



ЗАХИСТ АВТОРСЬКОГО ПРАВА PDF-ДОКУМЕНТІВ З ВИКОРИСТАННЯМ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ І ЕЛЕКТРОННОГО ПІДПISУ

Розглянуто проблему захисту авторських прав для електронних документів, які розробляються і поширюються в PDF-форматі. Наявні засоби захисту електронних документів, такі як паролі або стандартне шифрування PDF-файлу, не забезпечують достатнього рівня його стійкості до атак, пов'язаних із видаленням або модифікацією захисних механізмів, що вказують на автентифікацію самого документа. З огляду на це актуальним є розроблення багаторівневих систем захисту електронного документа, які поєднують різні методи приховування та захисту інформації. Значне поширення PDF-документів у практичній діяльності в різних сферах діловодства та правовій сфері, що пов'язана з укладанням та завершенням договорів з використанням електронних документів, зумовлює нагальну потребу їхнього захисту від підробок модифікації чи присвоєння чужих документів з порушенням авторських прав. Це, водночас, ставить завдання для розробників, видавців і поширювачів електронних документів у мережі Інтернет впроваджувати певні механізми захисту таких документів, пов'язаних з їхньою автентифікацією та з дотриманням прав авторства. Розроблено програмну систему багаторівневого захисту PDF-документів на основі вибору та поєднання методів цифрових водяних знаків (ЦВЗ), криптографічного шифрування і стеганографії. Запропоноване програмне забезпечення реалізує декілька незалежних підходів до приховування та захисту інформації: метадані PDF-документа, видимі водяні знаки, приховані анотації, методи частотної області DCT (англ. *Discrete Cosine Transform*), криптографічне шифрування AES (англ. *Advanced Encryption Standard*) та стелс-стеганографію. Окремо реалізовано модуль цифрового підпису документів. Програмну реалізацію виконано мовою Python із використанням бібліотек PyPDF2, OpenCV, cryptography та Tkinter. Комплексний захист документів із впровадженням в їхню структуру цифрових водяних знаків дає змогу підвищити їхню стійкість до несанкціонованого доступу, модифікації та порушення авторського права. Охарактеризовано кожен із засобів нанесення цифрових водяних знаків на PDF-документ, їхні переваги та недоліки. Експериментально перевірено стійкість кожного методу захисту та автентифікації документа до зовнішніх атак на виявлення в них цифрових водяних знаків і обґрунтовано використання комбінованих методів захисту залежно від класу документа і його подальшого призначення, що може слугувати базою для розроблення автоматизованої системи захисту авторських прав.

Ключові слова: інформаційні технології; безпека електронних документів; інформаційна безпека; криптографічний захист електронного документа; автентичність документів; цілісність документів; цифрова ідентифікація електронного документа; стеганографія.

Вступ / Introduction

Стрімкий розвиток електронного документообігу, цифрових бібліотек, інституційних репозитаріїв і хмарних платформ призвів до істотного збільшення кількості електронних документів, що поширюються мережею Інтернет. Одним із найпоширеніших форматів їх зберігання є PDF, який використовують для наукових публікацій, монографій, дисертацій, юридичних документів, технічної документації та електронних видань.

Дослідження цифрового водяного маркування, стеганографії, цифрових підписів та захисту електронних документів здійснено у значній кількості наукових праць [2, 4, 8, 9, 15, 16, 17, 18, 19]. Серед сучасних досліджень у цій предметній області варто відзначити праці Ziyu Hongxia Wang та Soung Yuan Han [20], Saif Al-

deen S. Naem та Sarab M. Hameed [11], Linfeng Jiang [7] та інших авторів. У їхніх роботах запропоновано методи цифрового водяного маркування, криптографічного захисту, електронного підпису, використання метаданих та стеганографії для захисту цифрових документів. Водночас, більшість наявних досліджень стосується окремих методів захисту електронних документів і практично не розглядає можливості їх комплексного використання у складі єдиного програмного комплексу для PDF-документів із подальшим експериментальним оцінюванням їхньої ефективності.

У сучасних інформаційних системах PDF-документи є одним із найпоширеніших форматів зберігання та обміну інформацією. Наразі можна навести такий перелік найпоширенішого їх використання:

- PDF є міжнародним стандартом ISO 32000 [6];

© Copyright 2026 by the author(s)

Сабат Володимир Іванович, д-р техн. наук, професор, кафедра мультимедійних технологій.

Email: volodymyr.i.sabat@lpnu.ua; <https://orcid.org/0000-0001-8130-7837>

Богоніс Олександр Орестович, аспірант, кафедра комп'ютерних технологій у видавничо-поліграфічних процесах.

Email: oleksandr.o.bohonis@lpnu.ua; <https://orcid.org/0009-0005-1341-6245>

Цитування за ДСТУ: Сабат В. І., Богоніс О. О. Захист авторського права PDF-документів з використанням цифрових водяних знаків і електронного підпису. Науковий вісник НЛТУ України. 2026, т. 36, № 4. С. 151–158.

Citation APA: Sabat, V. I., & Bohonis, O. O. (2026). Copyright protection of PDF documents using digital watermarks and digital signatures. *Scientific Bulletin of UNFU*, 36(4), 151–158. <https://doi.org/10.36930/40360417>

- PDF використовують як основний формат для електронного документообігу, наукових публікацій, юридичних документів, технічної документації та поліграфічної продукції;
- практично всі великі цифрові бібліотеки (IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Wiley, MDPI, arXiv тощо) поширюють повнотекстові статті саме у форматі PDF;
- більшість державних установ, університетів і видавництв використовують PDF як фінальний формат документів для збереження структури та оформлення.

Зростання обсягів електронного документообігу зумовлює нагальну потребу захисту PDF-документів від несанкціонованого копіювання, підроблення та модифікації. Тому актуальним завданням є розроблення програмних засобів комплексного захисту PDF-документів, які поєднують цифрові водяні знаки (ЦВЗ), криптографічні методи та цифровий підпис із можливістю експериментального оцінювання їх ефективності.

Об'єкт дослідження – захист авторського права електронних PDF-документів.

