УДК 621.391

П.Ю. КОСТЕНКО
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *kpyu@ukr.net*.

К.С. ВАСЮТА
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *kohafish@ukr.net*.

В.В. СЛОБОДЯНЮК
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *sloval@i.ua.*

В.І. ЧИСТОВ
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *valera.chistov43@gmail.com.*

Д.М. ЗАПАРА
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *mw19@ukr.net*.

Р.О. КАЧАЙЛО
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *rkacajlo@gmail.com.*

І.В. ГУРЄЄВ
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, e-mail: *sms5000sms@gmail.com*.

МЕТОД СТЕГАНОГРАФІЇ, СТІЙКИЙ ДО СТАТИСТИЧНОГО АНАЛІЗУ

Анотація. В роботі запропоновано метод стеганографії на основі попереднього «вибілювання» стеганографічного контейнера перед вбудовуванням у нього конфіденційної інформації. Під «вибілюванням» розуміють приведення статистичних характеристик контейнера до відповідних характеристик «білого» шуму. Як контейнери та приховану в них інформацію використано цифрові зображення у відтінках сірого формату BMP. «Вибілювання» зображень-контейнерів здійснено за допомогою перемішування їхніх пікселів у псевдовипадковий спосіб з використанням хаотичної послідовності, сформованої поліномом Чебишова першого роду третього порядку. Стеганографічний аналіз (стегоаналіз) зображення із вбудованою в нього конфіденційною інформацією виконано із застосуванням індексу передбачуваності (SG-статистики). Результати моделювання підтверджують ефективність запропонованого методу стеганографії порівняно з класичним методом заміни найменш значущих бітів та методом LSB matching.

Ключові слова: стеганографія, статистичний стеганографічний аналіз, «вибілювання» контейнера, індекс передбачуваності, непараметрична статистика, найменш значущий біт.

DOI 10.34229/KCA2522-9664.26.6.14

ВСТУП

В умовах інтенсивного розвитку сучасних інформаційно-комунікаційних систем (ІКС) та збільшення обсягів обміну цифровими даними істотно зростає актуальність гарантування інформаційної безпеки. Одним із підходів до її забезпечення у цих системах є використання стеганографічних методів для організації прихованих каналів зв'язку за допомогою вбудовування конфіденційної інформації у так званому контейнері, роль якого можуть виконувати, зокрема, аудіо- та відеосигнали, цифрові зображення, а також сигнали інших типів, що передаються або зберігаються в ІКС [1].

Для гарантування інформаційної безпеки розроблено численні методи та алгоритми стеганографії [1–5]. Проте для багатьох із них характерний недолік, який полягає у зміні статистичних характеристик контейнера після вбудовування інформації, що робить їх вразливими до методів статистичного аналізу, зокрема статистичного стегоаналізу [6–10].

© П.Ю. Костенко, К.С. Васюта, В.В. Слободянюк, В.І. Чистов, Д.М. Запара, Р.О. Качайло, І.В. Гурєєв, 2026