



**Mykola Yu.
Ovchinnikov
Овчинников
Микола
Юрійович**

УДК 004.056:629.5

INTEGRATED MULTIMEDIA DATA PROTECTION IN SHIPBUILDING AND MARITIME INFRASTRUCTURE

**ІНТЕГРОВАНІЙ ЗАХИСТ МУЛЬТИМЕДІЙНИХ ДАНИХ
У СУДНОБУДУВАННІ Й МОРСЬКІЙ ІНФРАСТРУКТУРІ**

DOI [https://doi.org/10.15589/smi2026.1\(22\).15](https://doi.org/10.15589/smi2026.1(22).15)

**Mykola Yu.
Ovchinnikov**

Овчинников Микола Юрійович, асистент кафедри
штучного інтелекту та математичного моделювання
jurahost@gmail.com
ORCID: 0009-0009-8221-7193

National University «Odesa Law Academy», Odesa, Ukraine

Національний університет «Одеська юридична академія», Одеса, Україна

Abstract. The digital transformation of shipbuilding and maritime infrastructure (Shipbuilding 4.0) has resulted in an explosive growth of multimedia data: UAV-based hull and superstructure inspection imagery, ROV underwater footage, non-destructive testing (NDT) visual artefacts, as well as 3D models and digital twins of vessels, port structures and subsea assets. Such datasets are simultaneously objects of intellectual property (they embed design solutions, manufacturing know-how and system configurations) and evidence-critical artefacts for quality assurance, class surveys and dispute resolution. However, multi-party exchange workflows amplify the risks of content leakage, unauthorised reuse, file replacement, hidden defect retouching and loss of version traceability. This paper proposes an integrated protection approach combining: robust watermarking for attribution and leak-source tracing, fragile integrity controls (hashing and/or digital signatures) for tamper evidence, perceptual hashing for near-duplicate search and leak monitoring, and event logging with trusted timestamps to support a chain-of-custody model. The proposed scheme is mapped to the Identify–Protect–Detect–Respond–Recover functional elements commonly used in maritime cyber risk management and cyber resilience guidance. The evaluation plan includes imperceptibility and robustness metrics (PSNR/SSIM and NC/BER) and attack scenarios typical for maritime operational content: video transcoding, JPEG recompression, rescaling, partial cropping and document-level conversions (PDF embedding, screenshots, messaging apps). Imperceptibility is evaluated using the PSNR and SSIM metrics, which characterize the level of distortion and structural similarity of images after watermark embedding. Robustness is assessed by the NC and BER indicators, reflecting the correlation and bit error rate of the extracted watermark after typical operational transformations of multimedia data. The practical outcome is a standardised evidential package for engineering reports and legal procedures where each artefact carries a verifiable identifier and a controlled circulation history.

Key words: shipbuilding; maritime infrastructure; multimedia data; digital watermarking; perceptual hashing; integrity assurance; digital twins; cyber resilience.

Анотація. Цифрова трансформація суднобудування та морської інфраструктури (Shipbuilding 4.0) супроводжується стрімким зростанням обсягів мультимедійних даних: фото й відео оглядів корпусу та надбудов з БПЛА, підводних

інспекцій з ROV, матеріалів неруйнівного контролю (NDT), а також 3D-моделей і цифрових двійників суден, портових споруд і підводних конструкцій. Такі дані одночасно є об'єктом інтелектуальної власності (містять унікальні конструктивні рішення, виробничі ноу-хау, конфігурації систем) і мають доказове значення у процесах контролю якості, класифікаційних оглядів та врегулювання спорів. Проте багатосторонній обмін контентом (верфі, підрядники, постачальники, сюрвеєри, страхові та юридичні сторони) створює ризики: витік, несанкціоноване повторне використання, підміна файлів, прихована ретуш дефектів і втрата простежуваності версій. У статті запропоновано інтегрований підхід, який поєднує: робастні водяні знаки для атрибуції та відстеження джерела, крихкі механізми контролю цілісності (хешування/підпис) для виявлення змін, перцептивне хешування для пошуку копій і моніторингу витоків, журналювання подій та часові мітки для формування ланцюга зберігання доказів. Відповідність запропонованої схеми вимогам управління кіберризиками розглядається через функціональні елементи Identify–Protect–Detect–Respond–Recover, що є типовими для морських керівних документів. Для оцінювання ефективності передбачено використання метрик непомітності й робастності (PSNR/SSIM, NC/BER) та сценаріїв атак, характерних для морського контенту: перекодування відео, стиснення JPEG, масштабування, часткове кадрювання і документні перетворення (PDF, скриншоти, месенджери). Непомітність оцінюється за метриками PSNR і SSIM, які характеризують рівень спотворення та структурну подібність зображень після вбудовування водяного знака. Робастність визначається за показниками NC та BER, що відображають кореляцію і частку помилок при вилученні водяного знака після типових операційних перетворень мультимедійних даних. Практичний результат – формування стандартизованих доказових пакетів для інженерних звітів і юридичних процедур, де кожен артефакт має перевірюваний ідентифікатор та контрольовану історію обігу.

Ключові слова: суднобудування; морська інфраструктура; мультимедійні дані; цифровий водяний знак; перцептивне хешування; цілісність даних; цифровий двійник; кіберстійкість.