Предмет дослідження – методи та засоби впровадження ЦВЗ і електронного підпису для підтвердження авторства PDF-документів і їхнього захисту, що дасть змогу розробити комплексний підхід для створення системи захисту авторських прав для PDF-документів.

Мета роботи – розробити комплексну систему захисту авторського права PDF-документів на основі поєднання ЦВЗ, електронного підпису та криптографічного захисту й експериментально оцінити ефективність запропонованих засобів захисту електронних документів, що дасть змогу підвищити стійкість електронних документів до несанкціонованої модифікації, підроблення та видалення засобів автентифікації.

Для досягнення зазначеної мети визначено такі основні завдання дослідження:

- реалізувати у програмній системі модулі видимих і прихованих ЦВЗ для їх впровадження у PDF-документи, що дасть змогу провести їх дослідження і зробити порівняльний аналіз стійкості до зовнішніх атак;
- інтегрувати криптографічний захист алгоритмом AES для шифрування службової інформації, що використовується під час вбудовування ЦВЗ, що дасть змогу протидіяти атакам "грубої сили", спрямованим на методи зламу системи шляхом підбору ключа;
- розробити стеганографічний метод прихованого вбудовування ЦВЗ на основі методу частотної області DCT (англ. *Discrete Cosine Transform*), що дає можливість впровадити в растровий документ невидимі мітки, стійкі до типових атак, пов'язаних зі стисненням, шумом та модифікацією документа;
- забезпечити приховане вбудовування у структуру PDF-документа ЦВЗ, що унеможливить їх виявлення для сторонніх осіб;
- реалізувати модуль цифрового підпису документів, що дає змогу накладати цифровий підпис для підтвердження авторства, автентичності та цілісності документа.

Аналіз останніх досліджень та публікацій. У роботі [11] підсумовано частину загальних принципів, що регулюють механізми захисту PDF-документів, зокрема – зосереджено увагу на введенні принципів стеганографії та криптографії у протоколи безпеки PDF-документа, а також на виборі змістовних та репрезентативних дослідницьких робіт, щоб підсумувати переваги та недоліки запропонованих методів.

Впровадження у структурні елементи PDF-файлу, такі як текст, зображення та форми, зашифрованого во-

дяного знаку наведено у роботі [20]. Також у цій роботі запропоновано алгоритм виявлення несанкціонованого доступу в документ, який забезпечує цілісність контенту та полегшує ідентифікацію змінених областей у файлі з водяним знаком.

У роботі [21] запропоновано схему, яка може автоматично адаптувати алгоритм та параметри водяних знаків відповідно до характеристик даних для числових і текстових даних. Теоретично встановлено та експериментально перевірено ефективність запропонованого методу з точки зору стійкості та меншого спотворення даних. Це робить його придатним для захисту авторських прав, ідентифікації власника або відстеження порушників авторського права.

Методи захисту PDF-документів, які розробила фірма Adobe, розглянуто в електронній публікації [12]. При цьому основну увагу приділено реалізації захисту PDF-документів у програмі Adobe Acrobat на основі політик безпеки. Компанія Adobe розробила комплексний набір вбудованих методів та інструментів захисту для формату PDF, які реалізовані у програмному забезпеченні Adobe Acrobat. Ці методи поділяються на кілька рівнів: від базового обмеження доступу до корпоративного керування правами та безпеки самого середовища перегляду.

У роботах [16, 18] розглянуто методи нанесення водяного знаку на цифрові зображення, запропоновано алгоритм печворку для надання зображенню автентичності, щоб неавторизовані користувачі не могли претендувати на нього. Створений програмний додаток для вбудовування інформації у вигляді невидимого водяного знаку на зображенні стійкий до зовнішніх впливів.

У запропонованому дослідженні [15] розроблено систему для автентифікації та перевірки транскрипту та тимчасового сертифіката цифрового електронного підпису на основі алгоритму хешування Вегурт для захисту документа. Модель генерує ключ шифрування для унікальної ідентифікації та оцінювання документа, щоб визначити, чи він підроблений чи автентичний.

У працях [13, 14] розглянуто інформаційні технології впровадження ЦВЗ в електронні документи та визначено їх основні параметри. Запропоновано алгоритми внесення ЦВЗ в електронні документи.

У науковій публікації [9] розглянуто принцип формування цифрового підпису на основі використання криптографічних хеш-функцій та асиметричної криптографії для підписання даних. Він також забезпечує автентифікацію походження, цілісність даних та невідомість підписувача. Основна ідея полягає в тому, щоб згенерувати хеш даних за допомогою криптографічної хеш-функції, а потім зашифрувати його підписуючою стороною за допомогою свого закритого ключа. У роботі [17] розглянуто вирішальне значення цифрових підписів у гарантуванні дійсності, цілісності та неспростовності електронних комунікацій. Досліджено технологічний прогрес цифрових підписів і їх практичне використання в різних секторах шляхом ретельного аналізу базових технологій, враховуючи інфраструктуру відкритих ключів (PKI) та криптографічні хеш-функції.

У роботі [8] здійснено огляд поточного стану правового регулювання у сфері захисту авторських прав в українському законодавстві, зокрема – в контексті використання мережі Інтернет. На основі проведеного аналізу сформульовано пропозиції щодо вдосконалення пра-

вових механізмів охорони авторських прав у цифровому середовищі. Виявлено, що стрімкий розвиток цифрових технологій та активне застосування Інтернету, поряд із численними перевагами, породжують і значну кількість викликів у сфері захисту авторських прав.

У роботі [4] розглянуто та проаналізовано проблеми, з якими стикаються власники авторських прав через обхід законів людьми задля незаконного доступу до контенту, а також розглянуто судові заходи в цифрову епоху, які залишаються невирішеними. У статті наведено деякі рішення та ідеї, які можна використати для регулювання порушень цифрових авторських прав для PDF-документів.

