УДК 681.32

Андрій САДЧЕНКО, Олег КУШНІРЕНКО, Олександр ТРОЯНСЬКИЙ, Микола ВІГОВСЬКИЙ

Національний університет Одеська політехніка

АЛГОРИТМ ВБУДОВУВАННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ В ЗОБРАЖЕННЯ, СТІЙКИЙ ДО ШУМОВОГО ВПЛИВУ ТА ПІДРОБЛЕННЯ

Вступ. Дистанційна освіта (ДО) - це система освіти, яка передбачає активне спілкування студента з викладачем за допомогою сучасних інформаційних технологій та дає свободу вибору місця, часу та темпу навчання.

Переваги ДО очевидні, проте є й чималий ряд недоліків. По-перше, це ускладнена ідентифікація здобувачів, які навчаються. Досить складно перевірити, хто насправді складає іспит з того боку екрану комп'ютера. Не менш вагомою проблемою є недосконаліть та низька пропускна спроможність мережі Інтернет під час навчальних та екзаменаційних комунікацій. Крім того, в умовах відсутності освітлення, здобувачі фотографують виконані в зошиті рукописні роботи і вже в такому вигляді відправляють для перевірки викладачеві. Також можлива паперова роздруківка та пересилання матеріалів звичайною поштою.

З метою аутентифікації особи здобувача можливе використання цифрового підпису електронних документів, що надсилаються у бік викладача. Для формування цифрового підпису є сервіси, що вбудовані, наприклад до додатку банківського обслуговування Приват 24 та хмарного сховища електронних документів - Дія. Однак такий підхід не дозволяє виявити підробку графічного матеріалу і навряд чи підходить при здійснені поштового відправлення у паперовому вигляді. Розглянемо наступну ситуацію. Хай згідно із завданням до розрахунково-графічної (РГР) чи курсової роботи (КР) потрібно розробити блок-схему алгоритму роботи програмного забезпечення, структурну схему якогось пристрою чи малюнок захищеної мережі. Тобто саме графічні матеріали є основою таких РГР чи КР. При цьому схожі малюнки є у методиці до КР чи РГР. Здобувач може здійснити копіювання графічного матеріалу з наступним додаванням до своєї роботи.

У таких умовах для боротьби з підробкою або заміною виконаних завдань зручно використовувати цифровий водяний знак (ЦВЗ, англійською DWM - digital watermark) [1]. Так як бажано забезпечити інваріантність ЦВЗ щодо носія інформації приходимо до висновку про використання різновиду адитивного алгоритму додавання ЦВЗ.

Мета: підвищення завадостійкості та криптостійкості ЦВЗ завдяки використанню попереднього шифрування і динамічної зміни роздільної здатності за яскравістю в залежності від рівню шуму, що очікується в каналі розповсюдження інформації.

1. Сценарії використання ЦВЗ у навчальних закладах в умовах дистанційного навчання

Розглянемо наступний сценарій. Викладач надсилає завдання здобувачу з впровадженим індивідуальним ЦВЗ. Здобувач виконує завдання, наприклад,

заповнює тестову таблицю щодо модульного контролю, при цьому не пошкоджуючи ЦВЗ та відправляє викладачеві.

Фальсифікації результату можливі за умови, якщо студент підміняє ЦВЗ, попередньо знищивши оригінал.

Варіанти сценаріїв у вигляді алгоритму взаємодії у межах викладача та здобувача показані на рисунку 1.

Перший сценарій застосування ЦВЗ припускає розповсюдження бланку завдання у повністю електронної формі, тобто завдання передається та повертається в електронному вигляді.

Спочатку викладач формує електронний бланк із ЦВЗ і передає його по каналу зв'язку, студент отримує і модифікує електронний бланк із неушкодженим ЦВЗ. У подальшому, здобувач виконує зворотне передавання за каналом зв'язку і, вже на приймальному боці, викладач перевіряє справність ЦВЗ - підроблено чи ні.

