5. Котенко І.В., Крибель А.М., Лаута О.С., Саєнко І.Б. Аналіз процесу самоподібності мережевого трафіку як підхід до виявлення кібератак на комп'ютерні мережі // Електрозв'язок. 2020. № 12. С.54-59.

УДК 004.056.5:621.397.12

Кунцов М.С., здобувач 3 курсу
спеціальність 125 «Кібербезпека»
Наукові керівники:
Загоруйко Л.В., к.т.н., доцент, доцент кафедри інформаційних технологій
Мартьянова Т.А. к.т.н., ст. викладач кафедри інформаційних технологій

СТАТИСТИЧНИЙ СТЕГАНОАНАЛІЗ ФОТОРЕАЛІСТИЧНИХ ЗОБРАЖЕНЬ

Донецький національний університет ім. Василя Стуса, м. Вінниця

В результаті дослідження експериментально здійснено підбір оптимальних, параметрів алгоритму знаходження градієнтних шляхів. Отримано та проаналізовано результати застосування моделей машинного навчання, визначено оптимальний масштаб ядра *SVM*-регресора. Розраховано час обчислення векторів ознак, навчання моделі, розпізнавання контейнерів. Показано, що вектор ознак на основі градієнтних шляхів доцільно використовувати для вирішення завдань, де необхідно варіювати точність виявлення вкладення в залежності від навантаження на систему стеганоаналіті, оскільки цей вектор ознак дозволяє визначити співвідношення розмірність/точність. Також шляхом експерименту підібрано комплексний вектор з кількох одновимірних кількісних стеганодетекторів і вектора ознак на основі градієнтних шляхів, ефективність якого можна порівняти з вектором ознак *SPAM*.

Ключові слова: вектор ознак, градієнт яскравості, стеганодетектор, машинне навчання, регресія, машина опорних векторів, просторова область зображення, найменш значні біти, сегментація бітової площини за складністю.

Вступ

Основою статистичного стеганоаналізу зображень є факт порушення певних закономірностей зображення, спричинений реалізацією стегановкладення. Одна з класифікацій існуючих методів стеганоаналізу (сигнатурні, статистичні, евристичні) дозволяє віднести до групи статистичних методи, які ґрунтуються на зіставленні характеристик узагальнених порожнього і заповненого зображень, іншими словами, оцінюють близькість досліджуваного зображення до реального.

Статистичні методи є засобом, що дозволяє гарантовано визначати наявність прихованої інформації. Вони дають можливість аналітику з певною ймовірністю судити про те, чи використовується стеганографія чи ні. Результати роботи методів залежать від стеганографічного перетворення, що використовується для вбудовування даних, що приховуються, а також від їх обсягу. Як правило, виявлення факту приховання можна здійснити при значному заповненні зображення. До того ж методи цієї групи зазвичай побудовані на алгоритмах, що вимагають попереднього навчання на серіях із заповнених і порожніх зображеннях.

Однією з ознак фотореалістичності є плавна зміна освітленості сцени. Таким чином, за інших рівних, стегановкладення має вносити більш значні спотворення в групу пікселів, розташованих уздовж лінії градієнта яскравості. Отже, виникає завдання перевірити цю гіпотезу шляхом побудови градієнтних шляхів та проведення обчислювального експерименту.

Слід зазначити, що моделі на основі градієнта в стеганоаналізі просторової області зображення успішно застосовуються, зокрема, для виявлення фонових областей.

Порівняння стеганоаналітичних векторів ознак на основі середньоквадратичної помилки та коефіцієнта детермінації, отриманих за допомогою *SVM*-регресії у *Matlab* покращило точність стеганоаналізу до 10% порівняно з модифікацією *WSPAM*.

Узагальнена схема проведення експерименту подана на рис.1.

Статистичний стеганоаналіз фотореалістичних зображень.