References

- [1] International Maritime Organization. (2025). MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (4 April 2025). URL: <https://www.wcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.3.pdf>
- [2] International Association of Classification Societies. (2023). UR E26 Rev.1: Cyber resilience of ships (Complete Revision, Nov 2023). URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf
- [3] International Association of Classification Societies. (2022). UR E27: Cyber resilience of on-board systems and equipment (Apr 2022). URL: <https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf>
- [4] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. <https://doi.org/10.1109/83.650120>
- [5] Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7), 1079–1107. <https://doi.org/10.1109/5.771066>
- [6] Monga, V., & Evans, B. L. (2006). Perceptual image hashing via feature points: Performance evaluation and trade-offs. *IEEE Transactions on Image Processing*, 15(11), 3452–3465. <https://doi.org/10.1109/TIP.2006.881948>
- [7] Swaminathan, A., Mao, Y., & Wu, M. (2006). Robust and secure image hashing. *IEEE Transactions on Information Forensics and Security*, 1(2), 215–230. <https://doi.org/10.1109/TIFS.2006.873601>
- [8] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4), 600–612. <https://doi.org/10.1109/TIP.2003.819861>
- [9] Delmotte, A., Tanaka, K., Kubo, H., Funatomi, T., & Mukaigawa, Y. (2020). Blind 3D-printing watermarking using moment alignment and surface norm distribution. *IEEE Transactions on Multimedia*. <https://doi.org/10.1109/TMM.2020.3025660>
- [10] Mauro, F., & Kana, A. A. (2023). Digital twin for ship life-cycle: A critical systematic review. *Ocean Engineering*, 269, 113479. <https://doi.org/10.1016/j.oceaneng.2022.113479>

- [11] Iwańkiewicz, R., & Rutkowski, R. (2023). Digital Twin of Shipbuilding Process in Shipyard 4.0. *Sustainability*, 15(12), 9733, pp. 1–27. <https://doi.org/10.3390/su15129733>
- [12] González-Sabbagh, S. P., & Robles-Kelly, A. (2023). A Survey on Underwater Computer Vision. *ACM Computing Surveys*, 55(13s), Article 268, pp. 1–39. <https://doi.org/10.1145/3578516>
- [13] López Peña, F., Deibe Díaz, Á., Orjales, F., & Losada Pita, J. (2024). An UAV system for visual inspection and wall thickness measurements in ship surveys. *Measurement*, 238, 115262. <https://doi.org/10.1016/j.measurement.2024.115262>
- [14] Lin, B., & Dong, X. (2023). Ship hull inspection: A survey. *Ocean Engineering*, 289(Part 1), 116281. <https://doi.org/10.1016/j.oceaneng.2023.116281>
- [15] Ovchynnykov, M. Yu., & Slatvinska, V. M. (2024). Tekhnichniy ta normatyvno-pravoviy aspekt y zakhystu ob'ektiv intelektualnoi vlasnosti na rynku audio-vizualnoi produktsii [Technical and regulatory aspects of intellectual property protection in the audio-visual market]. *Visnyk KhNTU*, (3), 259–270. <https://doi.org/10.35546/kntu2078-4481.2024.3.32>
- [16] Ovchynnykov, M. Yu. (2025). Komparatyvnyi analiz alhorytmiv vidbytku kontentu dlia system zakhystu intelektualnoi vlasnosti na multymediini dani [Comparative analysis of content fingerprinting algorithms for intellectual property protection systems for multimedia data]. *Naukovi perspektyvy*, 7(48), 1766–1779. [https://doi.org/10.52058/2786-6025-2025-7\(48\)-1766-1779](https://doi.org/10.52058/2786-6025-2025-7(48)-1766-1779)
- [17] Gul, E., & Tam, G. K. L. (2025). Survey: 3D watermarking techniques. *Journal of Visual Communication and Image Representation*, 112, 104572. <https://doi.org/10.1016/j.jvcir.2025.104572>
- [18] Scaradozzi, D., Gioiello, F., Ciuccoli, N., & Drap, P. (2024). A Digital Twin Infrastructure for NGC of ROV during Inspection. *Robotics*, 13(7), 96. <https://doi.org/10.3390/robotics13070096>
- [19] Topalov, A. M. (2025). Tsyfrova transformatsiia v zadakhakh upravlinnia suchasnoiu portovoiu infrastrukturoiu [Digital transformation in tasks of managing modern port infrastructure]. *Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl*, 3(85), 62–69. <https://doi.org/10.30748/zhups.2025.85.07>
- [20] Piadyshiev, V. H. (2023). Pytannia vdoshkonalennia kiberbezpeky morskogo transportu: zarubizhnyi dosvid [Improving maritime transport cybersecurity: foreign experience]. *Morska bezpeka ta oborona*, (1), 78–86. <https://doi.org/10.32782/msd/2023.1.10>
- [21] Mok, H., Uchanin, V. M., Lysenko, Y. Y. (2024). Doslidzhennia vykhrostrumovykh peretvoriuvachiv dlia kontroliu zvarnykh shviv konstruktsii iz aliuminiievnykh splaviv z vykorystanniam defektoskopa na bazi smartfona [Eddy current probes for inspection of weld seams using a smartphone-based flaw detector]. *Tekhnichna diahnostyka ta neruivnyi kontrol*, (3), 32–38. <https://doi.org/10.37434/tdnk2024.03.05>
- [22] Melnyk, O., Onyshchenko, S., Pavlova, N., Kravchenko, O., & Borovyk, S. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. *International Journal of Computer Science and Network Security*, 22(3), 135–140. <https://doi.org/10.22937/IJCSNS.2022.22.3.18>

Постановка задачі. У сучасному суднобудуванні та морській інфраструктурі мультимедійні дані стали частиною критичних виробничих і експлуатаційних процесів: фотозвіти й відеоматеріали оглядів корпусу, знімки дефектів, результати неруйнівного контролю (NDT), підводні інспекції портів споруд, а також 3D-моделі та цифрові двійники. Такі артефакти є об'єктом інтелектуальної власності та доказовим матеріалом для приймання робіт, класифікаційних оглядів і спорів. Виникає задача створення інформаційної схеми, яка одночасно забезпечує захист прав на контент, контроль ці-

лісності та простежуваність версій у багатосторонньому обміні.

