DOI: 10.18372/2225-5036.31.20568

МЕТОДИ ІНТЕГРАЦІЇ ПРИХОВАНИХ ПОВІДОМЛЕНЬ ДО ВІЗУАЛЬНОГО ПОДАННЯ КОНФІДЕНЦІЙНОГО ДОКУМЕНТУ

Микола Сніжинський[1], Владислав Ковтун[2], Марія Ковтун[3] , Юлія Кіндрат[4]

[1]Адміністрація Державної служби спеціального зв'язку та захисту інформації України
[2] ТОВ «САЙФЕР ІТ», Україна
[3]Державний університет «Київський авіаційний інститут», Україна
[4] Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Україна

СНІЖИНСЬКИЙ Микола Миколайович
Рік та місце народження: 1990 рік, с. Стаївка, Львівська область, Україна. Україна.
Освіта: Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», 2012 рік.
Посада: заступник керівника підрозділу з формування та реалізації державної політики у сфері захисту інформації та електронних довірчих послуг у закритих системах Адміністрації Державної служби спеціального зв'язку та захисту інформації України з 2020 року.
Наукові інтереси: інформаційна безпека, реагування на інциденти інформаційної безпеки, інфраструктура відкритих ключів.
E-mail: smm_mail_ua@proton.me
ORCID: 0009-0008-3553-6880

КОВТУН Владислав Юрійович, к.т.н., доцент
Рік та місце народження: 1978 рік, с. Петрове, Кіровоградська обл., Україна.
Освіта: Харківський військовий університет, 2000 рік.
Посада: директор ТОВ «САЙФЕР ІТ».
Наукові інтереси: криптографічні перетворення на алгебраїчних кривих.
Публікації: більше 60 наукових публікацій, серед яких монографії, наукові статті та патенти на винаходи.
E-mail: vlad.kovtun@cipher.com.ua
ORCID: 0000-0002-4303-3510

КОВТУН Марія Григорівна, к.т.н.
Рік та місце народження: 1989 рік, м. Львів, Україна.
Освіта: Національний авіаційний університет, 2011 рік.
Посада: старший науковий співробітник НДЛ протидії кіберзагрозам в авіаційній галузі Державний університет «Київський авіаційний інститут».
Наукові інтереси: асиметрична криптографія, постквантова криптографія.
Публікації: більше 20 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях та патенти.
E-mail: mg.kovtun@gmail.com
ORCID: 0000-0002-3021-2659

КІНДРАТ Юлія Русланівна.
Рік та місце народження: 2003 рік, м. Тернопіль, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2024 рік.
Посада: курсант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» з 2021 року.
Наукові інтереси: криптографія, інформаційна безпека, захист даних у цифровому середовищі.
E-mail: kindrat0407@gmail.com
ORCID: 0009-0006-7054-5323

Анотація. *У статті досліджено підходи до інтеграції прихованих повідомлень у візуальне подання конфіденційних документів для забезпечення контрольованого поширення. Розглянуто практичні аспекти побудови цифрових водяних знаків (ЦВЗ), які можуть зчитуватися з електронної або паперової версії документа навіть після його друку, сканування чи фотографування. Описано методи формування повідомлення, його шифрування, завадостійкого кодування та графічного представлення. Проаналізовано сучасні методи виявлення і зчитування ЦВЗ із використанням штучного інтелекту, а також наведено порівняння класичних кодів (Луна, CRC, Гемінга, Ріда-Соломона) для забезпечення стійкості до спотворень.*

Ключові слова: *інформаційна безпека, цифрові водяні знаки, стеганографія, завадостійке кодування, ідентифікація витоків, шифрування*

Вступ. Робота з документами, що містять конфіденційну інформацію, вимагає чіткого визначення кола осіб, які матимуть до нього доступ, з урахуванням рівня обмеження доступу до відомостей, що містяться в документі. Однією з ключових вимог є забезпечення контрольованого поширення документа, що, у свою чергу, передбачає можливість: 1) обмеження доступу до документа

лише для визначеного кола осіб; 2) відстеження джерела витоку у разі несанкціонованого розповсюдження; 3) автентифікації створювача кожного примірника.

Життєвий цикл документа, який містить конфіденційну інформацію, може передбачати його неодноразове друкування та сканування на різних пристроях, з метою доведення його змісту до усього кола визначених осіб.

При цьому, чим більше коло осіб має доступ до документа, тим важче визначити на якому етапі відбувся витік, у разі його настання.

У зв'язку з цим актуальною науково-практичною задачею, що має теоретичне і практичне значення, є розробка методів, які забезпечують приховане маркування кожного примірника документа, що дозволяє:

– визначити джерело створення (користувача або пристрій);

– встановити час формування конкретного примірника;

– зберігати приховану інформацію навіть після друку або повторного сканування;

– забезпечити автентичність та конфіденційність прихованої інформації;

– не порушувати візуальне сприйняття документа.

Метою є визначення джерела створення повідомлення, встановлення часу формування конкретного примірника, зберігання прихованої інформації після друку і повторного сканування документу та забезпечення автентичності і конфіденційності прихованої інформації без порушення візуального сприйняття документу, за рахунок розробки методів цифрової стеганографії та методів завадостійкого кодування з визначенням і виправленням помилок.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1) Проаналізувати існуючі підходи до приховування і визначення прихованої інформації у візуальну складову документу з використанням візуальної стеганографії.

2) Запропонувати нові чи удосконалити існуючі методи до приховування і визначення інформації у візуальну складову документу.

3) Запропонувати нові чи удосконалити існуючі методи до визначення і виправлення помилок, під час відтворення прихованої інформації із візуальної складової документу.

