МОДИФІКОВАНИЙ АДИТИВНИЙ МЕТОД ВБУДОВИ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

К. т. н. А. В. Садченко, О. А. Кушніренко, Н. П. Кушніренко, О. В. Садченко, В. О. Пучков

Одеський національний політехнічний університет
Україна, м. Одеса
koa@opu.ua

Запропоновано модифікацію алгоритму вбудовування цифрового водяного знаку (ЦВЗ) в найменш значущий біт зображення в умовах руйнівного впливу білого гаусівського шуму. Оригінальне зображення являє собою двовимірний масив з розрядністю 8 бітів на кожен піксель, при цьому вбудований ЦВЗ має адаптивну розрядність, що залежить від середньої яскравості зображення-контейнера.

Ключові слова: цифровий водяний знак, метод Least Significant Bit, білий гаусівський шум, скремблер.

Захист авторських прав в межах вузівського діловодства та документів, переданих мережами загального доступу, набуває все більшої актуальності у зв'язку з активним впровадженням дистанційного навчання [1]. На рис. 1 зображено приклад галузей застосування (ЦВЗ) в вищому навчальному закладі.

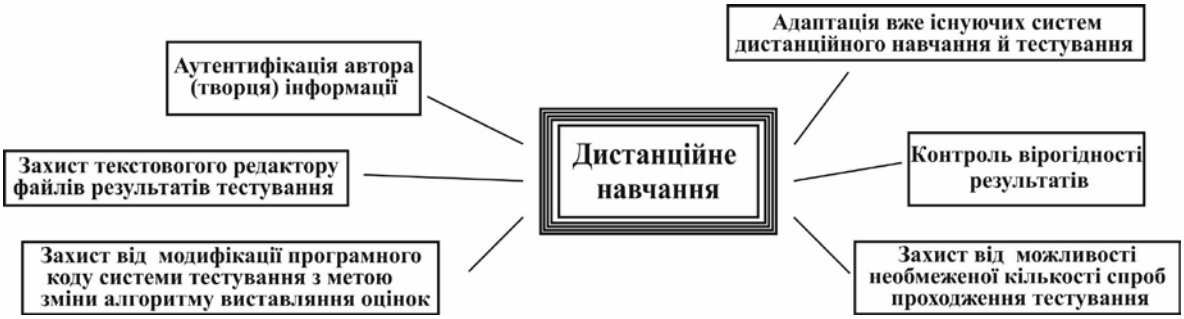

Рис 1. Галузі застосування цифрового водяного знаку в вищому навчальному закладі

Для впровадження ЦВЗ застосовуються два основні підходи [2]:
— приховування ЦВЗ в просторовій області контейнера;
— приховування ЦВЗ в частотної області контейнера.

У зв'язку з простотою реалізації широко використовуються методи приховування ЦВЗ в просторової області, а саме метод заміни найменш значущого біта (Least Significant Bits — LSB).

Однак, незважаючи на наявні переваги, методи LSB є нестійкими до багатьох видів атак і можуть бути легко скомпрометовані.

В даній роботі описаний метод підвищення стійкості ЦВЗ до спотворення і підробки з використанням попереднього скремблювання і підбору оптимального коефіцієнта підсилення для боротьби з шумом в каналі передачі даних.

У загальному випадку процедура передачі ЦВЗ виглядає наступним чином:
— вбудовування ЦВЗ у контейнер;
— передавання контенту каналом з перешкодами;
— порівняння контейнера і стегоконтейнера;
— вилучення ЦВЗ;
— порівняння вхідного і вихідного ЦВЗ.

Але такий алгоритм є абсолютно нестійким до підробки ЦВЗ, оскільки зловмисник може самостійно модифікувати інформацію.

У пропонованому нами модифікованому алгоритмі передавання цифрового водяного знаку (рис. 2) з метою захисту контенту від несанкціонованого перегляду застосовується попереднє скремблірованіе зображення ЦВЗ: оригінальне зображення водяного знаку після бінарізації піддається скремблюванню, після чого сформований ЦВЗ сприймається як шум. Для підвищення завадостійкості пікселі зображення контейнера зменшуються за амплітудою множенням на коефіцієнт масштабу K_m (в роботі K_m = 0,5—0,7). Відповідно, бінарізовані значення ЦВЗ модифікуються за амплітудою шляхом множення на коефіцієнт підсилення K_u. Після передачі інформації каналом зв'язку з шумом на приймальному кінці виконується операція віднімання бінарізірованого ЦВЗ з урахуванням коефіцієнта підсилення K_u. В результаті отримується скрембльоване бінаризоване зображення з додатковим шумом з урахуванням атак на канал зв'язку. Далі відбувається відновлення ЦВЗ. При цьому необхідно, щоб одержувач і відправник заздалегідь мали ключ скремблювання (ця інформація засекречена). Оскільки внаслідок шумових атак можливе проходження окремих імпульсних завад через всю схему шифрування, на зображенні ЦВЗ можуть з'явитися спотворені пікселі.