Згідно другому запропонованому сценарію застосування ЦВЗ бланк завдання також передається в електронному вигляді, а потім роздруковується та повертається у паперовому. Тобто здобувач робить рукописні відповіді, сканує чи фотографує те, що вийшло та передає назад графічний об'єкт з ЦВЗ. Викладач, як і в першому випадку перевіряє справжність ЦВЗ, виконане завдання і тільки після цього оцінює саме завдання.

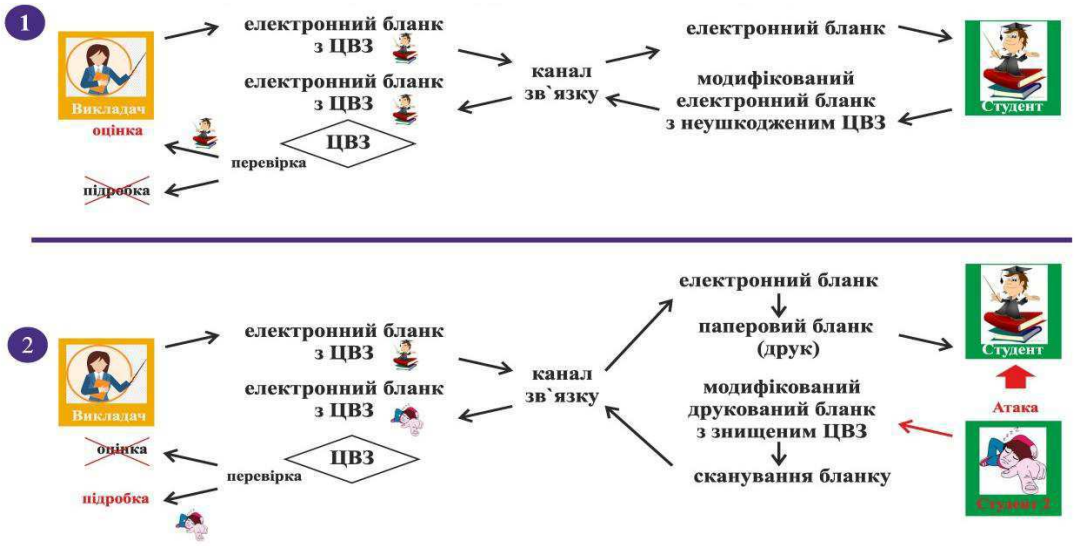

Рисунок 1 - Сценарії застосування ЦВЗ на прикладі НУ Одеська політехніка

Викладач => електронний бланк із ЦВЗ => канал зв'язку => електронний бланк => перетворення бланку в паперовий вигляд => студент => модифікований друкований бланк із неушкодженим ЦВЗ => сканування => канал зв'язку => Викладач.

Загальна процедура передачі зображення із ЦВЗ має такий вигляд:

1. Вбудовування ЦВЗ у контейнер.
2. Передача контенту каналом з перешкодами.
3. Порівняння контейнера та стегоконтейнера (контейнер з вбудованим ЦВЗ).
4. Вилучення ЦВЗ.
5. Порівняння вхідного та вихідного ЦВЗ.

Загальна процедура передачі ЦВЗ показана на рисунку 2.