Аналіз останніх досліджень і публікацій. Класичні підходи робастного вбудовування цифрових водяних знаків орієнтовані на непомітне вбудовування сигналу та стійкість до типових перетворень. Фундаментальним для цього напрямку є підхід розширеного спектра (spread spectrum), запропонований І. Коксом та співавторами, який забезпечує стійкість водяного знака до шуму, компресії та інших операційних спотворень мультимедійного контенту [4, с. 1673–1676]. Подальші дослідження і

узагальнювальні огляди розвивають ці підходи та використовують методи розширеного спектра для підвищення робастності й безпеки вбудовування [5, с. 1673–1674]. Узагальнювальні огляди також підкреслюють компроміс між непомітністю, робастністю та безпекою, а також відмінність сценаріїв захисту авторських прав і трасування (copyright/tracking) та автентифікації (authentication) [6, с. 1079–1082].

Перцептивне хешування формує компактний «відбиток» вмісту для пошуку схожих зображень і виявлення підмін. Підходи на основі інваріантних ознак («feature points») описують вимоги до робастності, крихкості та керованості ключем [7, с. 1–3], а інформаційно-теоретичні критерії дозволяють оцінювати безпеку хешування у змагальному середовищі [8, с. 215–216]. Додатково в українських дослідженнях виконано систематизацію та порівняння алгоритмів відбитка контенту (перцептивного хешування) для задач захисту інтелектуальної власності на мультимедійні дані [16, с. 1766–1768].

Окремий контекст для морської галузі задають вимоги кіберризик-менеджменту та кіберстійкості. Настанови ІМО рекомендують інтегрувати управління кіберризиками в існуючі процеси безпеки [1, с. 1–2], тоді як IACS Unified Requirements UR E26/UR E27 визначають мінімальні вимоги до кіберстійкості судна та бортових систем упродовж життєвого циклу [2, с. 2–3; 3, с. 1].

Окрему групу сучасних досліджень формують роботи, присвячені цифровим двійникам у суднобудуванні та морській інфраструктурі. Систематичний огляд цифрових двійників у судновій індустрії підкреслює, що термін «digital twin» часто використовується надто широко, а ключовою ознакою справжнього двійника є двосторонній обмін даними між фізичним об'єктом і віртуальним середовищем упродовж фаз життєвого циклу судна [10, с. 1–3]. Це прямо підсилює вимоги до якості первинних даних: інспекційні фото/відео та NDT-результати стають «датчиками реальності», а будь-які спотворення або втрата простежуваності версій можуть призвести до некоректних висновків щодо технічного стану й ризиків експлуатації.

На рівні верфі цифровий двійник розглядається як інструмент інтеграції планування, моніторингу та аналізу виробничих процесів. У роботі щодо «Shipyards 4.0» наголошується на потребі цифровізації реальних виробничих активностей і узгодженні потоків даних між підрозділами, щоб підвищити керованість процесів і контроль якості готових суден [11, с. 1–3]. Відповідно, мультимедійні артефакти (фото дефектів, відео оглядів, візуалізації 3D-моделей) слід трактувати як повноцінні цифрові активи, для яких потрібні процедури керування доступом, версіонування та підтвердження автентичності.

Паралельно стрімко розвивається напрям автоматизації інспекцій корпусу судна, що охоплює як «in-dock», так і підводні огляди. Огляд «Ship hull inspection: A survey» систематизує інспекційні підходи за класами (в доку, підводні, на основі SHM), а також розглядає NDT-техніки, автоматизовані платформи і методи обробки великих масивів даних, які зменшують суб'єктивність та небезпеку для інспектора [14, с. 1–4]. Така еволюція створює новий «потік доказів», у якому якість і достовірність цифрових матеріалів мають не менше значення, ніж власне точність вимірювань.

Показовим є приклад застосування БПЛА у суднових оглядах: у статті про UAV-систему для візуальної інспекції та ультразвукових вимірювань товщини в вантажних танках суден запропоновано інтегровану архітектуру збору зображень і вимірювань у реальних умовах експлуатації [13, с. 1–3]. Подібні рішення підвищують оперативність інспекцій, але одночасно збільшують ризики несанкціонованого поширення контенту та потребу у доведенні того, що дані не були змінені після зняття.

Для підводних інспекцій морських споруд і корпусів критичним є якісний аналіз зображень у складному середовищі (погана видимість, кольорові викривлення, каламутність, нестабільне освітлення). Узагальнюючий огляд з підводного комп'ютерного зору демонструє, що значна частина досліджень фокусується на реконструкції та відновленні зображень як передумови для задач

розпізнавання і відновлення форми, адже саме «якість» підводного зображення визначає достовірність вищорівневих висновків [12, с. 1–5]. У контексті ROV-інспекцій цифрові двійники розглядаються як інструмент навчання, тестування та підтримки навігації/керування, що також залежить від надійності даних і коректного обміну між віртуальною та реальною частиною системи [18, с. 1–4].