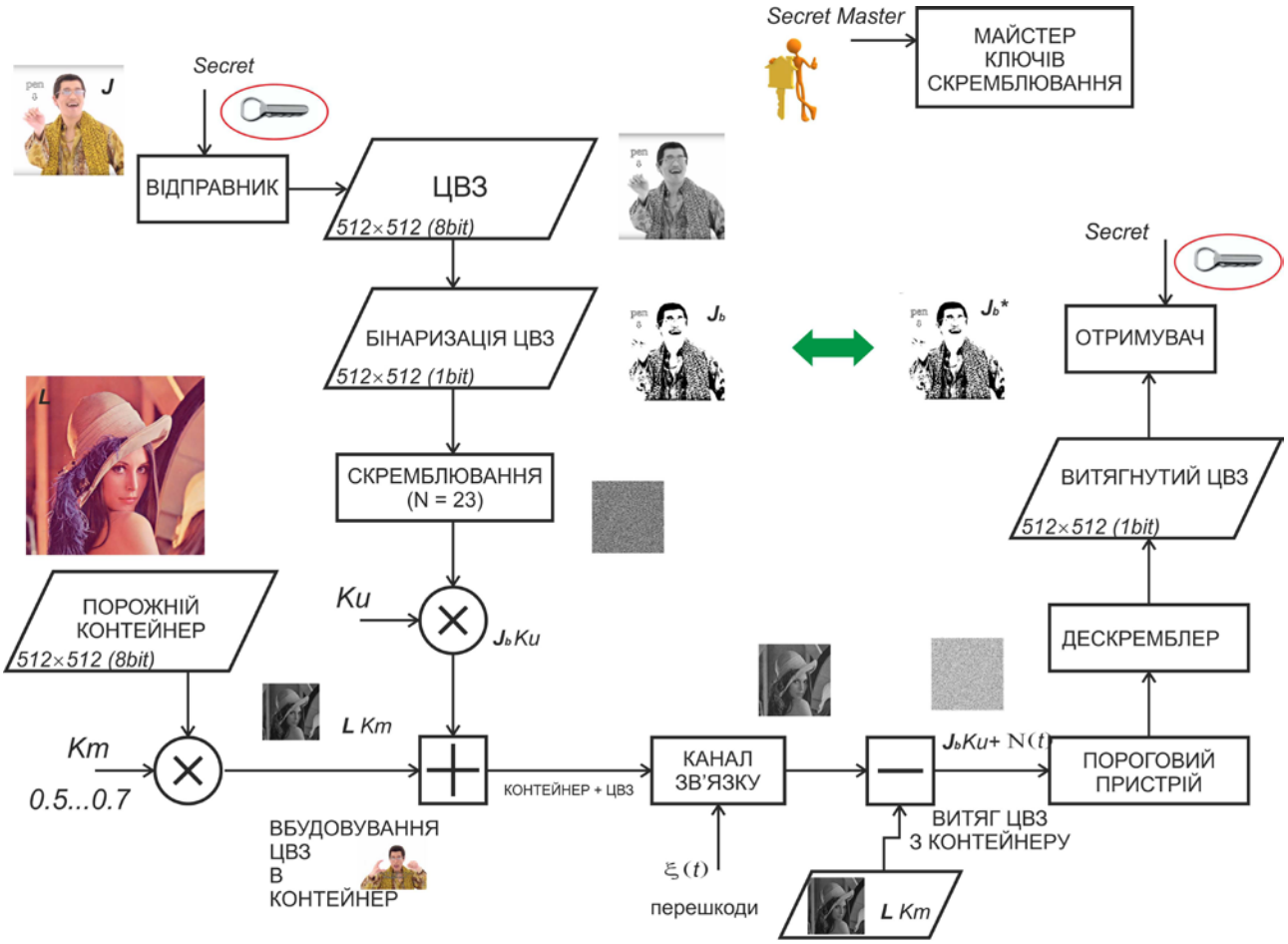

Рис. 2. Модифікований алгоритм передавання цифрового водяного знаку в найменш значущий біт зображення в умовах білого гаусівського шуму

Критерієм для аналізу завадостійкості було обрано залежність коефіцієнта кореляції між неспотвореним ЦВЗ та ЦВЗ, отриманим після його витягування з контейнера, від різної дисперсії шуму в каналі зв'язку. Результати моделювання, що виконані в хмарному [3] сервісі MATLAB, наведено на рис. 3.