4) Запропонувати нові чи удосконалити існуючі методи до забезпечення конфіденційності прихованої інформації у візуальній складовій документу.

Проведений аналіз існуючих методів приховування інформації, дозволив сформувати класи методів цифрової стеганографії, які дозволяються досягати визначену мету, у табл. 1.

Таблиця 1

Визначення класів візуальних методів цифрових цифрової стеганографії

Клас методу	*Опис*
Візуальний водяний знак	Візуально слабо помітні знаки чи написи, видимі при перегляді на моніторі або на папері після друку.
Модифіковані шрифти і форматування тексту	Візуальні мікрозміни у відстанях між літерами, абзацами, пробілами та використання різних/специфічних шрифтів для деяких символів, груп символів, слів, речень тощо, із використанням методів штучного інтелекту (ШІ).
Написання інших версій тексту, без зміни суті	Формування всього тексту, частин тексту, речень, фраз чи лише слів відмінною для кожного примірника документу, з використанням методів лінгвістичної стеганографії на основі довідників або моделей ШІ [28].

Постановка задачі

Приховані повідомлення можуть інтегруватися до візуального подання документа на різних етапах життєвого циклу:

– етапі його створення;

– та/або на етапі сканування його паперової версії шляхом інтеграції до створюваного візуального подання в електронній формі (сканкопії);

– та/або на етапі друкування паперового примірника, шляхом нанесення прихованого повідомлення на паперову версію документа.

Згідно поставленої мети, приховане повідомлення має відповідати наступним вимогам:

– Містити дату, час (з точністю до хвилини) та ідентифікатор обладнання (робочого місця), на якому воно створене.

– Бути непомітним/нечитабельним для кореспондентів та зловмисника.

– Зчитуватись, з використанням спеціального програмного забезпечення, з візуального подання (в т.ч. фотографії/сканкопії) оригінального документа на паперовому носії, або виведеного на екран монітора (без необхідності доступу до оригінального документа).

– Бути захищеним від підробки.

– Бути конфіденційним.

– Мати можливість почергової інтеграції кількох різних прихованих повідомлень до одного документа на різних етапах його життєвого циклу (приведених вище).

– Можливість незалежного зчитування наявних окремих прихованих повідомлень, інтегрованих до одного документа.

Особливості вбудовування та зчитування прихованого повідомлення до візуального подання документа накладають суттєві обмеження на використовувані класи методів.

Так, стеганографічні методи, засновані на приховуванні стегоконтейнера у тексті документа за допомогою зміни шрифтів і форматування тексту, тощо для даного випадку не застосовні тому, що інтеграція прихованого повідомлення може здійснюватися саме до готового документу, після набору його тексту та друку. Однак може бути розглянуто, як варіант для подальшого розвитку систем захисту.

З іншого боку, використання класичних методів стеганографії шляхом приховування даних у просторовій області зображень, типу заміни найменш значущого біта, псевдовипадкового інтервалу, псевдовипадкової перестановки, заміни палітри, приховування даних у частотній області зображень методами дискретного косинусного перетворення, розширення спектра тощо, суттєво ускладнене необхідністю зчитування стегоконтейнера із візуального подання документа, без доступу до його оригіналу та можливими спотвореннями під час поступових друків документу і наступних його сканувань та неможливістю аналізу документів, для яких були встановлені несанкціоновані витоки через фотографування і зйомку на відео.

Методи стеганографії, що будуються на написанні інших версій вихідного тексу документу, потенційно можуть біти використовувані, однак потребують верифікації та підтвердження відповідності сенсу документу з боку відповідальної особи. Не зважаючи на допомогу з боку ШІ для побудови інших версій документу, існують методи виявлення написання текстів за допомогою ШІ та принципова неможливість застосування для деяких формалізованих документів. Однак може бути розглянуто, як варіант для подальшого розвитку систем захисту.

Основна частина дослідження

Аналіз існуючих досліджень і публікацій показав успішне використання механізмів нанесення цифрових водяних знаків (ЦВЗ) крихітними точками, які практично невидимі при звичайному освітленні, їх можна побачити у світлі синього спектру, або при збільшенні чи через модифікації на комп'ютері.

Про існування відстеження ЦВЗ в друкованих документах стало відомо у 2004 році, коли нідерландська влада використала їх для боротьби з фальшивомонетниками [1]. Проте сама технологія візуальних ЦВЗ закладена ще у 1993 році компанією Fuji Xerox Co. Ltd. і описана в патенті США №5515451 під назвою «Image processing system for selectively reproducing documents» [2][3].

Дослідження Electronic Frontier Foundation (EFF): у 2005 році EFF розкрила код, що використовується деякими кольоровими лазерними принтерами для прихованого маркування документів. Вони опублікували керівництво з декодування позначок принтерів DocuColor, яке пояснює, як зчитувати дату, час та серійний номер принтера з таких міток [4]. Список принтерів з мітками від EFF: EFF також створила список принтерів, які додають або не додають такі мітки, щоб допомогти користувачам визначити, чи їхній пристрій використовує цю технологію.

Публікація BBC Future (2017): у статті «Як принтери "стежать" за нами» [5] обговорюється, як ці «мікроточки» використовуються для відстеження джерела друкованих документів, і піднімаються питання конфіденційності, пов'язані з цією технологією.

У 2017 році було виявлено витік секретних документів Агентства національної безпеки США щодо фальсифікації виборів, слідство встановило, що особа, яка мала доступ до таких документів, передала їх копії журналістам, однак документ був не оригінальним PDF документом, а містив зображення друкованої версії, яка потім була відсканована. Скориставшись наявністю ЦВЗ на сканкопії слідством було встановлено час та пристрій, яким ці документи друкувались, а за журналами завдань друку було встановлено особу, яка здійснювала друк у визначений час на вказаному пристрої [6].