У роботі [19] проаналізовано переваги різних перетворень для вибору кращих комбінацій для вбудовування водяних знаків і зазначено, що методи додавання водяних знаків, що містять дискретне косинусне перетворення DCT (англ. *Discrete Cosine Transform*), забезпечують кращу стійкість до потенційних атак на основі стиснення PDF-файлів за алгоритмом JPEG (англ. *Joint Photographic Experts Group*), дискретне хвильове (вейвлет) перетворення DWT (англ. *Discrete Wavelet Transform*) має сильне енергетичне ущільнення з властивостями геометричної інваріантності для захисту від геометричних атак, тоді як розкладання за сингулярним значенням SVD (англ. *Singular Value Decomposition*) забезпечує стабільність, інваріантність пропорцій та інваріантність обертання, а також забезпечує сильну стійкість до атак на основі шуму. Зокрема, комплексне дослідження дискретного косинусного перетворення для побудови ЦВЗ проведено у роботі [2].

На підставі аналізу останніх досліджень та публікацій щодо проблем захисту PDF-документів випливає, що наразі не існує комплексного методу захисту PDF-документа, зважаючи на його особливі характеристики та подальші призначення. Існує проблема класифікації документів, а також відповідно до цієї класифікації, внесення тих чи інших ЦВЗ і цифрових підписів, які адекватно захищали б документ з точки зору дотримання авторського права та його автентичності. Такі підходи властиві для подальших розробок системи захисту авторських прав для електронних документів і боротьби з нелегальним розповсюдженням електронних PDF-документів з порушенням їх авторського права.

Матеріали та методи дослідження. У роботі використано методи системного аналізу – для дослідження сучасних підходів до захисту авторського права електронних документів і вибору засобів цифрового водяного їх маркування; методи логічного моделювання – під час побудови архітектури програмного комплексу; методи цифрового водяного маркування, криптографічного захисту та електронного підпису – для реалізації механізмів захисту PDF-документів; методи об'єктно-орієнтованого програмування – під час розроблення програмного забезпечення мовою Python; методи експериментального дослідження – для оцінювання ефективності запропонованих засобів захисту за часовими характеристиками, зміною розміру документа та відновлюваністю ЦВЗ.

Результати дослідження та їх обговорення / Research results and their discussion

Методи впровадження ЦВЗ у PDF-документ активно досліджують у контексті захисту авторських прав і кон-

тролю цілісності документів. Виділяють три основні підходи [19]: просторові методи (метадані, текстові вставки); структурні методи (PDF-анотації); частотні методи (DCT, DWT).

Окремо застосовують криптографічні методи захисту службової інформації, що використовуються для вбудовування ЦВЗ, зокрема – алгоритм AES, що забезпечує конфіденційність даних.

Однак більшість наявних рішень використовує тільки один підхід для впровадження ЦВЗ у PDF-документ, що робить їх вразливими до спеціалізованих комбінованих атак.

Метадані PDF як засіб ідентифікації автора. Цей метод використовується як основа стандарту формування PDF-файлів і підтримує такі службові поля [12]: Author; Creator; Producer; Title; Subject; Keywords.

Переваги вказаного вище методу полягають у простоті його реалізації, відсутності впливу на вміст документа та підтримці усіма PDF-редакторами файлів. Проте, завдяки такій простоті реалізації виникають і певні недоліки захисту авторських прав на PDF-документи у користувачів, а саме: легке редагування або видалення інформації про автора документа; відсутність криптографічного захисту службової інформації, що використовується для вбудовування ЦВЗ, а звідси і впливає – низька доказова сила. Наприклад, у таких PDF-редакторах як Adobe Acrobat, PDF-XChange Editor, Foxit PDF Editor, вказані вище службові поля можна змінювати кожному, хто має доступ до відкриття і редагування документа.

Кваліфікований електронний підпис (КЕП). Наразі – це один із найпоширеніших механізмів підтвердження авторства та цілісності електронних документів, що базується на асиметричному шифруванні. До основних переваг цього методу можна віднести [8]: юридична значущість; перевірка цілісності; автентифікація автора.

Проте існують також і недоліки використання КЕП. До них можна віднести [4]: залежність від інфраструктури довірчих послуг; необхідність сертифікатів; проблема довготривалого зберігання підписів; не всі автори мають КЕП.

До основних центрів видачі електронних ключів і сертифікатів можна віднести: Adobe Sign; DocuSign; українські КЕП (ПриватБанк, Дія.Підпис, Вчасно.КЕП, "Військова частина" (для силових структур та військовослужбовців), ТОВ "Дебет Плюс, ТОВ "Центр сертифікації ключів "Україна" тощо).

Видимі водяні знаки. Типові приклади використання видимих водяних знаків у документах [14]: "CONFIDENTIAL"; "DRAFT"; логотип організації; ім'я автора. Переваги таких методів – це очевидна наявність ЦВЗ та психологічний стримувальний ефект для його копіювання та розповсюдження. До недоліків використання видимих ЦВЗ потрібно віднести погіршення зовнішнього вигляду документа та можливість видалення або обрізання ЦВЗ програмними засобами.

Приховані ЦВЗ. До таких ЦВЗ можна віднести декілька їхніх груп згідно з методами їх формування, а саме – текстові та частотні ЦВЗ, що містять різні методи їх створення.

Текстові ЦВЗ. Для створення таких ЦВЗ використовують атрибути форматування символів і їх місце розташування, а саме вони формуються за рахунок [14]: міжсимвольних інтервалів; міжрядкових відстаней; по-

ложення символів; використання невидимих Unicode-символів.

Переваги використання таких методів полягають насамперед у тому, що вони не впливають на сприйняття документа користувачем і тому їх повністю можна віднести до невидимих ЦВЗ. Але основним недоліком такого методу є слабкий захист від будь-яких змін у документі, – ЦВЗ можуть втрачатися під час конвертації документа.

Частотні ЦВЗ. Цей метод формування ЦВЗ полягає у перетворенні текстового матеріалу в зображення, на яке наносяться одним із вказаних методів ЦВЗ [13]:

- DCT (англ. *Discrete Cosine Transform* – дискретне косинусне перетворення) – це ортогональне лінійне перетворення, яке виражає послідовність даних у вигляді суми косинусних функцій;
- DWT (англ. *Discrete Wavelet Transform*) – дискретне вейвлет-перетворення (або дискретне хвильове перетворення), для якого характерна висока стійкість до геометричних перетворень (масштабування, повороту, обрізання);
- SVD (англ. *Singular Value Decomposition*) – розкладання за сингулярними значеннями, яке забезпечує стабільність і стійкість до шумових спотворень.