В українському науковому полі захист інтелектуальної власності на мультимедійні артефакти розглядається як комплекс технічних і нормативно-правових заходів. Зокрема, М. Ю. Овчинников та В. М. Слатвінська поєднують правовий аналіз механізмів охорони авторських прав із оглядом технічних підходів стеганографії та цифрових водяних знаків, а також підкреслюють перспективність використання глибинного навчання для підвищення стійкості маркування до атак [15, с. 259–263]. Для суднобудування й морської інфраструктури такий підхід є прикладним, оскільки інспекційні фото/відео та NDT-візуалізації одночасно виступають виробничими доказами і об'єктами ІР, а отже потребують і технічного захисту, і коректної юридичної атрибуції.

Перцептивне хешування та алгоритми «відбитка контенту» (content fingerprinting) виконують роль масштабованого інструмента пошуку копій і відстеження повторного використання мультимедійних матеріалів. У роботі М. Ю. Овчинникова наведено компаративний аналіз підходів до формування відбитків для різних типів мультимедіа (зображення, відео, текст), окреслено критерії робастності до атак і трансформацій та відзначено доцільність гібридних схем у комплексних системах захисту ІР [16, с. 1766–1768]. У морському домені це напряму підтримує задачі швидкого зіставлення інспекційних серій (UAV/ROV), виявлення дублювання кадрів у звітах та моніторинг витоків контенту підрядників.

У сучасних виробничих пайплайнах все більшу роль відіграє 3D-контент (CAD/mesh/point clouds), який використовується і як проектний артефакт, і як частина цифрового двійника. Огляди з 3D watermarking

відзначають різноманіття типів 3D-даних, атак (ремешинг, спрощення, нормалізація) та метрик оцінювання залежно від цільового сценарію (copyright, authentication, tracing) [17, с. 1–4]. Практично це підтверджує доцільність двоконтурної моделі: (а) захищати вихідні 3D-артефакти спеціалізованими методами та (б) додатково маркувати похідні 2D-візуалізації (рендери, скриншоти), які найчастіше потрапляють у документообіг і є найуразливішими до витоків.

Таким чином, сучасна література описує одночасний розвиток (1) технологій збирання інспекційних даних у морському домені (UAV/ROV, автоматизовані платформи, underwater CV), (2) цифрових двійників як інтегратора життєциклових даних, і (3) методів захисту автентичності/прав мультимедіа (watermarking, perceptual hashing). Водночас нормативні рамки морської кіберстійкості (IMO/IACS) підсилюють вимогу керування ризиками та доказовості даних у життєвому циклі, що робить інтегровані схеми захисту мультимедіа технологічно й організаційно обґрунтованими [1, с. 1–2; 2, с. 2–3].

В українському науковому дискурсі цифровізація морської інфраструктури також розглядається як фактор підвищення ефективності та прозорості портових операцій. Зокрема, А. М. Топалов аналізує інтеграцію технологій штучного інтелекту, Інтернету речей, блокчейну, автоматизації, великих даних і цифрових двійників у контур управління сучасною портовою інфраструктурою та наголошує на потребі уніфікованих моделей даних і взаємодії стейкхолдерів у «розумному порту» [19, с. 62–69]. Для нашого дослідження це важливо, оскільки саме мультимедійні артефакти (фото/відео інспекцій, візуалізації 3D) стають частиною такого інтегрованого контуру і потребують захисту прав та контрольованої простежуваності.

Питання кібербезпеки морського транспорту в Україні висвітлюються як окремий напрям у рамках морської безпеки, де підкреслюється зростання уразливостей через поєднання інформаційних технологій та операційних технологій у судноплаванні. В. Г. Пядишев узагальнює зарубіжний досвід

організації кібербезпеки морського судна та акцентує, що «відкритість» ОТ-контурів робить можливими сценарії зовнішнього втручання і потребує системного кіберризик-менеджменту на рівні компаній та галузі [20, с. 78–86]. Доповнює цей напрям робота українських авторів О. Мельника, С. Онищенко, Н. Павлової та співавторів, які розглядають впровадження управління кіберрисиками у судноплавній індустрії та формують рекомендації щодо безпечної експлуатації судна і його систем [22, с. 135–140]. У контексті нашої теми це задає вимогу: доказовість і цілісність інспекційних мультимедіа мають підтримувати процедури кіберстійкості, а не існувати ізольовано.

Вітчизняна школа неруйнівного контролю та технічної діагностики також демонструє тенденцію до цифровізації вимірювань і віддаленого обміну результатами. У статті Г. Мока, В. М. Учаніна та Ю. Ю. Лисенка запропоновано підхід до вихрострумової дефектоскопії з використанням дефектоскопа на базі смартфона з перспективою бездротової передачі та збереження даних контролю для подальшого аналізу [21, с. 32–38]. Такий клас рішень посилює роль «цифрового ланцюга доказовості»: результати контролю (у т.ч. мультимедійні представлення/графіки/зображення) мають супроводжуватись механізмами атрибуції, контролю цілісності та журналювання, щоб бути придатними для інженерних звітів і спорів у суднобудуванні й експлуатації морської інфраструктури.

Відокремлення невирішених раніше частин загальної проблеми. Недостатньо опрацьованими залишаються: (I) інтеграція вбудовування цифрових водяних знаків і хешування у багатосторонні ланцюги взаємодії верфі, підрядників і сюрвеєрів; (II) суміщення робастного контуру (що має зберігатися після операційних перетворень контенту) з крихким контуром (що має виявляти несанкціоновані зміни); (III) формування стандартизованого «доказового пакета» з метаданими, версіями та журналом подій; (IV) відображення технічних механізмів захисту на функціональні елементи кіберстійкості «Ідентифікація – Захист – Виявлення – Реагування – Відновлення»

(Identify–Protect–Detect–Respond–Recover) [2, с. 2–3].