Як наслідок, наукова спільнота зацікавилась такими можливостями спеціальних служб, що призвело до дослідження Технічним університетом Дрездена (2018): було проаналізовано 106 моделей принтерів від 18 виробників і виявили чотири різні схеми кодування позначок. Вони розробили інструмент для виявлення та аналізу цих ЦВЗ, а також методи їх анонімізації, щоб підтримати інформаторів у публікації конфіденційної інформації [7].

Публікація в Egyptian Journal of Forensic Sciences (2019): у цій роботі вивчалася унікальність розподілу жовтих точок у різних моделях кольорових лазерних принтерів. Було з'ясовано, що кожен принтер має унікальний шаблон позначок, який залишається постійним з часом, що дозволяє ідентифікувати конкретний пристрій друку [8].

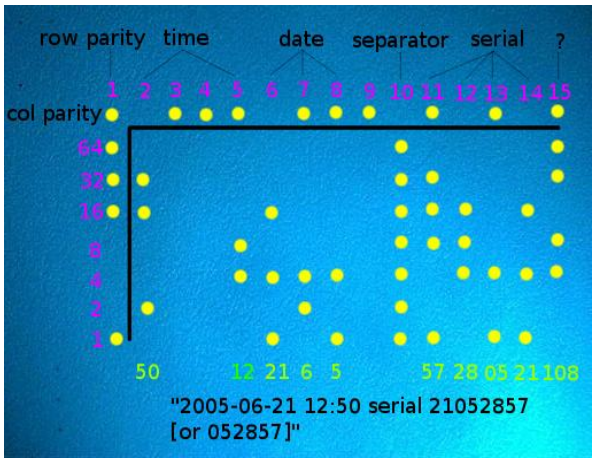

Рис. 1. Узагальнена семантична модель на прикладі точкової сітки Xerox DocuColor 12

Семантична модель алгоритму (рис. 1) передбачає побудову матриці розмірами 8 рядків на

15 стовпців. Сім рядків є степенями двійки та верхній рядок – біт парності (проставляється у разі парної кількості точок у стовпці). За кожним із стовпців закріплена своя роль (дата, час, серійний номер пристрою тощо). Проставлення точок у кожному із стовпців дозволяє відобразити число від 1 до 127.

Одна і та сама сітка друкується неодноразово на всій сторінці паралельно її краям, але із зміщенням сітки одна відносно одної, для кращого відокремлення. Водночас, враховуючи давність технології та доступність алгоритму її роботи у відкритому доступі, вона все ж залишається ефективною та потенційно використовуються для автентифікації джерела інформації і в теперішній час.

Також у конкурсі організованому у 2011 Агентством передових оборонних дослідницьких проектів США група програмістів використала матрицю дрібних повторюваних точок ЦВЗ для успішного «відновлення» п'яти документів подрібнених на 10 000 клаптиків [9][10]. Водночас деталі вищеозначеного алгоритму на цей час не публікувались його розробниками у відкритому доступі та можуть мати певні додаткові функції, які поки не виявлені, але використовуються урядовими організаціями інших країн, яким відомий повний алгоритм створення/виявлення ЦВЗ.

Наведений огляд публікацій, дозволяє зосередитися на способах використання ЦВЗ, як методу автентифікації джерела інформації. З цією метою можливе використання [11]:

– *Вже наявних ЦВЗ*, які накладаються кольоровими і чорно-білими принтерами та багатофункціональними пристроями при роздрукуванні документів.

- Даний підхід дозволяє з мінімальними зусиллями впровадити механізми ЦВЗ.
  - ✓ Для цього необхідно виявити та декодувати наявні ЦВЗ, встановивши унікальний ідентифікатор пристрою та відповідність системного часу пристрою реальному.
  - ✓ У подальшому для підтвердження/спростування друку документів на конкретному пристрої (ідентифікації джерела витоку) та встановлення часу такого друку достатньо здійснити декодування ЦВЗ на виявленому друкованому документі (його візуальному поданні) та співставлення його значень із попередньо декодованими еталонними.
- Серед недоліків цього підходу є:
  - ✓ Необхідність використовувати лише певні моделі принтерів і певних виробників, що суттєво збільшує вартість друку і вартість впровадження такого підходу (необхідністю заміни вже існуючого парку принтерів та багатофункціональних пристроїв).
  - ✓ Несе ризик використання зловмисником відомих методів нанесення ЦВЗ для фальсифікації походження інформації з певного джерела (підміни автентичності) та можливості деактивації ЦВЗ.
  - ✓ Відома підтримка ЦВЗ лише пристроями, які виконують кольоровий друк і, що вони не проставляються під час чорно-білого друку.

– *Розробка власного методу ЦВЗ*, що наносяться на візуальне подання документа певним методом (наприклад матричним) та є **видимими** для людського ока, але які можуть вважатися за несуттєві артефакти, що додалися до зображення під час друку чи скануванні документу.

- Даний підхід вважається найбільш перспективним з боку можливості виявлення несанкціонованого витоку через фотографування і зйомку на відео.
- Серед недоліків цього підходу є можливість видалення таких артефактів під час сканування чи фотографування чи відео зйомки, як навмисно, так і автоматично (буде вважатися, що це подряпини, дефекти принтеру, пил чи бруд, тощо).

– *Розробка власного методу ЦВЗ*, що наносяться на візуальне подання документа певним методом (наприклад матричним) та є **невидимим** для людського ока та нечитабельним для кореспондентів/зловмисника.