Переваги частотного методу формування ЦВЗ полягають у високій стійкості таких ЦВЗ до будь-яких спотворень і складності їх виявлення та видалення без наявного програмного забезпечення.

До недоліків вказаних вище методів можна віднести складність їх реалізації, потребу перетворення текстового матеріалу у зображення та відповідно його оброблення за певним алгоритмом. При цьому, якщо PDF-документ містить багато сторінок з текстовою інформацією, то після такого перетворення розмір файлу значно зростає, бо, наприклад, для друку таких документів, потрібно дотримуватись вимог до роздільної здатності та якості документа.

Хмарні сервіси та комерційні системи. Наразі до найвідоміших світових виробників технологій ЦВЗ можна віднести Digimarc, Adobe Content Credentials, Microsoft Information Protection.

1. Особливості формування ЦВЗ і захисту документів в Digimarc полягають у такому [15]: створення ЦВЗ на основі прихованих маркерів; відстеження походження контенту документа; захист авторських прав.
2. Програмний застосунок фірми Adobe – Content Credentials використовує концепцію CAI (англ. *Content Authenticity Initiative*). Це дає змогу [12]: зберігати інформацію про автора; історію редагування документа; походження цифрового контенту.
3. Microsoft Information Protection застосовує такі методи захисту авторських прав [14]: класифікацію документів; цифрові мітки; контроль доступу до документа.

На підставі проведеного аналізу методів створення та використання ЦВЗ для автентифікації та захисту авторських прав у роботі розроблено порівняльну таблицю їхніх параметрів (табл. 1). Проаналізовані в цій таблиці методи або легко модифікуються (метадані), або потребують спеціалізованої інфраструктури довірчих послуг (КЕП), або забезпечують тільки частковий захист авторства (видимі водяні знаки). Тому актуальним є розроблення комбінованого методу підтвердження авторства PDF-документів, який поєднає переваги декількох технологій цифрового маркування. Це твердження є абсолютно логічним і відображає сучасний тренд у сфері інформаційної безпеки. Комбінований метод підтвердження авторства дає можливість нівелювати

недоліки окремих технологій та забезпечити багаторівневий захист PDF-документів.

Табл. 1. Порівняння основних методів створення та застосування ЦВЗ / Comparison of the main methods of creating and applying digital watermarks

Метод	Підтвердження авторства	Стійкість до модифікації	Юридична сила	Складність
Метадані PDF	Частково	Низька	Низька	Низька
Видимий ЦВЗ	Частково	Середня	Низька	Низька
КЕП	Висока	Висока	Висока	Середня
DCT/DWT ЦВЗ	Висока	Висока	Середня	Висока
Комбінований метод	Висока	Висока	Висока*	Висока

Примітка: *за умови поєднання із криптографічним підписом або зовнішнім реєстром.

Програмна реалізація методів підтвердження авторства PDF-документів. Реалізацію програмного забезпечення із впровадження ЦВЗ для PDF-документів і накладення власного цифрового підпису (КЕП) на PDF-документ виконано мовою Python. Графічний інтерфейс побудовано на Tkinter та реалізує багаторівневу структуру із пропозицією вибору доступних ЦВЗ: метадані; видимий ЦВЗ; прихований текст; метод DCT; алгоритм AES; метод Stealth; цифровий підпис.

Для роботи з PDF-документами використовується PyPDF2, для криптографії – AES-реалізація бібліотеки cryptography, а для рендерингу сторінок – популярна бібліотека з відкритим вихідним кодом Poppler. Програма підтримує запуск як у середовищі Python, так і у вигляді EXE-файлу, зібраного за допомогою PyInstaller.

Експериментальне дослідження ефективності запропонованого методу. Експериментальне дослідження проведено задля оцінювання ефективності програмного комплексу під час впровадження різних типів ЦВЗ у PDF-документи, а також визначення впливу структури документа на швидкодію окремих алгоритмів.

Для дослідження ефективності запропонованого методу у роботі було сформовано тестовий набір із 20 PDF-документів різного типу призначення, які умовно поділено на чотири групи: текстові документи (тільки текст); змішані документи (текст із графічними елементами); скановані документи; поліграфічні видання з великою кількістю кольорових зображень.

Характеристики тестових документів наведено в табл. 2. Головними характеристиками PDF-документів є кросплатформність, фіксований макет (вигляд не змінюється на різних пристроях), підтримка інтерактивних елементів та високий рівень безпеки.

Табл. 2. Характеристики досліджуваних PDF-документів / Characteristics of the PDF documents under study

Група PDF	Кількість сторінок	Розмір файлів	Особливості
Текстові	5-30	0,2-1,5 МБ	Тільки текст
Змішані	10-50	2-10 МБ	Текст та рисунки
Скановані	10-100	8-35 МБ	Растрові сторінки
Поліграфічні	5-40	15-80 МБ	Високоякісні кольорові ілюстрації для типографського друку

Під час експерименту оцінювалися такі основні показники: T_i – тривалість відкриття документа; T_e – три-

валість збереження модифікованого документа; T_s – тривалість вбудовування ЦВЗ; T_r – тривалість зчитування ЦВЗ.

Тоді загальна тривалість оброблення документа становитиме:

$$T_{\Sigma} = T_l + T_e + T_s + T_r \quad (1)$$

Окрім часових характеристик, оцінювалися інші параметри PDF-документа, зокрема – приріст розміру PDF-файлу після внесення ЦВЗ

$$\Delta S = \frac{S_i - S_0}{S_0} \cdot 100, \% \quad (2)$$

де: S_0 – розмір початкового PDF-файлу; S_i – розмір після внесення змін ЦВЗ у PDF-файл.

Також оцінювався коефіцієнт відновлення документа (R) після зчитування ЦВЗ, який можна подати у вигляді такого співвідношення:

$$R = \frac{N_v}{N_z} \cdot 100, \% \quad (3)$$

де: N_v – кількість елементів документа, що після вилучення ЦВЗ повністю відповідають оригіналу (кількість символів або бітів, коректно відновлених під час зчитування); N_z – загальна кількість контрольованих елементів (кількість символів або бітів, вбудованих у документ). При $R = 100$ % свідчить про те, що цифровий водяний знак після його зчитування повністю відновлений.