Мета дослідження. Мета – обґрунтувати інтегровану схему захисту інтелектуальної власності та доказової цілісності мультимедійних даних у суднобудуванні й морській інфраструктурі, поєднавши робастне вбудовування цифрових водяних знаків, крихкий контроль цілісності, перцептивне хешування та журналювання подій.

Методи, об'єкт та предмет дослідження. Об'єкт – процеси створення, обробки, передачі та зберігання інспекційних і виробничих мультимедійних даних у життєвому циклі судна/об'єкта інфраструктури. Предмет – методи вбудовування цифрових водяних знаків і хешування для захисту прав та контролю цілісності у змагальній моделі загроз, що передбачає наявність активного порушника. Використано підходи робастного вбудовування цифрових водяних знаків [5, с. 1673–1674; 6, с. 1094–1097], перцептивного хешування на основі ознак [7, с. 1–3; 8, с. 215–216] та метрики якості зображень (SSIM) [9, с. 5–6].

Наукова новизна одержаних результатів полягає в удосконаленні підходу до захисту мультимедійних даних шляхом інтеграції робастного вбудовування цифрових водяних знаків, крихкого контролю цілісності, перцептивного хешування та журналювання подій у межах єдиного доказового контуру з урахуванням специфіки інженерних мультимедійних даних (дані інспекцій UAV/ROV, результати неруйнівного контролю (NDT), 3D-моделі конструкцій).

Вперше для задач суднобудування та морської інфраструктури запропоновано застосування такої інтегрованої багаторівневої схеми до обробки мультимедійних даних інспекційного та технічного призначення.

Набув подальшого розвитку підхід до формування доказового пакета мультимедійних артефактів, що поєднує атрибуцію, контроль цілісності, пошук копій і простежуваність змін.

Основний матеріал. Запропонована схема має чотири рівні (A–D), що розділяють функції атрибуції, фіксації ознак втручання (tamper evidence), пошуку копій і лан-

цюга доказовості, забезпечуючи сумісність з операційними перетвореннями контенту (JPEG/відео перекодування, PDF-вставки, скріншоти, пересилання у месенджерах).

Рівень А (атрибуція та трасування) реалізує робастний водяний знак. Корисне навантаження (payload) включає owner_id, project_id, doc_id, timestamp і за потреби recipient_id для сценаріїв персоналізованого маркування (fingerprinting) / виявлення джерела витоку (traitor tracing). Робастність повинна зберігатися після компресії та масштабування, що узгоджується з класичними підходами вбудовування цифрових водяних знаків (watermarking) [5, с. 1673–1676].

Рівень В (контроль цілісності) використовує крихкий контур: криптографічний хеш (наприклад, SHA-256) і/або цифровий підпис канонічної копії. Ключова ідея: водяний знак (watermark) відповідає на питання «чиє/звідки», а підпис – «чи змінювали». Це особливо важливо для NDT-даних та фото дефектів.

Рівень С (пошук копій) застосовує перцептивні хеші для виявлення повторного використання та витоків. Властивості перцептивного хеша мають забезпечувати робастність до «content-preserving» пере-

творень та чутливість до змістових підмін [7, с. 2]. Безпекові аспекти оцінюються через ключову рандомізацію й критерії невідзначеності [8, с. 215–216].

Рівень D (журналювання та часові мітки) формує незмінюваний журнал подій з послідовним додаванням записів (append-only): приймання даних (інжест), перевірка, експорт у звіт, передача отримувачам, оновлення версії. Це забезпечує ланцюг зберігання доказів (chain of custody) та відповідає ідеї інтеграції управління кіберризиками в наявні процеси безпеки [1, с. 2].

З метою конкретизації взаємодії рівнів запропонованої схеми доцільно розглянути послідовність обробки мультимедійного артефакту, яка відображена на Рис. 1.

Після завантаження зображення або відеофайлу формується його унікальний ідентифікатор та базові метадані. На рівні А виконується вбудовування робастного цифрового водяного знака, що забезпечує подальшу атрибуцію та трасування. Паралельно на рівні В обчислюється криптографічний хеш і, за потреби, формується цифровий підпис канонічної копії для фіксації її цілісності. На рівні С генерується перцептивний хеш, який використовується

