АЛГОРИТМ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ТА КРИПТОСТІЙКОСТІ ЦИФРОВОГО ПІДПИСУ ГРАФІЧНИХ ЗОБРАЖЕНЬ

К. т. н. А. В. Садченко, О. А. Кушніренко, к. т. н. О. В. Троянський,
В. А. Кисляк, В. Г. Лисечко

Національний університет «Одеська політехніка»
Україна, м. Одеса
koa@op.edu.ua

Запропоновано адаптивний алгоритм цифрового підпису кольорових і чорно-білих графічних зображень, одержуваних, наприклад, з камер фіксації порушень правил дорожнього руху. Сутність алгоритму полягає у використанні завадостійкого кодування цифрового підпису з попередньою оцінкою величини дисперсії шуму вихідного зображення. Для підвищення завадостійкості цифрового підпису залежно від отриманого значення дисперсії шуму використовуються коди, що дозволяють виправити помилку відповідної кратності, а для підвищення криптостійкості до зображення перед завадостійким кодуванням може додаватися штучний шум.

Ключові слова: цифровий підпис, завадостійке кодування, дисперсія шуму зображення.

Стеганографічні системи передачі, на відміну від криптографічних, застосовуються у випадках, коли необхідно як захистити інформацію, так й приховати сам факт її передачі. Типова функціональна схема стеганографічної системи передачі представлена на рис. 1.

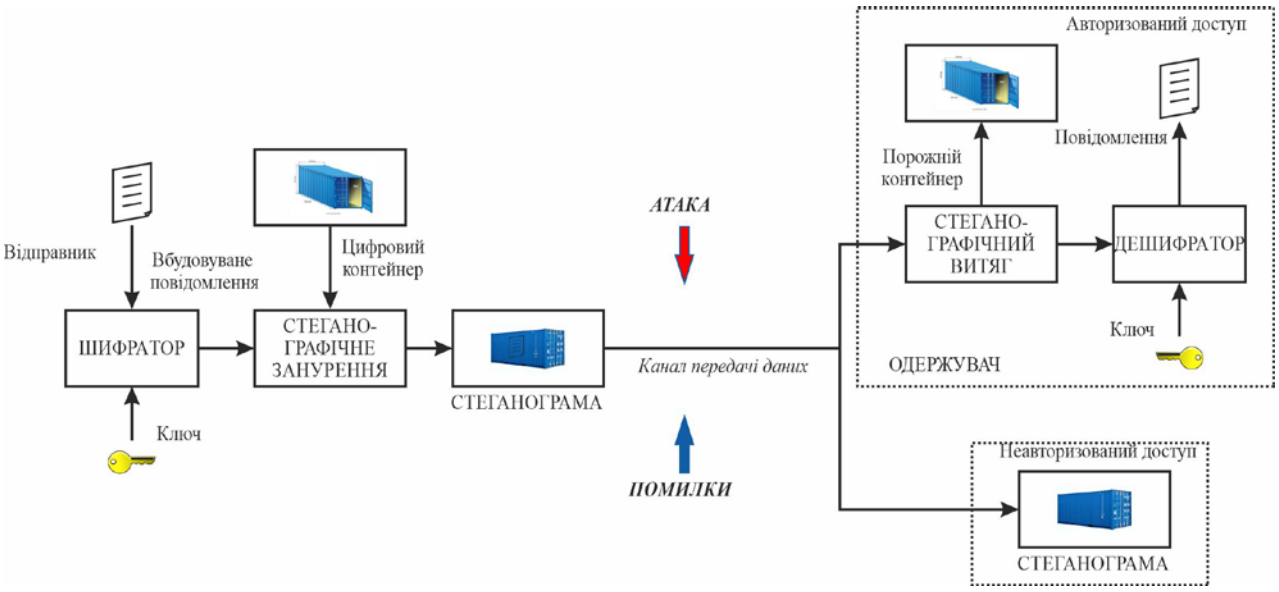

Рис. 1. Типова функціональна схема стеганографічної системи передачі інформації (цифрового підпису)

Як цифровий контейнер може використовуватися зображення з камер відеоспостереження, призначених для фіксації порушень правил дорожнього руху, стоянок тощо. Вбудовуване повідомлення може містити дані геолокації або іншу інформацію, що підтверджує автентичність зображення (контейнера).

Стеганографічне вбудовування цифрового підпису (ЦП) зображення полягає в модифікації молодших розрядів яскравості пікселів ділянки зображення [1]. В ролі ділянки зображення може використовуватися як окремий рядок або стовпець двовимірного масиву, так і поєднання кількох рядків або стовпців. Процедура вилучення ЦП з графічного контейнера зазвичай відбувається шляхом обчислення згортки секретного ключа і прийнятого зображення в ковзному вікні.

Завдання, що виникають при організації каналу стеганографії передачі інформації можна умовно розділити на дві групи.

Перша група завдань, що пов'язана з проблемами забезпечення секретності, — це вибір оптимального розміру контейнера, типу секретного ключа, пошук областей зображення, які найкраще підходять для занурення секретної інформації тощо. Друга група завдань — забезпечення завадостійкості, що передається за допомогою стеганографічної інформації [2, 3]. Перелічені групи завдань зазвичай суперечливі, оскільки збільшення довжини секретного ключа призводить до збільшення криптостійкості та одночасного зниження завадостійкості.

Метою цієї роботи є адаптація типової схеми (алгоритму) формування цифрового підпису до рівня природного шуму вихідного зображення (контейнера) для усунення протиріччя між зростанням криптостійкості та зниженням стійкості до перешкод.

Для забезпечення одночасного зростання криптостійкості та завадостійкості пропонується використовувати коригувальний згортковий код, що виправляє пакетну помилку, при цьому замість криптостійкого кодування (скремблювання) ключа адитивно додати шум, що формує помилки меншої кратності, ніж може виправити коригувальний код.

