1. Wysocki, R. K. (2019). Effective Project Management: Traditional, Agile, Extreme, Hybrid. — New Jersey: Wiley. — 696 p.
2. Phillips, J. (2021). PMP Project Management Professional Study Guide. — New York: McGraw-Hill. — 592 p.
3. Ross, R. S., et al. (2020). Security and Privacy Controls for Information Systems and Organizations. — NIST SP 800-53 Rev. 5. — 492 p.
4. Bryk O., Mudryk I., Holubovskyi M., Stoianov Y. Machine learning models and methods aspects of processing unstructured data. Proceedings of the 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024), Zboriv, Ukraine, 2024. 2024. P. 64–74.

Гібридний метод приховування ЦВЗ у цифрових зображеннях

УДК 004.056.5

Ірина Борисенко[1], Даніїл Стрельченко[2]

Національний університет «Одеська політехніка»,
[1]borisenko.i.i@op.edu.ua, [2]10182258@stud.op.edu.ua

Для побудови стійких систем ЦВЗ використовуються різні підходи перетворення контейнера, наприклад, дискретне перетворення Фур'є (ДПФ) та сингулярний розклад матриць (SVD), які демонструють високу ефективність у задачах спектрального аналізу та приховування даних. ДПФ дозволяє перейти у частотну область, забезпечуючи стійкість ЦВЗ до геометричних атак, SVD виділяє стабільний енергетичний кістяк зображення (сингулярні числа), який є надзвичайно стійким до стиснення алгоритмом JPEG та шумових перешкод.

Актуальність теми полягає в необхідності інтеграції переваг обох математичних апаратів у єдину комбіновану (гібридну) схему, яка забезпечуватиме максимальну стійкість захисту авторських прав до комплексних атак, зберігаючи при цьому високу візуальну якість зображення.

Метою роботи є розробка комбінованого стеганографічного алгоритму вбудовування ЦВЗ, що поєднує частотну декомпозицію на основі ДПФ і SVD перетворень та дослідження його стійкості до стеганоаналітичних атак.

Доведено [1], що перше (найбільше) сингулярне число S_{11} сингулярного розкладу матриці контейнера концентрує в собі основну енергію зображення, що робить його модифікацію надзвичайно стійкою до зовнішніх впливів, цю властивість будемо використовувати в алгоритмі вбудовування ЦВЗ.

Алгоритм вбудовування. Зображення-контейнер розбивається на незалежні блоки розміром 8×8 пікселів, для кожного блоку виконується ДПФ, до коефіцієнтів середньої частоти застосовується кільцева маска з радіусами R_{min} та R_{max}, яка виділяє коефіцієнти, які є найбільш оптимальними для приховування даних, після чого до виділеного кільця застосовується SVD. Значення S_{11} ділиться на коефіцієнт сили вбудовування α – одержуємо S'_{11}. Якщо секретний біт дорівнює 0, значення S'_{11} округлюється до найближчого парного числа, якщо 1 – до непарного. Отримуємо матрицю S_{new}. Далі робимо зворотні перетворення: $US_{new}V^T$ та зворотне ДПФ. Відновлюється повідомлення шляхом зворотних перетворень: ДПФ –> кільце з радіусами R_{min} та R_{max} –> SVD виділеного кільця частот; зчитується перше сингулярне число,

по його парності роблять висновок, який саме біт (0 чи 1) було приховано у даному блоці.

Проведені експерименти показали високу візуальну якість стегоконтейнера (PSNR > 35 dB) та високу стійкість до шумів: гаусівського (при σ = 5 – відсоток відновлення повідомлення до 100%; σ = 15 – середній рівень шуму, відновлення до 80%); мультиплікативного (при низькому рівні імпульсного шуму P < 0,5 %) точність відновлення майже 100 %. Стійкість до компресії JPEG (Q=70, Q=50), завдяки варіативному вибору параметра α, одержували PSNR 45-40дБ.

1. Кобозєва А.А., Хорошко В.О. Аналіз захищеності інформаційних систем. К.: Вид. ДУІКТ, 2010. 309 с.

Вимоги до простежуваності та обґрунтованості результатів вимірювання критичності кіберінцидентів

УДК 004.056:006.91

Ярослав Тарасенко[1], Роман Орлов[2]

[1]Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, yaroslav.tarasenko93@gmail.com,
[2]Державний університет інформаційно-комунікаційних технологій, romanorlov0110@gmail.com

У сучасних інформаційно-комунікаційних системах важливою умовою обґрунтованого реагування та вибору пріоритетів подальших дій є визначення критичності кіберінцидентів. У задачах реагування на кіберінциденти результат вимірювання критичності є основою для прийняття рішень. У роботі [1] автоматизована класифікація кіберінцидентів за рівнями тяжкості ґрунтується на наборі ознак і моделей їх інтерпретації. Підсумкова оцінка критичності повинна бути простежувана та спиратися на цифрові спостереження.

Перша вимога полягає у простежуваності результату до вихідних даних. Кожна оцінка повинна бути відновлювана на основі журналів подій, телеметрії, засобів виявлення та інших відомостей, використаних для її формування. Друга вимога простежуваності відноситься до обробки інформації та полягає у фіксації послідовності обробки даних і формуванні правил переходу від спостережень до підсумкової оцінки. Такий підхід ґрунтується на охопленні сутності, процесів та користувачів, пов’язаних з історією даних, що представлено у роботі [2]. До третьої вимоги варто віднести структурну обґрунтованість результату. Під структурною обґрунтованістю мається на увазі потребу у врахуванні впливу сукупності змістовних компонентів та контексту події на оцінку критичності. Четверта вимога, пов’язана з пояснюваністю, націлена на можливість демонстрації шляхів формування підсумкового результату критичності за рахунок ознак, вагових коефіцієнтів та порогових значень. Доцільність такої вимоги пояснена у роботі [3], де непрозорість моделей виступає чинником зниження довіри до кібербезпекових рішень, зокрема з використанням штучного інтелекту. П’ятою вимогою є відтворюваність результату. Отже, простежуваність даних і перетворень,