- Даний підхід вважається найбільш перспективним з боку можливості виявлення несанкціонованого витоку через розповсюдження документів саме у вигляді, як вони розповсюджуються.
- Серед недоліків цього підходу є складність відслідковування таких артефактів під час несанкціонованого сканування чи фотографування і зйомки на відео.

Розглянемо відомі і можливі методи деактивації ЦВЗ, як навмисні, так і ненавмисні, але які можуть призводити до деактивації ЦВЗ:

1) Вже наявних ЦВЗ.

- ✓ Виключення модуля проставлення ЦВЗ на програмно-апаратному рівні. Потребує дослідження принципів роботи кожної окремої серії друкуючих пристроїв на предмет можливості такого виключення та програмно-апаратну модернізацію кожного окремого пристрою, у разі наявності такої можливості.
- ✓ Використанні для друку паперу з кольоровою заливкою (наприклад жовтою), що потенційно унеможливить виокремлення структури ЦВЗ із загального фону документа. Такий спосіб найменш ресурсоємний, однак використання кольорового паперу (наприклад жовтого) для друку може бути сумнівними рішенням для офіційних документів.
- ✓ Доповнення ЦВЗ випадковими позначками (кольоровими точками, наприклад жовтими), які в подальшому

унеможливлюють достовірне декодування змісту стегоконтейнера. Даний метод «анонімізації» друкованих документів запропонований Стефаном Ешером та його колегами із Дрезденського технічного університету [12],[13]. Він передбачає зчитування і декодування оригінального шаблону ЦВЗ та створення матриці додаткових точок, яка буде виводитись на друк разом оригінальним ЦВЗ спотворюючи його зміст. Однак застосування цього методу передбачає попередній процес калібрування з метою точного співставлення матриці додаткових точок з матрицею оригінального ЦВЗ [14].

2) Власного методу ЦВЗ:

- ✓ Використання інструментів графічних редакторів для прибирання артефактів (подряпин, дефекти принтеру, пил чи бруд, тощо), або інструментів для підвищення контрастності, що призведе до знищення більшості нанесених точок ЦВЗ.
- ✓ Використання спеціалізованих інструментів із ШІ для відновлення зображень, які можуть прибрати артефакти із зображень, що призведе до знищення більшості нанесених точок ЦВЗ.

Вищевикладені методи вбудовування та деактивації ЦВЗ, дозволяє сформулювати кроки запропонованого методу накладання ЦВЗ, який зображено на рис.2:

1. Наявна сторінка (або більше) документу, яка може містити текст або зображення.
2. Отримуємо позначку: дата, час, робоче місце або сеанс.

2.1. Цей етап не обов'язковий. Дану позначку можна надалі використовувати в незашифрованому вигляді, а можна зашифрувати. Серед недоліків зашифровування: оскільки при зворотній схемі декодування можуть бути помилки, зашифрована позначка, під час розшифровування, буде повністю спотворена, і не буде можливості навіть частково отримати дані про позначку.

3. Виконується завадостійке кодування. Позначка (зашифрована або ні) перетворюється у бітову послідовність з корекцією помилок з використанням кодів, для прикладу: Гемінґа (7,4) – виправляє 1 помилку, виявляє 2; CRC– виявляє помилки, не виправляє; Ріда-Соломона (n, k) – дуже стійкий, особливо в сканованих копіях; можна також використати BCH або LDPC коди.

4. Отримана закодована інформація представлена у вигляді символьної послідовності, наприклад, бітової послідовності. І саме на цьому етапі потрібно виробити стратегію вбудовування ЦВЗ у документ.

4.1. Сторінка ділиться на області різної геометричної форми, наприклад, матриці 4×4 або 8×8 блоків), куди заноситься прихована позначка.

4.2. Точки мають знаходитися на світлому контрастному фоні.

4.3. Виділяються інформаційні і не інформаційні зони в межах визначених областей, куди саме буде заноситься прихована позначка. Наприклад, інформаційні точки чи групи точок, знаходяться за межами друкованих символів, а неінформаційні точки чи групи точок, знаходяться в межах друкованих символів, які додаються для протидії методам деактивації ЦВЗ.

4.4. Для можливості зменшення помилок під час зчитування точок, слід один інформаційний символ або біт відображати у одну або кілька груп точок (забезпечується надлишковість). Геометрична форма групи та розподіл груп на сторінці в межах однієї чи кількох областей. Тобто, одна група точок, може бути повторена кілька разів у межах однієї області, або повторена у інших областях. Зазначимо, що розподіл точок у межах повторюваних груп може бути різними (одна і та сама інформація відображається у групи точок з різним розподілом), для протидії методам деактивації ЦВЗ.

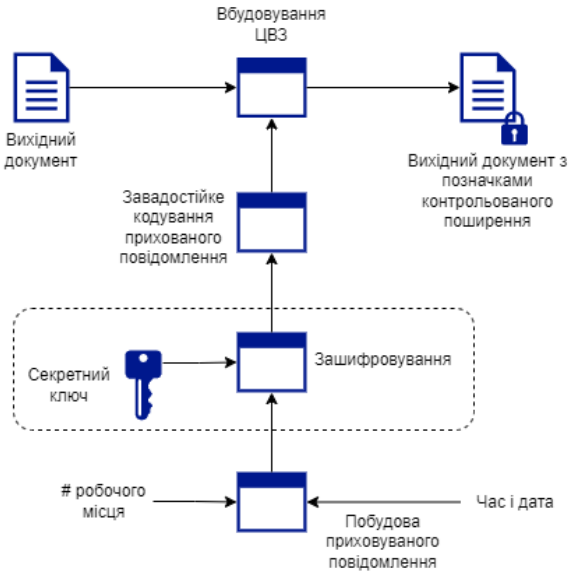

Рис. 2. Графічне зображення схеми додавання ЦВЗ до документа із конфіденційною інформацією

Зазначимо, що саме вбудовування ЦВЗ до вхідного документу, з можливістю подальшого визначення наявності ЦВЗ і його декодування, є досить складною і цікавою задачею, вирішенню якої, у сучасних публікаціях, не приділяється увага.