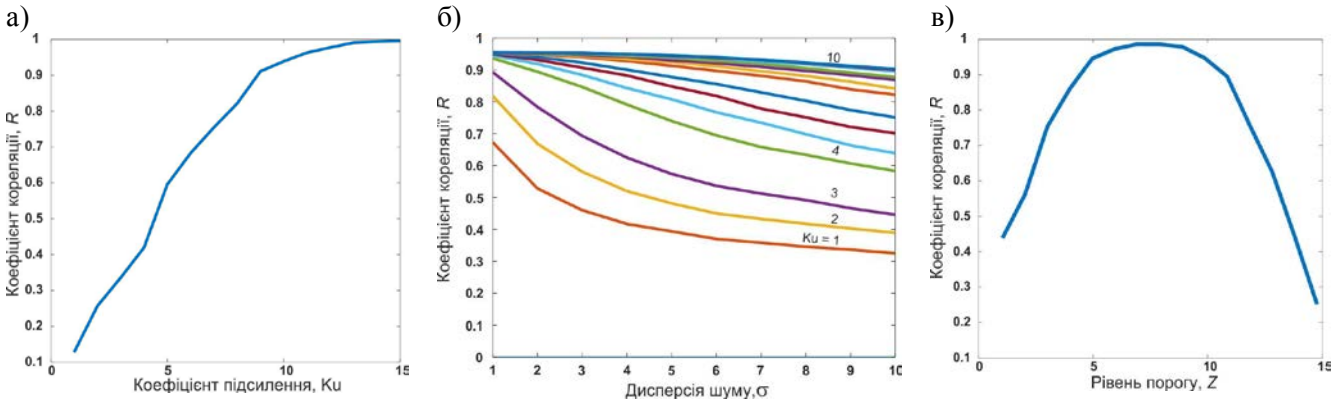

Рис 3. Графіки залежності коефіцієнта кореляції від коефіцієнта посилення ЦВЗ (*а*), від дисперсії шуму за різних значень K_u (*б*) та від порога за фіксованого рівня шуму (*в*)

З аналізу залежностей видно, що зі зростанням коефіцієнта посилення завадостійкість ЦВЗ збільшується, проте при цьому знижується динамічний діапазон яскравості контейнера, що приводить до погіршення скритності ЦВЗ. Також проводилася оптимізація вибору порога в вирішальному пристрої (рис. 3, *в*), де поновлюється ЦВЗ.

Таким чином, застосування попереднього скремблювання зображення ЦВЗ дозволяє підвисити стійкість алгоритму до підробки. Основний недолік алгоритму додавання інформації про ЦВЗ до молодшого значущого біту є його дуже низька завадостійкість. Для боротьби зі знищенням або пошкодженням інформації про ЦВЗ запропоновано алгоритм адаптивного підсилення амплітуди пікселів зображення, що вбудовується відповідно до яскравості пікселів зображення самого контейнеру. Також знайдено оптимальні значення порога бінарізації, при відхиленні від яких завадостійкість ЦВЗ погіршується.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шаньгин В.Ф. Информационная безопасность и защита информации.— М.: ДМК Пресс, 2017.

2. Михайличенко О.В., Прохожев Н.Н., Коробейников А.Г. Оценка устойчивости ЦВЗ к внешним воздействиям, внедренных с помощью алгоритмов пространственной области встраивания // Научно-технический вестник СПб ГУ ИТМО.— 2008.— Вып. 51.— С. 168–172.

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

A. V. Sadchenko, O. A. Kushnirenko, N. P. Kushnirenko, O. V. Sadchenko, V. O. Puchkov

Modified additive method of embedding a digital watermark

The authors propose a modification of the algorithm for embedding a digital watermark in the least significant bit of the image under the conditions of the destructive effect of white Gaussian noise (WGN). The original image is a two-dimensional array with a resolution of 8 bits per pixel, while the built-in central digital readout has adaptive resolution, which depends on the average brightness of the container image.

Keywords: digital watermark, Least Significant Bit (LSB) method, white Gaussian noise (WGN), scrambler.