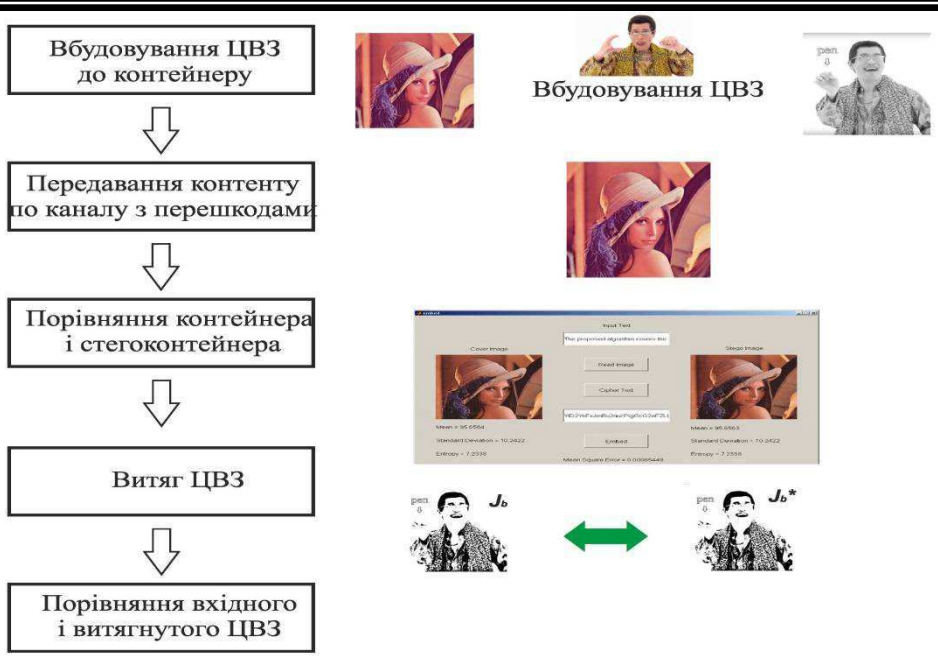

Рисунок 2 - Загальна процедура передачі зображення із ЦВЗ на прикладі НУ

Також звернемо увагу, що ЦВЗ називається надійним, якщо він протистоїть всім відомим видам атак. Такі ЦВЗ зазвичай використовуються в системах захисту від копіювання та ідентифікації. Непомітність та прозорість ЦВЗ впливають на складність його виявлення. Розрізняють впроваджуваний та вилучений обсяг даних. Будь-які витрачені зусилля на впровадження, атаку, детектування чи розшифрування вимірюються складністю ЦВЗ.

Найбільш популярні атаки на ЦВЗ, можна звести до наступних варіантів:

- знищення інформації, що містить власне ЦВЗ;
- масштабування контейнера (зміна розміру зображення стегоконтейнера)
- зашумлення захищеного зображення.

2. Підвищення завадостійкості та криптостікості адитивного алгоритму вбудови ЦВЗ

Модифікований алгоритм адитивний алгоритм вбудови ЦВЗ зображений на рисунку 3.

Для наочності в алгоритмі пропонуєтеся обмежити роздільну здатність зображення-контейнеру та ЦВЗ розміром 512x512 пікселів. Відправник спочатку виконує бінаризацію ЦВЗ [2] і подає його у такому вигляді на вхід скремблера із самосинхронізацію. Це є процедурою попереднього шифрування ЦВЗ з відкритим ключем за допомогою поліному 23-го ступеню. Якщо спробувати роздивитись зображення ЦВЗ на даному етапі - побачимо тільки шум.

Оскільки пропонується використання адитивного підходу, максимальну яскравість зображення контейнеру буде зменшено шляхом множення на коефіцієнт масштабу яскравості Km, що приймає значення від 0.5 до 0.7. Зображення ЦВЗ при цьому множиться на зворотне значення коефіцієнту масштабу яскравості (1/Km).