При вилученні ЦВЗ виконуються наступні дії з документом згідно запропонованому методу, який зображено на рис. 3:

1. Вилучення ЦВЗ. Виконується розпізнавання інформаційних точок на сторінках документа і їх

розподіл згідно областей і груп за попередньо обраним шаблоном на етапі вбудовування.

1.1. Кожна група точок чи кілька груп точок (при наявності надмірності), відображається у певний символ. Виконується перевірка результатів відображення кількох груп точок, на можливі помилки. Тобто чи всі групи відображаються у один і той самий символ, що дозволяє за кількістю співпадінь символів, прийняти рішення про наявність помилки під час вилучення ЦВЗ із документа.

1.2. Для виявлення групи точок і груп за довільним шаблоном, але за визначеним алгоритмом/правилом пропонується використовувати методи ШІ.

2. Виявлення та виправлення помилок у прихованому повідомлені з використанням завадостійких кодів.

2.1. Якщо мітка була зашифрована, то відбувається її розшифровування.

3. Декодування прихованого повідомлення. На цьому етапі може бути 100% отримання правильної мітки, або часткове її отримання, оскільки принтер може додати артефакти, а сканер може не розгледіти всі артефакти, або додати артефакти паперу, або причиною може бути звичайний пил.

4. На основі отриманих даних, можна виявити джерело витоку інформації та ідентифікувати зловмисника, дії якого призвели до витоку.

На Рис. 3 зображено схему вилучення позначок контрольованого поширення документу з конфіденційною інформацією, який було виявлено у неавторизованому джерелі (у зворотному напрямку): вилучення ЦВЗ, виявлення і виправлення помилок з використанням завадостійких кодів, розшифрування приховуваного повідомлення та декодування приховуваного повідомлення для отримання часу і дати, ідентифікатора робочого місця. Після чого можна зрозуміти можливі місця витоку конфіденційної інформації.

Для вилучення і розпізнавання ЦВЗ, як і для деактивації ЦВЗ, у конфіденційних документах (у вигляді зображень), себе добре зарекомендувати методи ШІ, серед яких слід виокремити наступні:

- Згорткові нейронні мережі (CNNs) [15],[16] і їх розвиток у Fast/Faster CNN. Дуже добре себе зарекомендували для аналізу зображень і виявлення в них певних шаблонів. Їх можна натренувати на тестових наборах таких документів, для виявлення ЦВЗ, їх вилучення і розпізнавання.
- Рекурентні нейронні мережі (RNNs), особливо LSTM [17],[18]. Дозволяють дуже добре виявляти певні послідовності чи просторове розташування ЦВЗ у вигляді точок на зображенні документів. Як і попередні мережі слід тренувати на схожому тестовому наборі таких документів.
- Автоенкодери [19]. Дозволяють дуже добре реконструювати вихідне зображення у вигляді тексту без нанесених ЦВЗ, що дозволяє ефективно протидії методам ЦВЗ.
- Генеративно-змагальні нейронні мережі (GANs) [20]. Мають великий потенціал для розрізнення природніх зображень без ЦВЗ і зображень з наявними ЦВЗ, тому такі мережі погано виявляють ЦВЗ.
- Мережі-трансформери [21]. Останнім часом показують дуже гарні результати при вирішенні задач комп'ютерного зору і розпізнаванні образів. Дозволяють виявляти ЦВЗ та здійснювати їх подальше розпізнавання. Ефективно виконують задачі деактивації ЦВЗ.

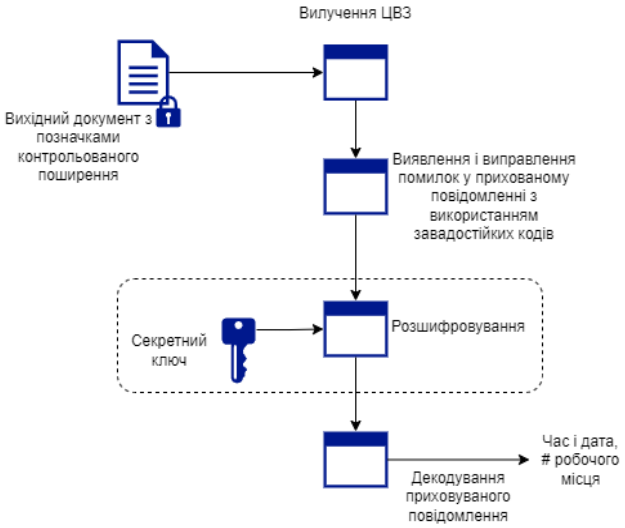

Рис. 3. Графічне зображення схеми вилучення ЦВЗ з документу із конфіденційною інформацією

Вказані моделі можуть використовуватися, як окремо, так і в комбінації для підвищення точності виявлення ЦВЗ та їх подальшого розпізнавання. Вибір конкретної моделі нейронної мережі виходить за межі даної роботи і буде розглянуто у майбутніх дослідженнях.