Для усіх проведених експериментів, із впровадженням ЦВЗ у PDF-документи, значення коефіцієнта відновлення становило $R = 100$ %, що свідчить про повне відновлення інформації ЦВЗ.

Результати дослідження середньої тривалості виконання операцій впровадження та зчитування ЦВЗ у PDF-документ наведено у табл. 3.

Табл. 3. Дослідження середньої тривалості операцій впровадження та зчитування ЦВЗ у PDF-документ / Study of the average time of operations for implementing and reading a digital watermark into a PDF document

Метод	Текстовий	Змішаний	Сканований	Поліграфічний
Metadata	12	14	15	16
Hidden Text	58	64	71	74
Visible Watermark	81	96	112	128
DCT	132	198	426	514
AES	72	76	95	108
Stealth	86	92	98	105
Цифровий підпис	142	149	158	167

Примітка: усі значення в таблиці наведено у мілісекундах.

Важливим параметром під час аналізу документів з ідентифікатором авторського права у вигляді ЦВЗ є зміна його розміру до і після введення ЦВЗ. Зазвичай цей параметр залишається майже незмінним після впровадження ЦВЗ на основі використання векторних зображень, що наведено у табл. 4.

Табл. 4. Зміна розміру PDF-файлу після внесення ЦВЗ / Resizing a PDF file after adding a digital watermark

Метод	Середнє збільшення розміру файлу, %
Metadata	0,2
Hidden Text	0,4
Visible Watermark	1,1
DCT	7,8
AES	0,1
Stealth	0,3
Цифровий підпис (Signature)	1,9

Обговорення отриманих результатів. За результатами проведеного дослідження встановлено, що найменшу тривалість виконання мають алгоритми впровадження ЦВЗ у метадані документа та прихований текст. Найбільш ресурсомістким виявився метод DCT, що можна пояснити потребою перетворення PDF-сторінок у растрові зображення, виконання дискретного косинусного перетворення та повторного формування документа.

При цьому застосування криптографічного захисту даних алгоритмом AES практично не впливає на розмір PDF-документа, а для накладання цифрового підпису характерне помірно збільшення тривалості оброблення та розміру файлу.

Методам отримання метаданих та прихованих анотацій характерна висока швидкість, але низька стійкість. Методи DCT та Stealth забезпечують високу прихованість ЦВЗ, але потребують більших обчислювальних витрат та часу на їх оброблення, що відображено у табл. 3. Також встановлено, що вони вносять незначні, на перший погляд непомітні, спотворення в документі. При цьому розмір файлу значно зростає, якщо PDF-документ містить велику кількість сторінок. Це пов'язано з перетворенням векторного формату у растровий з високою роздільною здатністю для подальшого друку.

Цифровий підпис забезпечує незалежний криптографічний рівень захисту авторства документа, що підвищує загальну безпеку системи. При цьому для інтеграції програмного продукту з вітчизняними надавачами послуг сертифікації ЦЕП планується доповнити його методом внесення цифрових підписів від українських КЕП (ПриватБанк, Дія.Підпис, Вчасно.КЕП тощо).

Для комплексного оцінювання ефективності запропонованих методів цифрового водяного маркування, окрім часових характеристик, доцільно враховувати також параметри якості, зокрема – стійкість до зовнішніх впливів, рівень прихованості, криптостійкість та юридичну значущість. Порівняльну характеристику зазначених параметрів наведено в табл. 5.

Табл. 5. Порівняльні характеристики параметрів, що впливають на якість ЦВЗ / Comparative characteristics of parameters affecting the quality of digital watermarks

Параметр якості	Метадані	DCT	AES	Stealth	Підпис
Стійкість	низька	висока	висока	висока	дуже висока
Прихованість	низька	висока	середня	дуже висока	
Криптостійкість	низька	середня	висока	висока	
Потенційна доказова значущість	низька	середня	середня	середня	

На підставі проведених спостережень експериментального дослідження встановлено, що не усі методи створення та впровадження ЦВЗ у PDF-документ можуть забезпечувати відповідні якісні показники для ідентифікації авторства документів. Зокрема, це видно з табл. 5, де метадані слугують тільки пересторогою для того, щоб вказати користувачам, що документ створений певним автором, зазначеним у його параметрах. Але у деяких випадках і для конкретних документів цього й не вимагається. Наприклад, для таких документів, як договори, у юридичній практиці достатньо електронного цифрового підпису, що завіряє юридичну чи фізичну особу на документі. Тому надалі, за вдоскона-

лення програмного продукту, потрібно також впроваджувати категорію класифікації документів, наприклад: наукова стаття, монографія, дисертація чи дипломна робота або договір. Для кожного документа доцільно розробляти свою стратегію чи політику захисту і за вибору класу документа програма має автоматично для нього формувати тип захисту автентифікації чи авторства документа: сукупність ЦВЗ чи навіть КЕП (як для договорів).

Загальну схему інформаційної технології впровадження ЦВЗ у PDF-документ у вигляді наведеного алгоритму вибору та послідовності застосування ЦВЗ і КЕП зображено на рис. 1. Перевірка наявності ЦВЗ, або цифрового підпису у PDF-документі реалізується також програмним методом, для цього достатньо завантажити документ у програму і вибрати будь-який із запропонованих у ній методів внесення/перевірки ЦВЗ, або цифрового підпису (Signature). Запропонований на рис. 1 алгоритм дає змогу впроваджувати у PDF-документи комбіновані ЦВЗ, як видимі, так і невидимі, змінювати параметри формування ЦВЗ, накладати на документ цифровий підпис, що засвідчує його автора, а також надалі зчитувати цю інформацію програмним методом.