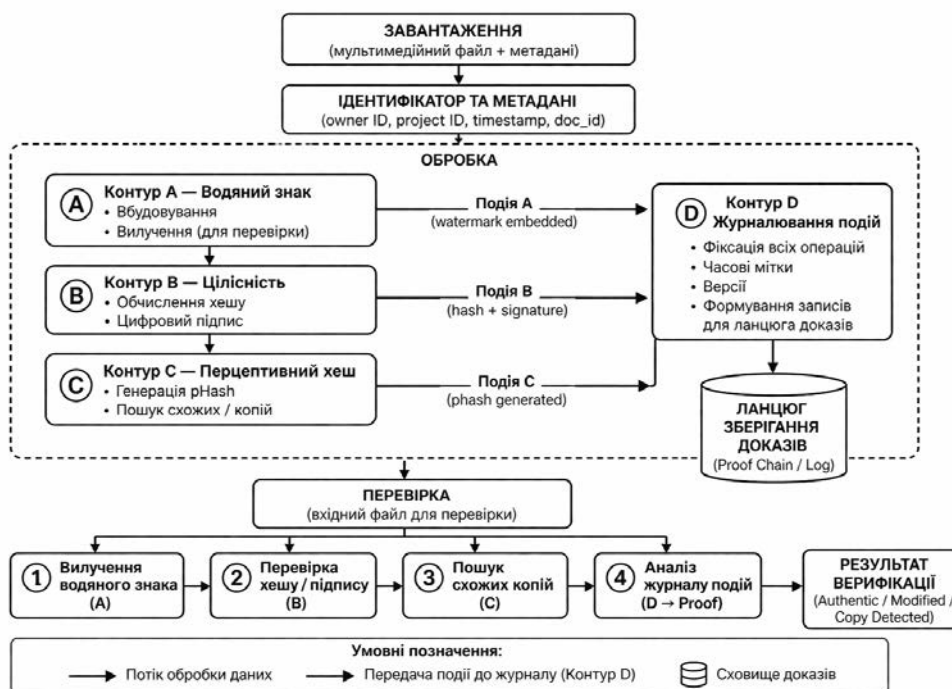


Рис. 1. Послідовність обробки мультимедійного артефакту в інтегрованій схемі

Джерело: авторська розробка.

для пошуку схожих або модифікованих копій у сховищі або зовнішніх джерелах. Усі операції фіксуються на рівні D у журналі подій із часовими мітками, що забезпечує формування ланцюга зберігання доказів. Під час перевірки зовнішньої копії система послідовно виконує вилучення водяного знака, перевірку цілісності за хешем або підписом, пошук схожих артефактів та аналіз історії змін, зафіксованої в журналі подій.

У таблиці 1 узагальнено типові ризики для мультимедійних даних у суднобудуванні/портовій інфраструктурі та відповідні механізми протидії.

Для документування компромісу «непомітність–робастність» у доказовому пакеті доцільно фіксувати базові метрики якості та робастності. Формули (1)–(3) не є складовими запропонованого методу, а використовуються як стандартні метрики оцінювання непомітності та робастності схеми.

Пікове відношення сигнал/шум (PSNR) визначається як:

$$PSNR = 10 \log_{10}(MAX_I^2 / MSE) \quad (1)$$

де MAX_I – максимальне можливе значення інтенсивності пікселя зображення, а MSE – середньоквадратична похибка між оригінальним і модифікованим зображеннями.

Нормалізована кореляція (NC) між вбудованим та вилученим водяним знаком обчислюється як:

$$NC = (\sum_i w_i \cdot \hat{w}_i) / (\sqrt{(\sum_i w_i^2)} \cdot \sqrt{(\sum_i \hat{w}_i^2)}), \quad (2)$$

де w_i – елементи початкового водяного знака, а $\hat{w}_i$ – відповідні елементи вилученого водяного знака.

Частка бітових помилок (BER) визначається за формулою:

$$BER = (1/L) \sum_{k=1}^L [b_k \neq \hat{b}_k], \quad (3)$$

де b_k і $\hat{b}_k$ – відповідно початковий та відновлений біти водяного знака, а L – загальна кількість бітів.

Наведені співвідношення є загальнозживаними в літературі з цифрового водяного маркування та застосовуються в роботі як інструменти оцінювання ефективності запропонованого підходу. Метрика SSIM застосовується як комплементарна до PSNR, оскільки оцінює структурні зміни зображення з урахуванням яскравості, контрасту та локальної структури, що є більш узгодженим із людським зоровим сприйняттям [9, с. 5–6].

Результати пілотної апробації. Для часткової кількісної оцінки запропонованого підходу проведено пілотну апробацію на базі локальної версії програмного комплексу ip-protect у контрольованому середовищі. Як експериментальний набір використано 3 JPEG-зображення корпусу судна, отримані з відкритого фотобанку Depositphotos, що легально придбані та використані для дослідницьких цілей. Зображення попередньо приведені до розміру 1600 px за довгою стороною. Для кожного зображення виконувалося вбудовування цифрового водяного знака з параметрами $\alpha = 0.98$, $\delta = 18$, $\text{repeat} = 11$, $\text{omega_count} = 24$, після чого оцінювалися показники непомітності та робастності після типових операційних перетворень: JPEG-стиснення (quality 90 та 75), масштабування до 50% і обрізання 10% зображення.



Рис. 2. Приклад мультимедійного артефакту (зображення корпусу судна), використаного для пілотної апробації запропонованої схеми

Джерело: Depositphotos, використано на умовах ліцензії

Таблиця 1. Загрози для мультимедійних даних та механізми протидії

Загроза/ризик	Прояв у процесах	Механізм протидії
Витік інспекційного контенту (IP leakage)	Розсилки підрядникам, месенджери, презентації	Watermark (A) + журналювання (D)
Підміна/ретуш дефектів	Заміна кадрів у звіті, прихована ретуш	Хеш/підпис (B) + журналювання (D)
Повторне використання матеріалів	Фото з іншого проєкту в поточному	Перцептивні хеші (C) + watermark (A)
Втрата простежуваності версій	Кілька «final_v3», «final_final»	Event log (D)

Джерело: авторська розробка.