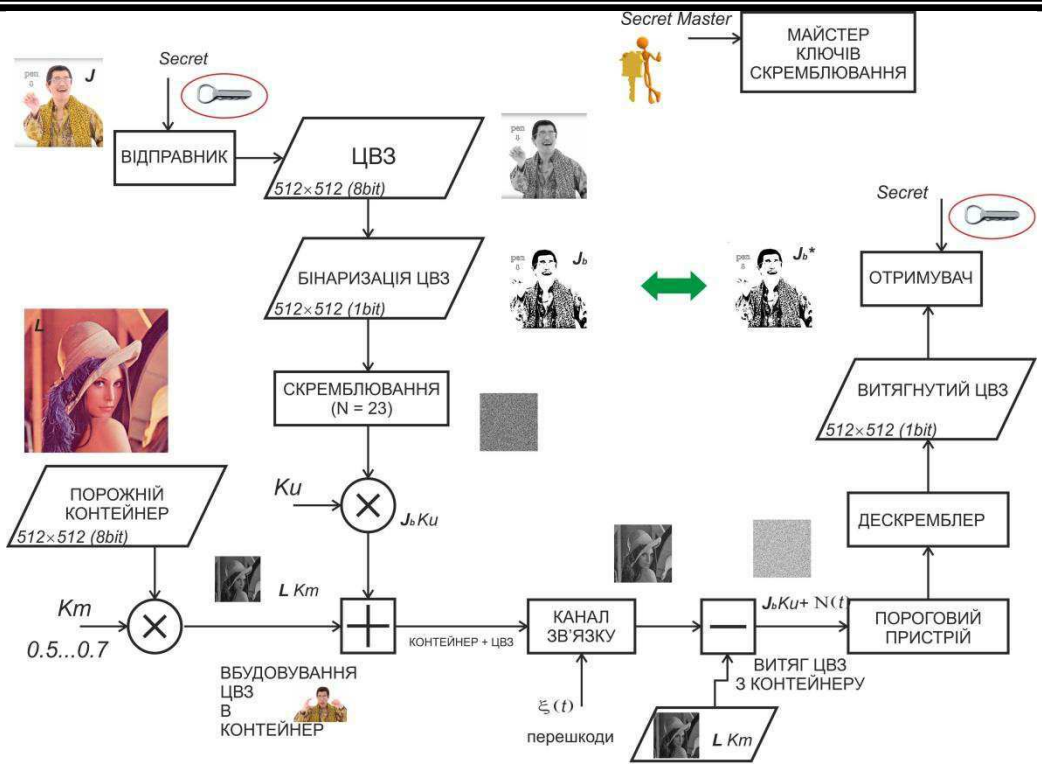

Рисунок 3 - Модифікований адитивний алгоритм вбудови ЦВЗ , стійкий до шумових впливів та підробки

Далі зашифроване зображення ЦВЗ додається до зображення контейнеру і в такому вигляді передається до каналу зв'язку. На приймальному кінці в цілому виконуються зворотні дії крім особливості щодо обробки ЦВЗ, яка полягає у використанні порогового пристрою, що має адаптивний поріг, що залежить від рівня шуму на зображенні. При вилученні ЦВЗ поріг щодо порогового пристрою поступово збільшується від мінімального значення 1 до 127 (якщо зображення має 8 біт розрядність за яскравістю). Збільшення значення порогу припиняється при досягнені найкращого вигляду ЦВЗ, що витягнутий.

Висновок. Запропоновано модифікований алгоритм додавання ЦВЗ у форматі градації сірого до кольорового чи монохромного зображень в умовах шумового впливу. Зображення-контейнер повинне володіти розрядністю за яскравістю не менш чим 8 біт на кожен піксель щодо монохромного зображення чи кольорового зображення, а ЦВЗ, що вбудовується має розрядність, що залежить від дисперсії шуму, що очікується та максимальної яскравості зображення - контейнера. Використання попереднього шифрування зображення ЦВЗ у вигляді алгоритму з відкритим ключем додатково знижує імовірність підроблення та фальсифікування графічних матеріалів, що можуть використовуватись в рамках дистанційного навчання.

Перелік використаних джерел.

1. Садченко А. В., Кушніренко О. А. Неспотворюючий алгоритм вбудовування цифрового водяного знаку у медичні зображення. Технологія та конструювання в електронній апаратурі, 2024, № 1 –2, с. 33–42. http://dx.doi.org/10.15222/TKEA2024.1-2.33

2. MATLAB Online. Use MATLAB through your web browser [Електроний ресурс]. - Режим доступу: https://ch.mathworks.com/products/matlab-online.html/