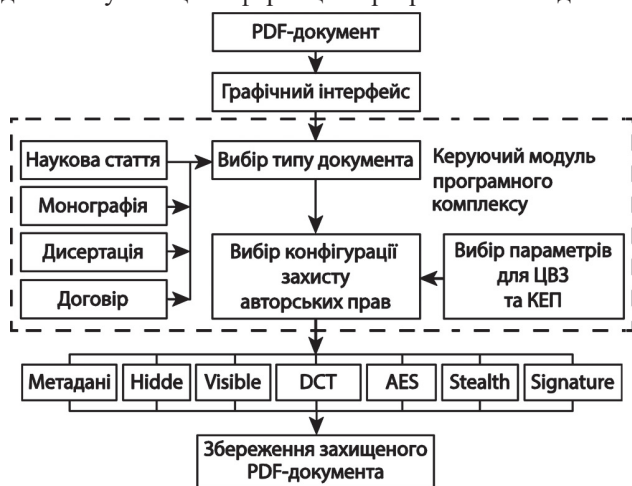


Рис. 1. Алгоритм вибору та послідовності застосування ЦВЗ програмним методом для PDF-документів / Algorithm for selecting and applying digital watermarks programmatically for PDF documents

Взаємодію модулів захисту авторських прав за допомогою введення у PDF-документ ЦВЗ та КЕП наведено на рис. 2. Як видно з цього рисунку, користувач може обирати цей чи інший метод впровадження ЦВЗ за допомогою програмних модулів, а також використовувати криптографічний захист ключів для подальшого зчитування захищених авторських документів. Цифровий підпис, як окремий модуль, має перевагу у тому, що явно вказує на авторство документа, що дає змогу протидіяти атакам на відмову від зобов'язань. Отже, можна до певного класу чи типу PDF-документа застосовувати комбіновані методи захисту авторського права, вибираючи не тільки один із запропонованих методів, а декілька, в т.ч. із цифровим підписом. Це підвищує ефективність захисту таких документів та сприяє подальшому визначенню їх авторства у спірних випадках чи в судовому порядку вирішення проблем авторства того чи іншого документа. На підставі отриманих в роботі результатів дослідження можна робити вибір для впровадження ЦВЗ у PDF-документ, враховуючи певні його особливості, та розробляти свою стратегію чи політику захисту і за вибору класу документа.

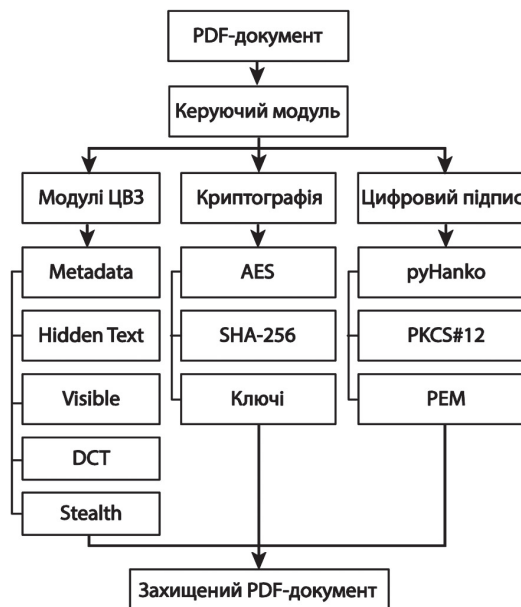


Рис. 2. Функціональна схема модулів захисту авторського права в PDF-документі / Algorithm for selecting and applying digital watermarks programmatically for PDF documents

Отримані результати дослідження показують, що цифровий водяний знак та електронний підпис виконують різні, але взаємодоповнювальні функції у захисті авторства PDF-документа. Цифровий водяний знак забезпечує можливість ідентифікації авторства та прихованого або відкритого маркування документа, тоді як електронний підпис забезпечує автентифікацію підписувача та контроль цілісності підписаних даних. При цьому зміна підписаних даних PDF-документа після накладання цифрового підпису, зокрема – модифікація або видалення вбудованого цифрового водяного знака, має призводити до невідповідності підписаних даних і, відповідно, виявлятися під час перевірки дійсності підпису. Отже, поєднання ЦВЗ та ЕЦП дає змогу сформувати взаємодоповнювальний механізм захисту, у якому ЦВЗ виконує функцію маркування та підтвердження авторства, а ЕЦП – функцію контролю цілісності та автентичності документа.

Вибір конкретного поєднання зазначених механізмів можна здійснювати з урахуванням класу та призначення PDF-документа, що розширює функціональні можливості програмного комплексу та створює передумови для подальшої автоматизації вибору засобів захисту авторства PDF-документа.

Обговорення результатів дослідження. У дослідженні [1] автори проаналізували DCT та DWT методи створення та впровадження водяних знаків на зображеннях і захист їх від різних типів атак, спрямованих на модифікацію документа. При цьому виявлено, що метод DCT стійкіший до подальшої компресії зображення (атак стиснення JPEG), а метод DWT – до атак деформації (обертання, обрізування) зображень. Так, PDF-документи у процесі свого подальшого використання в переважній більшості можуть підлягати процесу стиснення (особливо растрові документи), а не деформації, що підтверджує доцільність використання саме DCT-методу цифрового водяного маркування у запропонованому програмному засобі.

У роботі [7] автор аналізує різні методи захисту PDF-документів, зокрема, основну увагу приділено принципам введення стеганографії та криптографії у про-

токоли безпеки PDF-документів. Але в ній не описано механізмів захисту авторства документа, тому стаття має оглядовий характер методів захисту PDF-документа, а не його авторства.

У дослідженні [10] наведено сучасні стандарти використання метаданих, зокрема – для створення, зберігання, виявлення та повторного використання дослідницьких даних у репозиторіях різних університетів. Такий підхід добре використовувати для пошуку PDF-документів, але він має вразливості під час їх ідентифікації, тому що метадані може змінити користувач, який має доступ до PDF-документа, що знижує їх надійність як єдиного засобу підтвердження авторства.

У праці [3] наведено цікавий підхід до виявлення авторства документів на підставі порівняння стильово-сумісного сумнівного тексту з відомими творами автора, завдання, яке є особливо складним в історичних епохах з частковою достовірністю. Але, на жаль, такі підходи прийнятні тільки для визначення авторства переважної більшості творів відомих літераторів, а не електронних документів загального призначення. Тому такий підхід семантичного аналізу тексту не підлягав розгляду.