Загалом сформовано 12 тестових комбінацій. У середньому по всіх тестах отримано такі значення: PSNR = 77.36 dB, NC = 0.25, BER = 0.75. Найкращі результати зафіксовано для сценарію JPEG-стиснення з quality 90, де частка успішного вилучення становила 100%, а середні значення склали PSNR = 87.70 dB, NC = 1.00, BER = 0.00. Для сценарію JPEG quality 75 середні значення становили PSNR = 81.96 dB, NC = 0.00, BER = 1.00. Для масштабування до 50% отримано PSNR = 77.44 dB, NC = 0.00, BER = 1.00, а для обрізання 10% – PSNR = 62.33 dB, NC = 0.00, BER = 1.00. Окрім метрик водяного знака, у дослідженні враховано функціонування допоміжних компонентів системи – перцептивного хешування та журналювання подій. Узагальнені результати експерименту наведено у таблиці 2.

Отримані результати свідчать, що запропонована схема забезпечує високий рівень непомітності вбудовування цифрового водяного знака та демонструє стійке його вилучення в умовах помірного JPEG-стиснення. Водночас для більш жорстких операційних перетворень, зокрема значного стиснення, масштабування та обрізання зображень, поточна конфігурація параметрів вбудовування і вилучення є недостатньо робастною, що підтверджується значеннями NC та BER.

Разом з тим результати показують, що навіть у випадках невеликого вилучення водяного знака система зберігає функціональність за рахунок інших компонентів, зокрема перцептивного хешування та журналювання подій. Зокрема, механізм пошуку схожих копій дозволяє ідентифікувати модифіковані зображення, а журналювання забезпечує фіксацію всіх операцій і формування ланцюга зберігання доказів.

Таким чином, запропонований підхід доцільно розглядати як інтегровану багато-

рівневу систему, у якій окремі механізми доповнюють один одного, забезпечуючи загальну стійкість до широкого спектра перетворень. Результати пілотної апробації підтверджують працездатність підходу для типових сценаріїв обробки мультимедійних даних у суднобудуванні та морській інфраструктурі та окреслюють напрями його подальшого вдосконалення.

Обговорення отриманих результатів.

Сильною стороною запропонованої схеми є поділ на робастний і крихкий контури: робастний водяний знак забезпечує атрибуцію та трасування після операційних перетворень контенту, тоді як крихкий контроль цілісності (хешування/криптографічний підпис) фіксує факт несанкціонованої зміни канонічної копії. Такий підхід узгоджується з класичним розмежуванням задач цифрового водяного маркування на сценарії трасування та персоналізованого маркування (tracking/fingerprinting) і автентифікації (authentication) [6, с. 1080–1082].

На рівні управління кіберризиками схему можна відобразити на IACS Identify–Protect–Detect–Respond–Recover: інвентаризація мультимедійних активів і потоків (Identify), контроль доступу та захист сховищ (Protect), перевірки watermark/хеша та пошук колізій (Detect), інцидент-процедури і відсікання скомпрометованих копій (Respond), повернення до канонічних версій і повторна валідація (Recover) [2, с. 2–3].

Порівняно з підходами, що ґрунтуються лише на робастному вбудовуванні цифрових водяних знаків, запропонована схема не обмежується атрибуцією та трасуванням, а доповнює їх крихким контролем цілісності, пошуком копій і журналюванням подій. На відміну від рішень, заснованих лише на криптографічному хешуванні або цифровому підписі, вона зберігає можливість ідентифі-

Таблиця 2. Кількісні результати оцінювання непомітності та робастності цифрового водяного знака при типових перетвореннях

Тип перетворення	PSNR, dB	NC	BER	Успішність вилучення	Виявлення копії (pHash)	Журналювання
JPEG (90)	87.70	1.00	0.00	1.00	Так	Так
JPEG (75)	81.96	0.00	1.00	0.00	Так	Так
Масштабування 50%	77.44	0.00	1.00	0.00	Так	Так
Стор 10%	62.33	0.00	1.00	0.00	Частково	Так
Середнє	77.36	0.25	0.75	0.25	-	Так

Джерело: авторська розробка.

кації походження мультимедійного артефакту після типових операційних перетворень. У свою чергу, системи, що використовують лише перцептивне хешування, є ефективними для пошуку схожих зображень і копій, однак не забезпечують ані підтвердження цілісності канонічної копії, ані формування повного ланцюга зберігання доказів. Отже, перевага запропонованого підходу полягає саме в інтеграції функцій атрибуції, контролю цілісності, виявлення копій і доказової простежуваності в межах єдиного технологічного контуру, орієнтованого на задачі суднобудування та морської інфраструктури.

Обмеження пов'язані з керуванням ключами та політиками довіри між стейкхолдерами, а також вибором порогів «схожості» для перцептивних хешів. Компроміс «робастність–безпека» для hashing-підходів потребує окремого налаштування під доменні атаки [8, с. 215–216].

Висновки. Обґрунтовано актуальність захисту інтелектуальної власності та доказової цілісності мультимедійних даних у суднобудуванні й морській інфраструктурі в умовах

цифрової трансформації та посилення вимог до кіберстійкості. Запропоновано інтегровану чотирирівневу схему: (I) робастне вбудовування цифрових водяних знаків, (II) хеш/підпис канонічної копії, (III) перцептивні хеші для пошуку копій, (IV) журналювання та часові мітки. Результати пілотної апробації підтвердили працездатність підходу для типових операційних перетворень, продемонструвавши високу непомітність маркування та його стійкість до помірного стиснення зображень. Показано відповідність запропонованих механізмів функціональним елементам управління кіберризиками Identify–Protect–Detect–Respond–Recover, що дозволяє інтегрувати схему в галузеві системи забезпечення безпеки згідно з настановами ІМО та вимогами ІАКС. Показано, що така схема є модульною та може впроваджуватися поетапно, забезпечуючи практичну сумісність з існуючими інженерними пайплайнами.

