, алгоритмічних і організаційних проблем, що виникають на всіх рівнях формування й транспортування відеопотоків. Однією з ключових проблем є нестача математичних моделей, здатних коректно описувати поведінку прихованих даних у потоках зі змінною структурою кадру, коли кодеки динамічно перебудовують прогнозні залежності й квантування відповідно до профілю навантаження. Високий рівень компресії в сучасних відеостандартах призводить до швидкої деградації вбудованих фрагментів, що робить класичні методи вбудовування малопридатними в режимах реального часу [11, p. 41952]. Додаткові труднощі створює варіативність поведінки адаптивних стримінгових алгоритмів, які змінюють бітрейт і періоди ключових кадрів, порушуючи передбачуваність структурних блоків, придатних для стеганографічного приховування.

Алгоритмічні обмеження пов'язані з необхідністю забезпечити баланс між непомітністю та стійкістю, що в умовах високонавантажених систем вимагає складних моделей оптимізації, здатних працювати за мінімальних затримок. Використання глибинних моделей аналізу стійких областей кадру передбачає значні обчислювальні ресурси, які в реальних системах можуть спричиняти збільшення затримок оброблення та зниження кадрування на секунду (frames per second, fps), що є критичним для задач відеоспостереження, дрон-аналітики та промислових систем контролю [11, p. 41956–41959]. Проблемою є також нестача універсальних алгоритмів, які залишаються працездатними після транскодування в різних профілях H.264/H.265/AV1, адже приховані дані по-різному деградують залежно від стратегії компресії та типу прогнозування [12].

Організаційні обмеження стосуються відсутності стандартизованих протоколів оцінювання стеганографічної безпеки у відеосистемах, що унеможливлює інтеграцію таких механізмів у сертифіковані комплекси захисту інформації. Складність упровадження посилюється тим, що оператори відеосистем часто не мають достатнього технічного досвіду для належного налаштування параметрів приховування, а відсутність регламентованих процедур контролю цілісності прихованих фрагментів призводить до ризику непомітної втрати службових даних під час високих навантажень [8]. Додатковою проблемою є конфлікт між потребою в глибокому моніторингу мережевого трафіку й вимогою не розкривати сам факт існування стеганографічного каналу, що ускладнює розгортання систем аудиту та кіберзахисту [11, p. 41959–41960].

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Для забезпечення ефективного застосування стеганографічних рішень у захисті відеоданих доцільно формувати адаптивні конфігурації алгоритмів, орієнтовані на тип відеоматеріалу, динаміку сцен, рівень компресії та інтенсивність інформаційних атак. Оптимізація протоколів передбачає коригування глибини модифікації відеосигналу відповідно до спектральних характеристик та рухомості кадрів: для високодинамічних сцен доцільно використовувати методи із просторово-часовим розподілом змін, тоді як для статичних відео ефективними є спектральні моделі з перетворенням вейвлетів або дискретного косинусного перетворення (Discrete Cosine Transform, DCT). Практична реалізація потребує інтеграції стеганографії з криптографічними механізмами, що забезпечує подвійний рівень захисту та ускладнює відновлення прихованої інформації навіть за умов часткового руйнування сигналу. Варто враховувати профіль потенційних атак: у системах, де переважають статистичні методи виявлення, слід використовувати моделі із псевдовипадковим розсіюванням або стохастичним перемиканням масок, тоді як у мережах із високою ймовірністю перехоплення та повторного кодування – методи, стійкі до втрат, як-от модифікація в піддіапазонах середньої частоти. Рекомендовано впроваджувати модульні архітектури, які дозволяють гнучко перемикати стратегії приховування залежно від пропускної здатності, затримок і якості каналу. Практичний ефект підвищується за умови попереднього профілювання відеопотоків, регулярного тестування на стійкість до атак розпізнавання та використання автоматизованих систем контролю візуальної якості, що забезпечує збалансованість між непомітністю, точністю та продуктивністю в реальних умовах експлуатації.

Висновки. У дослідженні встановлено, що стеганографічні протоколи забезпечують додатковий рівень захисту відеоданих завдяки прихованості каналу та здатності зберігати вбудовану інформацію в умовах перекодування, втрати пакетів і варіативності мережевого середовища. Доведено, що максимальна ефективність досягається за умови врахування властивостей відеосигналу, глибини компресії та режимів передавання, а інтеграція стеганографії з криптографічними механізмами формує стійку багаторівневу модель захисту. Виявлено основні проблеми, серед яких: нестабільність структур відеопотоку під час адаптивного стиснення, деградація прихованих даних за високих рівнів квантування, підвищені обчислювальні вимоги для роботи в реальному часі, а також відсутність стандартизованих підходів до оцінювання стеганографічної безпеки та інтеграції таких протоколів у наявні інфраструктури. Рекомендовано використовувати адаптивні моделі приховування, що враховують спектральні характеристики сцени та змінюють глибину модифікації залежно від динаміки кадру; комбінувати стеганографічні та криптографічні засоби для підвищення стійкості до атак; застосовувати дублювання або розподілене вбудовування даних у системах зі змінним бітрейтом; упроваджувати автоматизовані засоби оцінювання непомітності та стійкості.