У роботі [5] автори аналізують методи впровадження цифрових підписів в електронні документи. Вони підкреслюють основну вимогу до технології реалізації цифрового підпису, яка полягає у тому, що має бути практичне забезпечення копіювання цифрових підписів у надійному сховищі для подальшого арбітражу можливих суперечок. Такі методи автентифікації та ідентифікації авторів можна використовувати і в нашому дослідженні, впровадивши надалі підтримку вітчизняних стандартів сертифікації цифрових підписів. Але реалізація такої можливості потребує інтеграції із чинною інфраструктурою кваліфікованих надавачів електронних довірчих послуг та дотримання вимог національних стандартів.

Проведене обговорення результатів дослідження підтвердило доцільність розроблення запропонованого програмного комплексу для захисту авторського права PDF-документів. Аналіз сучасних наукових праць показав, що наявні дослідження переважно зосереджені на окремих методах цифрового водяного маркування, криптографічного захисту службової інформації про авторство документа, використання метаданих або цифрового підпису, тоді як запропонований у роботі підхід об'єднує зазначені механізми в єдиній програмній системі. Це забезпечує комплексний захист електронних документів, розширює функціональні можливості наявних рішень та створює основу для подальшого розвитку інтелектуальних систем автоматизованого вибору методів захисту залежно від типу PDF-документа.

За результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – отримала подальший розвиток комплексна система захисту авторського права PDF-документів, яка, на відміну від відомих, поєднує методи цифрового водяного маркування та електронний підпис в єдиному програмному засобі з можливістю експериментального оцінювання їх ефективності, що дає змогу підвищити стійкість такого документа до несанкціонованої модифікації, підроблення та видалення засобів автентифікації.

Практична значущість результатів дослідження – можна використати для підвищення рівня захисту ав-

торського права PDF-документів у видавничій діяльності, закладах вищої освіти, наукових установах та системах електронного документообігу шляхом застосування розробленого програмного комплексу, який забезпечує комплексне використання ЦВЗ, криптографічного захисту та електронного підпису для підтвердження авторства, забезпечення цілісності електронних документів і протидії їх несанкціонованому копіюванню та модифікації.

Висновки / Conclusions

Розроблено комплексну систему захисту авторського права PDF-документів на основі поєднання ЦВЗ, електронного підпису та його криптографічного захисту й експериментально оцінено ефективність запропонованих засобів захисту електронних документів, що дасть змогу підвищити стійкість такого документа до несанкціонованої модифікації, підроблення та видалення засобів автентифікації. За результатами проведеного дослідження можна зробити такі основні висновки.

1. Проаналізовано сучасні методи захисту авторського права PDF-документів, що дало змогу встановити доцільність комплексного використання ЦВЗ, криптографічного захисту й електронного підпису для підвищення рівня інформаційної безпеки електронних документів.
2. Розроблено програмний комплекс, який реалізує декілька незалежних методів цифрового водяного маркування (метадані, видимі водяні знаки, приховані анотації, DCT, AES та Stealth), а також модуль цифрового підпису PDF-документів, який забезпечує автентифікацію підписувача та контроль цілісності підписаного документа, і можна використовувати як засіб підтвердження авторства.
3. Проведено експериментальне дослідження ефективності запропонованих методів, за результатами якого встановлено їх працездатність та можливість використання для підтвердження авторства, забезпечення цілісності документів і підвищення стійкості до несанкціонованої модифікації.
4. Встановлено, що комплексне використання ЦВЗ й електронного підпису забезпечує більш високий рівень захисту PDF-документів порівняно із застосуванням окремих методів, що підтверджує доцільність запропонованого підходу.
5. Визначено, що перспективним напрямом подальшого дослідження є розроблення системи автоматичного вибору методів захисту залежно від типу електронного документа та створення інформаційної системи моніторингу поширення PDF-документів у мережі Інтернет для виявлення можливих порушень авторського права.

Декларація про використання засобів ШІ. Програмні засоби ChatGPT та Grammarly було використано авторами виправдано і винятково для лінгвістичного редагування, стилістичного коригування та перефразування окремих фрагментів тексту. Автори критично перевірили, систематизували й остаточно затвердили зміст роботи, беручи на себе повну відповідальність за поданий матеріал.

References

1. Al-khafaji, Hiba, Al-Himyari, Bayadir, & Hussain, Noor Fadel. (2024). Techniques for Digital Watermarking in Images: A Review. *Journal of University of Babylon for Pure and Applied Sciences*, 32(1), 93–107. <https://doi.org/10.29196/yedrt588>
2. Bohra, Krishna Kumar, & Soni, Vinod Kumar. (2024). Invisible watermarking using Discrete Cosine Transform (DCT): A comprehensive exploration. *World Journal of Advanced Research*