Для розробки власного методу вбудовування і вилучення ЦВЗ (як видимих, так і невидимих для людського ока), згідно наведених схем, доцільно визначити:

- перелік та структуру даних, які мають бути внесені;
- метод кодування та виправлення можливих помилок зчитування ЦВЗ.

Відповідно до вихідних умов повідомлення має містити дату, час (з точністю до хвилини) та ідентифікатор обладнання (робочого місця), на якому воно створене. Звичайне позначення дати та часу (без врахування пробілів та розділових знаків) займає від десяти до дванадцяти символів: 00.00 01.01.01 або 00.00 01.01.2001. Для зменшення кількості символів доцільно використати лічильник часу, який відображатиме порядковий номер хвилини, починаючи з 00.00 01.01.2000 до 23.59 31.12.2099. При такому поданні відображення дати та часу займатиме всього вісім символів (60 хв × 24 год × 365днів × 100років = 52 560 000 хв.).

Для ідентифікації джерела (обладнання на якому створювалося означене подання документа із прихованим повідомленням) пропонується відвести чотири символи (9999 можливих кореспондентів).

Таким чином для позначення дати, часу та ідентифікатора обладнання необхідно дванадцять символів десяткової системи числення, які мають бути закодовані у приховане повідомлення та інтегровані у візуальне подання документа в електронній або паперовій формі.

Робастність стеганографічної системи ЦВЗ може забезпечуватись шляхом багаторазового повторювання матриці ЦВЗ на візуальному поданні документа та/або використанням завадостійких методів нанесення даних ЦВЗ на зображення та/або методів завадостійкого кодування даних перед їх вбудовуванням кодуванням з використанням точок.

Водночас, використання завадостійкого кодування, як правило, вимагає використання змішаних систем числення або переведення повідомлення у різні системи числення, наприклад із десяткової у двійкову систему числення та введення певної надмірності, що суттєво збільшує розмір вихідного повідомлення.

Для порівняння методів формування ЦВЗ візьмемо значення, яке відповідає 7 год 10 хв 14.01.2022, ідентифікатор обладнання № 4339.

22 × 365 + 6 + 14 = 8050 днів, враховуючи 6 днів з високосних років, та 14 днів 2022 року і 8050 × 24 × 60 + 7 × 60 + 10 = 11595430 хвилин. Отже повідомлення, яке слід приховати, матиме значення 11595430433910 (Табл. 2).

Однак, зміна ідентифікатора обладнання та часу створення документів призводитиме до динамічної зміни правої частини повідомлення, водночас ліва його частина протягом тривалого часу залишатиметься відносно статичною. Самим простим способом збільшення рівномірності розподілу двійкових значень прихованого повідомлення, лавинного ефекту від зміни ідентифікатора обладнання чи часу на кілька хвилин, автори пропонують:

– Використовувати методи симетричного шифрування. Дозволить приховати сенс повідомлення, що приховується і захиститися від можливих атак нав'язування хибних прихованих повідомлень.

– Використовувати більш прості методи:

1) Метод псевдовипадкової перестановки.
2) Метод детермінованої перестановки.

Для демонстрації детермінованої перестановки, розглянемо перестановку непарних цифр повідомлення справа наліво (Табл. 2 та 3).

Таблиця 2

Задане число, яке слід приховати, кожна цифра якого розбита відповідно порядковому номеру

Порядковий № цифри	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
Початкове повідомлення	1	1	5	9	5	4	3	0	4	3	3	9

Таблиця 3

Представлення заданого числа, яке слід приховати використавши перестановку непарних цифр повідомлення справа наліво

Порядковий № цифри	*11*	*2*	*9*	*4*	*7*	*6*	*5*	*8*	*3*	*10*	*1*	*12*
Вихідне повідомлення	3	1	4	9	3	4	5	0	5	3	1	9

Схему додавання позначок контрольованого поширення документу з конфіденційною інформацією зображено на Рис. 2: побудову приховуваного повідомлення на основі часу і дати, номеру робочого місця, зашифровування приховуваного повідомлення, кодування зашифрованого повідомлення з використанням методу завадостійкого кодування та методів завадостійкого вбудовування ЦВЗ. Після чого документ з доданими позначками можна напряму відправити одержувачу захищеним каналом.

Висновки

У цій роботі розглянуто, як ЦВЗ можуть допомогти встановлювати джерело створення та можливі канали витоку інформації. Це особливо важливо, коли йдеться про захист конфіденційної інформації.

1. ЦВЗ, як видимі, так і невидимі, для людського ока дозволяють приховано вбудовувати у документ такі дані, як дата, час та номер пристрою де біло створено документ. Це допомагає відстежити джерело можливого витоку інформації.

2. Багато сучасних кольорових принтерів уже автоматично додають приховані мітки до кожного роздрукованого аркуша. Їх можна зчитати, щоб визначити, на якому принтері і коли був надрукований документ. Однак, їх використання не вирішує повністю поставлену задачу і потребує впровадження власних методів. Крім того використання кольорового друку для офіційних документів не завжди допустиме.

3. Якщо потрібно уникнути фіксації позначок, що додаються засобами вбудованими у сучасні кольорові принтери (наприклад, для захисту приватності), можна:
   - вимкнути функцію додавання ЦВЗ;
   - друкувати на кольоровому фоні;
   - додати до ЦВЗ випадкові точки, щоб їх неможливо було прочитати.
4. Було запропоновано власний метод вбудовування і вилучення ЦВЗ.
5. Для зменшення розміру автентифікаційних даних про джерело інформації та час і дату, запропоновано зберігати дату й час як єдине число (у хвилинах), а також використовувати прості перетворення для рівномірного розподілу інформації.

