УДК 681.322:621.391

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ ІНТЕГРАЛЬНОГО КРИТЕРІЮ СТІЙКОСТІ ДО АКТИВНИХ JPEG-АТАК

В. В. Лукічов, здобувач
Вінницький національний технічний університет
lukitchov@mail.ru

Коло задач, вирішуваних в межах сучасних комп'ютерних систем (КС), є надзвичайно широким. Однак основне призначення КС полягає у автоматизованому збирані, зберіганні, оброблені та передаванні інформації. Одним з основних аспектів підвищення ефективності КС є забезпечення високого рівня захищеності інформації в її межах. Серед інших напрямків захисту інформації стеганографія має ряд переваг, що обумовлені непомітністю її реалізації.

Стеганографія зображень є галуззю, що дістала стрімкого розвитку протягом останніх десяти років. Її ціль може бути окреслена як таємне та стійке до різноманітних перетворень приховування даних.

Оскільки порушення таємності може призвести до повної втрати повідомлення, то саме зазначена якість задає основні обмеження при проектуванні стегосистеми. Треба відмітити, що відносний характер цього показника обумовлює існування великої кількості критеріїв, ефективність яких неоднакова для різних методів вбудовування. Іншим важливим аспектом є вимога стійкості. Оскільки широко розповсюджені схеми надлишкового кодування з захистом від помилок, то питання робастності може бути вирішено з ефективністю, що визначається достовірністю відновленої інформації.

Таким чином, проектування будь-якої стегосистеми можна розглядати як задачу умовної оптимізації, де цільова функція певним чином пов'язує робастність із ступенем таємності, а обмеження визначають область адекватності критерію. Такий універсальний підхід дозволить забезпечити високу адаптивність до умов безпосереднього функціонування стегосистеми.

У стеганографії зображень особливо розповсюдженою є схема напівсліпого вбудовування де передається лише стегоконтейнер та відомий ключ. Це визначає особливості стегоаналізу, задача якого полягає у бінарній класифікації зображень на основі властивостей, що зазнають найбільших змін при вбудовуванні. Особливо перспективними є критерії на основі методу опорних векторів (МОВ).

Серед методів обробки зображень найбільшою популярністю користуються методи ущільнення. Найбільший коефіцієнт ущільнення здатні забезпечити методи ущільнення з втратами. Стандарт ущільнення JPEG і досі використовується широко, незважаючи на впровадження більш ефективних форматів на основі вейвлет перетворень (наприклад JPEG2000). Така ситуація, вочевидь, обумовлена інертністю концепцій розробки програмного забезпечення у цій сфері, що в свою чергу дозволяє прогнозувати значну тривалість переходу.

Тому як основну активну атаку на стегоконтейнер розглядається ущільнення за JPEG алгоритмом. З іншого боку, стеганографічне використання вейвлет перетворень дає підстави сподіватися на непомітність внесених змін. За допомогою розробленого інтегрального критерію пропонується дослідити комплексний зв'язок між таємністю та робастністю зазначеного використання в області вейвлет перетворень.