Модифікований алгоритм формування цифрового підпису наведено на рис. 2.

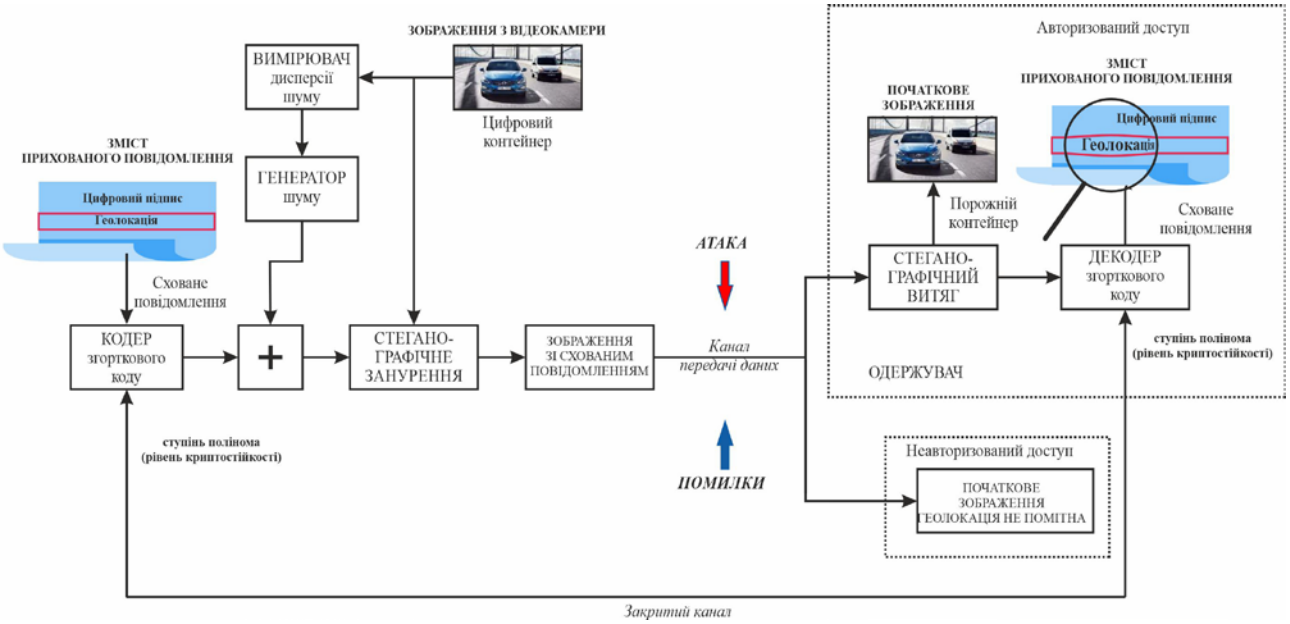

Рис. 2. Модифікована функціональна схема формування цифрового підпису

Блок аналізу (блок вимірника) дисперсії шуму та оцінки кратності помилки, що припадає на довжину дискретного повідомлення N, дозволяє вибрати рівень дисперсії генератора штучного шуму, який впливає на цифровий підпис. Кодер згорткового коду, встановлений після формувача цифрового підпису, адаптується до необхідного рівня криптостійкості за допомогою вибору довжини первісного непривідного полінома над полем Галуа [4] і, як наслідок, довжини перешкодостійкого коду.

У таблиці наведено рівень дисперсії шуму $\sigma_ш^2$, кратність пакетної помилки *r*, що виникає на довжині повідомлення *N*, кодова відстань згорткового коду *d*, необхідна для виправлення помилок коду, реальна кратність пакетних помилок *t*, що виправляє згортковий код зі швидкістю 1/2.

Характеристики штучного шуму та параметри згорткового коду зі швидкістю 1/2

$\sigma_ш^2$	*r*	*d*	*t*
0,1	1	3	2
0,2	3	7	4
0,4	5	11	6

Таким чином, попереднє кодування цифрового підпису завадостійким згортковим кодом дозволяє знизити складність алгоритму за рахунок відмови від стадії шифрування (скремблювання), а штучне зашумлення шумом з дисперсією рівної дисперсії шуму контейнера підвищує криптостійкість ЦП завдяки додатковому маскуванню ділянки вбудовування..

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Скляр Б. *Цифровая связь. Теоретические основы и практическое применение*. Издательский дом «Вильямс», 2004, 1104 с.

2. Конахович Г., Прогонов Д., Пузиренко О. *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних* [підручник]. Київ, Центр навчальної літератури, 2018, 558 с.

3. Мельник С., Кащук В. Методи цифрової стеганографії: стан та напрями розвитку. *Інформаційна безпека людини, суспільства, держави*, 2013, № 3, с. 65–70.

4. Кудряшов Б. Д. *Основы теории кодирования: учеб. пособие*. БХВ-Петербург, 2016, 400 с.

A. V. Sadchenko, O. A. Kushnirenko, O. V. Troyanskiy, V. A. Kysliak, V. G. Lysechko

Algorithm for increasing noise immunity and crypto resistance of digital signature for images

The authors propose an adaptive algorithm for the digital signature for color and black-and-white images obtained, for example, from cameras recording traffic violations. The essence of the algorithm consists in the use of interference-resistant coding of a digital signature with a preliminary assessment of the value of the noise dispersion of the output image. To increase the interference resistance of the digital signature — depending on the obtained value of the noise dispersion — codes are used that allow correcting the error of the corresponding multiplicity. To increase cryptoresistance, artificial noise may be added to the image before performing interference-tolerant coding.

Keywords: digital signature, interference-resistant coding, image noise dispersion.