ЦВЗ – це ефективний спосіб контролювати поширення документів. Вони допомагають встановити, хто саме створив чи роздрукував документ, навіть якщо він був відсканований або сфотографований. Але важливо враховувати й ризики для конфіденційності. Наступне дослідження буде зосереджене на вбудовуванні ЦВЗ (розробці методу) у сторінки документа у вигляді зображення.

Водночас, автори не рекомендують використання методів ідентифікації джерела інформації для цілей, які можуть порушувати конфіденційність приватних осіб.

Література

[1] Dutch track counterfeits via printer serial numbers [Електронний ресурс] // PC World Australia. – 2004. – Режим доступу: https://web.archive.org/web/20100420042322/http://www.pcworld.idg.com.au/article/8305/dutch_track_counterfeits_via_printer_serial_numbers.

[2] Hatch J. Printer tracking dots (steganography) [Електронний ресурс] / J. Hatch // Kook Science Research Wiki. – Режим доступу: https://hatch.kookscience.com/wiki/Printer_tracking_dots_%28steganography%29.

[3] Smith M.K. Method for embedding machine readable codes into printed documents : U.S. Patent № US5515451A [Електронний ресурс]. – 1996. – Режим доступу: https://patents.google.com/patent/US5515451A/en.

[4] DocuColor Tracking Dot Decoding Program [Електронний ресурс] // Electronic Frontier Foundation (EFF). – Без дати. – Режим доступу: https://w2.eff.org/Privacy/printers/docucolor/#program.

[5] Чому кольорові принтери "шифрують" ваші документи [Електронний ресурс] // BBC News Україна. – 28 лип. 2017. – Режим доступу: https://www.bbc.com/ukrainian/vert-fut-40754641.

[6] Cluley G. *How The Intercept might have helped unmask Reality Winner to the NSA* [Електронний ресурс] / G. Cluley. – 08.06.2017. – Graham Cluley: Cybersecurity Blog. – Режим доступу: https://grahamcluley.com/intercept-might-helped-unmasked-reality-winner-nsa/.

[7] Richter T., Escher S., Schönfeld D., Strufe T. Forensic Analysis and Anonymisation of Printed Documents [Електронний ресурс] / T. Richter, S. Escher, D. Schönfeld, T. Strufe // Proc. 6th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'18), Іннсбрук, Австрія. – 14 черв. 2018. – Режим доступу: https://doi.org/10.1145/3206004.3206019.

[8] Salim A.S., Abdalla A.A. The determination of identity and uniqueness of color laser printouts of Ricoh® brand by Adobe® Creative Cloud Photoshop® 2018 [Електронний ресурс] // Egyptian Journal of Forensic Sciences. – 2019. – Vol. 9, No. 1. – Article 40. – Режим доступу: https://doi.org/10.1186/s41935-019-0140-8.

[9] DARPA Shredder Challenge Fiscal Year 2012 Report [Електронний ресурс] // Defense Advanced Research Projects Agency. – січень 2013. – 56 с. – Режим доступу: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/DARPA/15-F-0059_SHREDDER_CHALLENGE_FISCAL_YEAR_2012_RPT.pdf.

[10] Tip for bad guys: burn, don't shred [Електронний ресурс] // Bloomberg. – 15.12.2011. – Режим доступу: https://www.bloomberg.com/news/articles/2011-12-15/tip-for-bad-guys-burn-dont-shred.

[11] *Стеганографія : навч. посіб.* / О.О. Кузнєцов, С.П. Євсєєв, О.Г. Король, А.А. Кузнєцов, С.П. Євсєєв. – Харків: ХНЕУ, 2011. – 232 с.

[12] *Forensic Analysis and Anonymisation of Printed Documents* [Електронний ресурс] / T. Richter, S. Escher, D. Schönfeld, T. Strufe // Proc. 6th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '18), Іннсбрук, Австрія. – 14 черв. 2018. – С. 127–138. – Режим доступу: https://doi.org/10.1145/3206004.3206019.

[13] Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser Ł., Polosukhin I. Attention is all you need // Advances in Neural Information Processing Systems. – 2017. – V. 30. – P. 5998–6008.

[14] Deutschlandfunk. *Tracking Dots unlesbar machen* [Електронний ресурс]. – 01.09.2015. – Режим доступу: https://www.deutschlandfunk.de/farblaserdrucker-tracking-dots-unlesbar-machen-100.html.

[15] Li Z., Yang W., Peng S., Liu F. A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects [Електронний ресурс] / Z. Li та ін. – 2020. – Режим доступу: https://arxiv.org/abs/2004.02806.

[16] An Extensive Study of Convolutional Neural Networks: Applications in Computer Vision for Improved Robotics Perceptions [Електронний ресурс] – 2025. – Режим доступу: https://www.mdpi.com/1424-8220/25/4/1033.

[17] Sherstinsky A. Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) Network [Електронний ресурс] / A. Sherstinsky. – 2018. – Режим доступу: https://arxiv.org/abs/1808.03314.

[18] Ghojogh B., Ghodsi A. Recurrent Neural Networks and Long Short-Term Memory Networks: Tutorial and Survey [Електронний ресурс] / B. Ghojogh, A. Ghodsi. – 2023. – Режим доступу: https://arxiv.org/abs/2304.11461.

[19] Zhang C., Zhang C., Song J., Yi J.S.K., Zhang K., Kweon I.S. Autoencoders and their applications in machine learning: a survey [Електронний ресурс] / C. Zhang та ін. – 2022. – Режим доступу: https://link.springer.com/article/10.1007/s10462-023-10662-6.