Перспективи подальших досліджень пов'язані зі створенням моделей прогнозування поведінки прихованих фрагментів у потоках зі змінною компресією, формуванням стандартів тестування та розробленням адаптивних інтелектуальних алгоритмів, здатних самостійно визначати оптимальні області для вбудовування в умовах реального часу.

Список використаних джерел:

1. Adee R., Mouratidis H. A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*. 2022. Vol. 22, no. 3. P. 1109. https://doi.org/10.3390/s22031109 (date of access: 17.11.2025).

2. Hasan R. F., Mahdi N. N., Rasheed A. A. R. Robust non-parametric regression models for some petroleum products. *Periodicals of Engineering and Natural Sciences (PEN)*. 2020. Vol. 8, no. 1. P. 263–271. https://doi.org/10.21533/pen.v8.i1.1045 (date of access: 17.11.2025).

3. Secure Image Transmission Using Multilevel Chaotic Encryption and Video Steganography / S. N. Alrekaby et al. *Algorithms*. 2025. Vol. 18, no. 7. P. 406. https://doi.org/10.3390/a18070406 (date of access: 17.11.2025).

4. Apau R., Asante M., Twum F., Ben Hayfron-Acquah J., Peasah K. O. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PLoS ONE.* 2024. Vol. 19, № 9. Article e0308807. DOI: https://doi.org/10.1371/journal.pone.0308807 (date of access: 17.11.2025)

5. Bokhari M. U., Gulfam, Hanafi B. Quantifying the impact of adversarial attacks on information hiding security with steganography. *International Journal of Information Technology*. 2025. Vol. 17. P. 409–422. URL: https://doi.org/10.1007/s41870-024-02191-4 (date of access: 17.11.2025).

6. Dalal M., Juneja M. A survey on information hiding using video steganography. *Artificial Intelligence Review*. 2021. Vol. 54, № 8. P. 5831–5895. https://doi.org/10.1007/s10462-021-09968-0 (date of access: 17.11.2025).

7. Darwis D., Fernando Y., Mehta A.R. Metadata-Based Video Steganography: Development of a New Model for Secure Information Embedding. *Engineering, Technology & Applied Science Research*. 2025. Vol. 15, № 5. P. 27076–27088. https://doi.org/10.48084/etasr.11937 (date of access: 17.11.2025).

8. Debnath S., Mohapatra R. K., Dash R. Secret data sharing through coverless video steganography based on bit plane segmentation. *Journal of Information Security and Applications*. 2023. Vol. 78. Article 103612. https://doi.org/10.1016/j.jisa.2023.103612 (date of access: 17.11.2025).

9. Guaña-Moya J., Borja-López Y., Gutiérrez-Constante G., Jaramillo-Flores P., Basurto-Guerrero O. Information Security Vulnerabilities Using Steganography as the Art of Hiding Information. In: Rocha Á. та ін. (eds). *Information Technology and Systems. ICITS 2024*. Lecture Notes in Networks and Systems, Vol. 932. Springer, Cham. https://doi.org/10.1007/978-3-031-54235-0_10 (date of access: 17.11.2025).

10. Horbenko Y. Secure Front-End Automation Framework: A Novel Approach to Client-Side Data Encryption and Zero Trust API Interaction. *Asian Journal of Research in Computer Science*. 2025. Vol. 18, № 6. P. 177–193. https://doi.org/10.9734/ajrcos/2025/v18i6690 (date of access: 17.11.2025).

11. Video steganography: recent advances and challenges / J. Kunhoth et al. *Multimedia Tools and Applications*. 2023. Vol. 82. P. 41943–41985. https://doi.org/10.1007/s11042-023-14844-w (date of access: 17.11.2025).

12. Liu S., Liu Y., Feng C., Zhao H., Huang Y. Blockchain Privacy Data Protection Method Based on HEVC Video Steganography. In: 2020 3rd International Conference on Smart BlockChain (SmartBlock). Zhengzhou, China, 2020. P. 1–6. https://doi.org/10.1109/SmartBlock52591.2020.00015 (date of access: 17.11.2025).

13. Modiga M.-M., Nita S.-L., Arseni S.-C. Secure Embedding of Sensitive Identity Data in Surveillance Videos Using Steganography. In: 2025 17th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). Targoviste, Romania, 2025. P. 1–6. https://doi.org/10.1109/ECAI65401.2025.11095540 (date of access: 17.11.2025).

14. Shidaganti G., M.V.L., Vinay M., Patil P. Enhancing Data Protection Using Cryptography and Image Steganography in Cloud Environment. In: 2024 5th International Conference on Circuits, Control, Communication and Computing (I4C). Bangalore, India, 2024. P. 93–99. https://doi.org/10.1109/I4C62240.2024.10748507 (date of access: 17.11.2025).

15. Srinidhi S. K., Vishal K. S., Shashank U. S., Nidhin Prabhakar T. V., Singh R. Video Based Steganography for Audio using LSB Approach. In: 2024 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI). Prayagraj, India, 2024. P. 1–6. https://doi.org/10.1109/CVMI61877.2024.10782459 (date of access: 17.11.2025).

Дата надходження статті: 28.11.2025
Дата прийняття статті: 10.12.2025
Опубліковано: 30.12.2025