- and *Reviews*, 24(2), 2639–2645. <https://doi.org/10.30574/wjarr.2024.24.2.3623>
3. Boriceanu, Ioana-Roxana, & Dinu, Liviu P. (2026). Style as Signature: Profile-Based Authorship Verification of Mihai Eminescu's Journalistic Corpus. *Conference: Proceedings of the 10th Joint SIGHUM Workshop on Computational Linguistics for Cultural Heritage, Social Sciences, Humanities and Literature*, 1, 102–110. <https://doi.org/10.18653/v1/2026.latechclfl-1.10>
 4. Dawar, Kanika, & Sudarshan, Ashwin. (2021). Copyright Protection in Digital Era. *International Advanced Research Journal in Science, Engineering and Technology*, 8(6), 611–616. <https://doi.org/10.17148/IARJSET.2021.86105>
 5. Harshit Jaiswal, Rishav Kumar, Himanshu Sharma, & Divyashikha Sethia. (2025). SecureXfer: Secure NFC RSA Mobile-based Framework for Digital Signing of Documents. *2025 International Conference on Next Generation Information System Engineering (NGISE)*, 1, pp. 1–6. <https://doi.org/10.1109/NGI-SE64126.2025.11085222>
 6. ISO 32000-2:2020. Document management – Portable document format Part 2: PDF 2.0. URL: https://www.iso.org/standard/75839.html?_cf_chl_f_tk=LX0GzdNRAisotRU1qwEnruFrSNyCRF9NoKH7n_LG3C4-1783276294-1.0.1.1-n66nXCV3wAcscYqAXAZ6fUez0ljmchHgQ.05ktXt74
 7. Jiang, Linfeng. (2023). A research on PDF protection mechanisms. *Applied and Computational Engineering*, 16(1), 159–165. <https://doi.org/10.54254/2755-2721/16/20230852>
 8. Kolb, O. S., Pyroha, I. S., & Dzhuhan, V. V. (2025). Aspects of copyright protection on the Internet. *Analytical and Comparative Jurisprudence*, 1(5), 204–208. <https://doi.org/10.24144/2788-6018.2025.05.1.35>
 9. Lin, Weyde. (2022). Digital Signature. *Trends in Data Protection and Encryption Technologies*, 77–81. https://doi.org/10.1007/978-3-031-33386-6_15
 10. Moscato, Vincenzo. (2023). Metadata Standard for Continuous Preservation, Discovery, and Reuse of Research Data in Repositories by Higher Education Institutions: A Systematic Review. *MDPI (Multidisciplinary Digital Publishing Institute)*, 14(8), article ID 427. <https://doi.org/10.3390/info14080427>
 11. Naem, Saif Aldeen S., & Hameed, Sarab M. (2025). Digital watermarking techniques, challenges, and applications: A review. *Mesopotamian Journal of CyberSecurity*, 5(2), 1–24. URL: https://www.researchgate.net/publication/393795938_Digital_watermarking_techniques_challenges_and_applications_A_review
 12. Overview of security policies in Adobe Acrobat. Last updated 06/24/2026. URL: <https://helpx.adobe.com/ua/acrobat/desktop/protect-documents/security-policies/security-policy.html>
 13. Sabat, V. I., & Bohonis, O. O. (2025). Formal Methods for Describing and Determining the Parameter Values of Copyright Protection Systems. *Science and Technology Today*, 8(49), 1674–1688. [https://doi.org/10.52058/2786-6025-2025-8\(49\)-1673-1688](https://doi.org/10.52058/2786-6025-2025-8(49)-1673-1688)
 14. Sabat, V. I., & Bohonis, O. O. (2025). Information Technology for Developing an Algorithm for Embedding Digital Watermarks into the Digital Environment. *Naukovi Zapysky*, 1(70), 21–34. <https://doi.org/10.32403/1998-6912-2025-1-70-21-34>
 15. Saira Yaqub, Hafiz Abdui, & Haseeb Khalid. (2022). Instantaneous Documents Authentication and Verification based on Robust Digital Signature 4. *International Journal of Computational Intelligence in Control*, 14, 229–235. <https://doi.org/10.13140/RG.2.2.12437.70886>
 16. Shaik Abdul Subhani, Lingala Akhila, Ganta Arun, & Jadhav Sankindhar. (2024). A Invisible Watermark For Digital Images. *International Journal of Advanced Research in Science, Engineering and Technology*, 11, 21748–21754. URL: <https://www.ijarset.com/upload/2024/april/18-sahubhani-22.pdf>
 17. Stanešić, J., & Morić, Z. (2025). Digital signatures and their legal significance. *Edelweiss Applied Science and Technology*, 9(1), 403–412. <https://doi.org/10.55214/25768484.v9i1.4154>
 18. Supiyandi, S., & Purnomo, A. (2018). Application of Invisible Image Watermarking. *International Journal of Engineering & Technology*, 7(3.2), 760–762. <https://doi.org/10.14419/ijet.v7i3.2.18749>
 19. Varghese, Justin, Hussan, Omer Bin, Subash, Saudia, & Razak, Abdul. (2023). An effective digital image watermarking scheme incorporating DCT, DFT and SVD transformations. *PeerJ Computer Science*, 1–26. <https://doi.org/10.7717/peerj-cs.1427>
 20. Wang, Ziyu Hongxia, & Han, Soung Yuan. (2024). A robust PDF watermarking scheme with versatility and compatibility. *Multimedia Tools and Applications*, 83, 64341–64367. URL: <https://link.springer.com/article/10.1007/s11042-024-18151-w>
 21. Yexing Zgang, Zihou Wang, Zhaoguo Wang, & Chuanyi Liu. (2022). A Robust and Adaptive Watermarking Technique for Relational Database. *Cyber Security*, article ID 1506, 3–26. URL: https://link.springer.com/chapter/10.1007/978-981-16-9229-1_1?fromPaywallRec=true

V. I. Sabat, O. O. Bohonis

Lviv Polytechnic National University, Lviv, Ukraine

COPYRIGHT PROTECTION OF PDF DOCUMENTS USING DIGITAL WATERMARKS AND DIGITAL SIGNATURES

The paper addresses the problem of copyright protection for electronic documents distributed in Portable Document Format (PDF). Existing protection mechanisms, such as password-based access control and standard PDF encryption, do not provide sufficient resistance against attacks aimed at removing or modifying security features used to verify document authenticity. Therefore, the development of multi-layered protection systems combining different information hiding and security techniques remains an important research task. The widespread use of PDF documents in publishing, scientific communication, business processes, legal practice, and electronic document management has significantly increased the need for reliable mechanisms that prevent unauthorized modification, forgery, and copyright infringement. This creates a demand for software solutions capable of ensuring document authenticity, integrity, and authorship verification. A software system for multi-layer protection of PDF documents has been developed based on the combined application of digital watermarking, cryptographic encryption, and steganographic methods. The proposed software integrates several independent protection techniques, including PDF metadata, visible watermarks, hidden annotations, Discrete Cosine Transform (DCT)-based watermarking, AES encryption, stealth steganography, and a digital document signing module. The software prototype was implemented in Python using the PyPDF2, OpenCV, cryptography, and Tkinter libraries. The developed approach improves document resistance to unauthorized access, modification, and copyright violations through the combined use of complementary protection mechanisms. The characteristics, advantages, and limitations of each watermarking technique are analyzed. Experimental evaluation demonstrates the robustness of the proposed methods against attacks targeting watermark detection and removal, while the obtained results confirm the effectiveness of combining multiple protection techniques according to the document class and its intended application. The proposed approach may serve as the basis for developing intelligent systems for automated copyright protection of electronic documents.

Keywords: information technology; electronic document security; information security; cryptographic protection; document authenticity; document integrity; digital identification; steganography.