Подяка й інформація щодо фінансування дослідження. Фінансування: дослідження виконано без зовнішнього фінансування.

Список літератури

- [1] International Maritime Organization. (2025). MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (4 April 2025). Url: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.3.pdf>
- [2] International Association of Classification Societies. (2023). UR E26 Rev.1: Cyber resilience of ships (Complete Revision, Nov 2023). Url: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf
- [3] International Association of Classification Societies. (2022). UR E27: Cyber resilience of on-board systems and equipment (Apr 2022). Url: <https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf>
- [4] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687. <https://doi.org/10.1109/83.650120>
- [5] Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7), 1079–1107. <https://doi.org/10.1109/5.771066>
- [6] Monga, V., & Evans, B. L. (2006). Perceptual image hashing via feature points: Performance evaluation and trade-offs. *IEEE Transactions on Image Processing*, 15(11), 3452–3465. <https://doi.org/10.1109/TIP.2006.881948>
- [7] Swaminathan, A., Mao, Y., & Wu, M. (2006). Robust and secure image hashing. *IEEE Transactions on Information Forensics and Security*, 1(2), 215–230. <https://doi.org/10.1109/TIFS.2006.873601>
- [8] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4), 600–612. <https://doi.org/10.1109/TIP.2003.819861>
- [9] Delmotte, A., Tanaka, K., Kubo, H., Funatomi, T., & Mukaigawa, Y. (2020). Blind 3D-printing watermarking using moment alignment and surface norm distribution. *IEEE Transactions on Multimedia*. <https://doi.org/10.1109/TMM.2020.3025660>

- [10] Mauro, F., & Kana, A. A. (2023). Digital twin for ship life-cycle: A critical systematic review. *Ocean Engineering*, 269, 113479. <https://doi.org/10.1016/j.oceaneng.2022.113479>
- [11] Iwańkiewicz, R., & Rutkowski, R. (2023). Digital Twin of Shipbuilding Process in Shipyard 4.0. *Sustainability*, 15(12), 9733, pp. 1–27. <https://doi.org/10.3390/su15129733>
- [12] González-Sabbagh, S. P., & Robles-Kelly, A. (2023). A Survey on Underwater Computer Vision. *ACM Computing Surveys*, 55(13s), Article 268, pp. 1–39. <https://doi.org/10.1145/3578516>
- [13] López Peña, F., Deibe Díaz, Á., Orjales, F., & Losada Pita, J. (2024). An UAV system for visual inspection and wall thickness measurements in ship surveys. *Measurement*, 238, 115262. <https://doi.org/10.1016/j.measurement.2024.115262>
- [14] Lin, B., & Dong, X. (2023). Ship hull inspection: A survey. *Ocean Engineering*, 289(Part 1), 116281. <https://doi.org/10.1016/j.oceaneng.2023.116281>
- [15] Овчинников, М. Ю., & Слатвінська, В. М. (2024). Технічний та нормативно-правовий аспекти захисту об'єктів інтелектуальної власності на ринку аудіо-візуальної продукції. *Вісник ХНТУ*, (3), 259–270. <https://doi.org/10.35546/kntu2078-4481.2024.3.32>
- [16] Овчинников, М. Ю. (2025). Компаративний аналіз алгоритмів відбитку контенту для систем захисту інтелектуальної власності на мультимедійні дані. *Наукові перспективи*, 7(48), 1766–1779. [https://doi.org/10.52058/2786-6025-2025-7\(48\)-1766-1779](https://doi.org/10.52058/2786-6025-2025-7(48)-1766-1779)
- [17] Gul, E., & Tam, G. K. L. (2025). Survey: 3D watermarking techniques. *Journal of Visual Communication and Image Representation*, 112, 104572. <https://doi.org/10.1016/j.jvcir.2025.104572>
- [18] Scaradozzi, D., Gioiello, F., Ciuccoli, N., & Drap, P. (2024). A Digital Twin Infrastructure for NGC of ROV during Inspection. *Robotics*, 13(7), 96. <https://doi.org/10.3390/robotics13070096>
- [19] Топалов, А. М. (2025). Цифрова трансформація в задачах управління сучасною портовою інфраструктурою. Збірник наукових праць Харківського національного університету Повітряних Сил, 3(85), 62–69. <https://doi.org/10.30748/zhups.2025.85.07>
- [20] Пядишев, В. Г. (2023). Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. *Морська безпека та оборона*, (1), 78–86. <https://doi.org/10.32782/msd/2023.1.10>
- [21] Мок, Г., Учанин, В. М., Лисенко, Ю. Ю. (2024). Дослідження вихрострумових перетворювачів для контролю зварних швів конструкції із алюмінієвих сплавів з використанням дефектоскопа на базі смартфона. *Технічна діагностика та неруйнівний контроль*, (3), 32–38. <https://doi.org/10.37434/tdnk2024.03.05>
- [22] Мельник, О., Онищенко, С., Павлова, Н., Кравченко, О., & Боровик, С. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. *International Journal of Computer Science and Network Security*, 22(3), 135–140. <https://doi.org/10.22937/IJCSNS.2022.22.3.18>

© Овчинников М. Ю.

Дата першого надходження статті до видання: 21.01.2026

Дата прийняття статті до друку після рецензування: 18.02.2026

Дата публікації (оприлюднення) статті: 15.05.2026



Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0