[20] Wang Z., She Q., Ward T.E. Generative Adversarial Networks in Computer Vision: A Survey and Taxonomy [Електронний ресурс] / Z. Wang, Q. She, T.E. Ward. – 2019. – Режим доступу: https://arxiv.org/abs/1906.01529.

[21] Khan S., Naseer M., Hayat M., Zamir S. W., Khan F. S., Shah M. *Transformers in Vision: A Survey* [Електронний ресурс] / S. Khan та ін. – 2021. – arXiv:2101.01169.

[22] Koopman P., Chakravarty T. Efficient Algorithms for CRC Computation / P. Koopman, T. Chakravarty. – 2004. – IEEE Transactions on Dependable and Secure Computing. – Vol. 1, No. 2. – P. 35–42. – Режим доступу: https://ieeexplore.ieee.org/document/1312394.

[23] Fossorier M., Lin S. Convolutional Codes: An Overview / M. Fossorier, S. Lin. – 2004. – IEEE Transactions on Information Theory. – Vol. 50, No. 3. – P. 523–537. – Режим доступу: https://ieeexplore.ieee.org/document/1264127.

[24] Richardson T. J., Urbanke R. L. The Art of Turbo Coding / T. J. Richardson, R. L. Urbanke. – 2008. – Cambridge, MA: MIT Press. – 280 с.

[25] Lin S., Costello D. J. Hamming Codes and Their Applications / S. Lin, D. J. Costello // Error Control Coding:

Fundamentals and Applications. – 2-е вид. – Upper Saddle River, NJ: Prentice Hall, 2004. – P. 92–105.

[26] Kuznetsov A. A., Gorbenko Yu. I., Lutsenko M. S., Prokopovych-Tkachenko D. I., Pastukhov M. V. NIST PQC: Code-Based Cryptosystems / A. A. Kuznetsov, Yu. I. Gorbenko, M. S. Lutsenko, D. I. Prokopovych-Tkachenko, M. V. Pastukhov // Telecommunications and Radio Engineering. – 2019. – Vol. 78, No. 5, pp. 429–441. – Режим доступу: https://hdl.handle.net/11389/70668.

[27] Stasev Yu. V., Kuznetsov A. A. Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes / Yu. V. Stasev, A. A. Kuznetsov // Kibernetika i Sistemnyi Analiz. – 2005. – No. 3. – P. 47–57.

[28] Науменко М. І., Стасєв Ю. В., Кузнєцов О. О. *Теоретичні основи та методи побудови алгебраїчних блокових кодів : монографія* / М. І. Науменко, Ю. В. Стасєв, О. О. Кузнєцов. – Х. : ХУПС, 2007. – 363 с.

[29] Борисенко О.А., Солярова Е.Н. *Стиснення інформації на основі багатозначних біноміальних кодів* [Електронний ресурс] / О. А. Борисенко, Е. Н. Солярова // Фізика, електроніка, електротехніка: матеріали конференції, м. Суми, 16–21 квіт. 2012 р. – Суми : СумДУ, 2012. – С. 170. – Режим доступу: http://essuir.sumdu.edu.ua/handle/123456789/27739.

[30] Luhn H. P. *Computer for verifying numbers : U.S. Patent No. 2950048A* / H. P. Luhn. – United States Patent and Trademark Office, 1960. – Режим доступу: https://patents.google.com/patent/US2950048A/en.

[31] Kuznetsov O, Chernov K, Shaikhanova A, Iklassova K, Kozhakhmetova D. DeepStego: Privacy-Preserving Natural Language Steganography Using Large Language Models and Advanced Neural Architectures. Computers. 2025; 14(5):165. https://doi.org/10.3390/computers14050165.

УДК 004.056.55

Snihzynskyi M.M., Kovtun V. Yu., Kovtun M. G., Kindrat Yu. R. Methods of integrating hidden messages into the visual representation of a confidential document

Abstract: *This paper examines methods for incorporating hidden messages into the visual representation of confidential documents to ensure controlled distribution. It discusses the practical implementation of digital watermarks (DWM) that can be extracted from both electronic and printed versions of a document. It's possible even after printing, scanning, or photographing. The authors describe the formation of embedded messages, encryption techniques, error-resistant encoding, and visual embedding strategies. Modern AI-based methods for detecting and extracting watermarks are reviewed. Additionally, the paper compares classical error correction codes (Luhn, CRC, Hamming, Reed-Solomon) used to enhance robustness against distortions.*

Keywords: *information security, digital watermarks, steganography, error correction coding, leakage identification, encryption.*

Сніжинський Микола Миколайович, заступник керівника підрозділу з формування та реалізації державної політики у сфері захисту інформації та електронних довірчих послуг у закритих системах Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Mykola Snizhynskyi, Deputy Head of the Division for the Development and Implementation of State Policy in the Field of Information Protection and Electronic Trust Services in Closed Systems of the Administration of the State Service of Special Communications and Information Protection of Ukraine.

Ковтун Владислав Юрійович, кандидат технічних наук, доцент, директор ТОВ «САЙФЕР ІТ».
Vladyslav Kovtun, PhD in Technical Sciences, Associate Professor, CEO of LLC "CIPHER IT".

Ковтун Марія Григорівна, кандидат технічних наук, старший науковий співробітник НДЛ протидії кіберзагрозам в авіаційній галузі Державний університет «Київський авіаційний інститут».
Mariia Kovtun, PhD in Technical Sciences, Senior Researcher Research Laboratory for Counteracting Cyber Threats in Aviation State University "Kyiv Aviation Institute".

Кіндрат Юлія Русланівна, здобувач вищої освіти ступеня магістра Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
Yuliia Kindrat, Master's Degree Student at the Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".