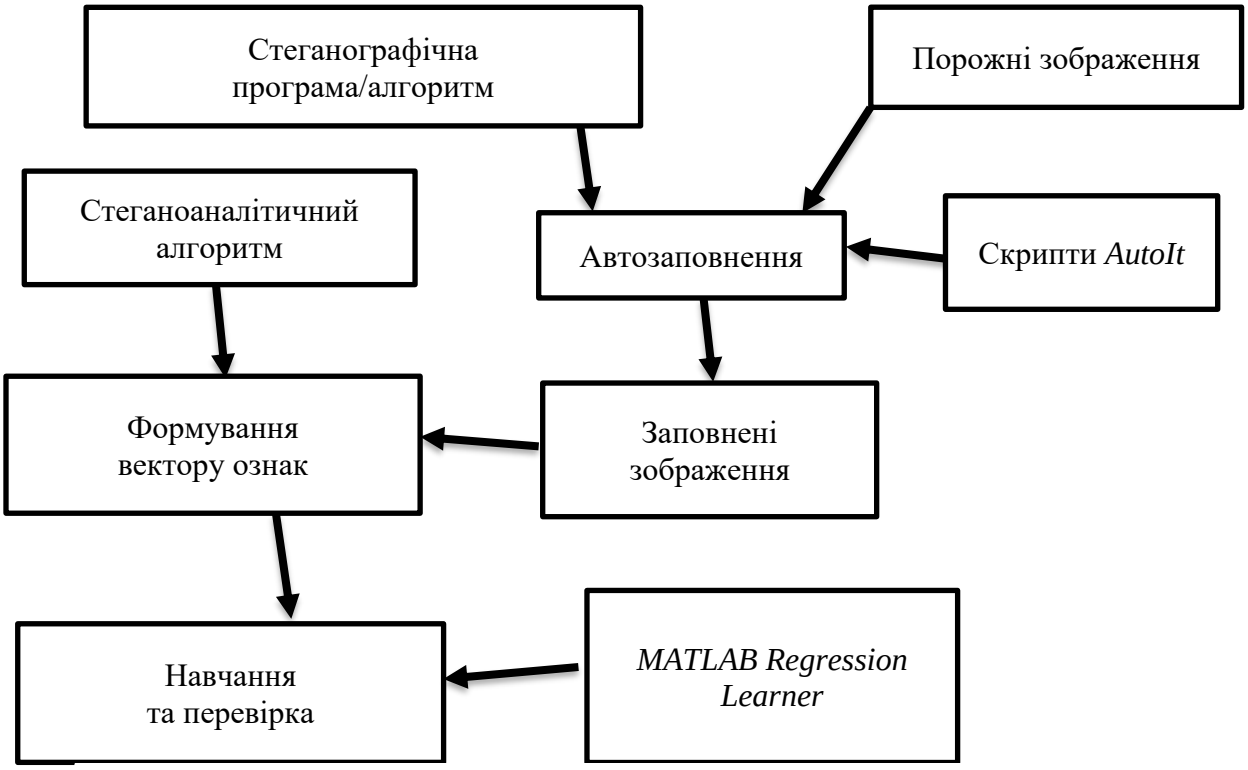

Рис. 1. Узагальнена схема проведення експерименту

Метою експерименту є перевірка вектора ознак на стеганопрограмах сегмента *freeeware*, що реалізують вкладення в просторову область зображення з послідовним і псевдовипадковим вибором пікселя для впровадження та порівняння з відомими стеганоаналітичними детекторами. Спочатку формується безліч заповнених з певним кроком стеганозображень. Для цього використовується середовище розробки *AutoIt*. Розмір вкладення розраховується у відсотках від максимального значення, яке зчитується зі стеганопрограми. Файл вкладення вирізається із випадкового місця випадкового *jpeg*-файла, потім архівується за допомогою *WinRar*. Таким чином, можна бути впевненим у тому, що якщо в стеганопрограмі присутня попередня архівація вкладення, то це не завадить експерименту. Далі до зображень застосовується стеганоаналітичний алгоритм, зіставляючи кожному файлу трасологічні дані. Ці дані можна комбінувати в різні за розміром і складом вектори ознак з подальшим навчанням, що визначає схему експерименту (рис.1). В експерименті використовується традиційне машинне навчання з учителем, але на відміну від аналогічних робіт з дослідження комбінацій <стеганографічний алгоритм, вектор ознак, класифікатор>, де стеганографічна модифікація моделюється або використовується « чистий» алгоритм (*HUGO, S-UNIWARD*), застосований підхід дозволяє врахувати особливості стеганоалгоритма з невідомими параметрами, реалізованого в конкретної програми, що важливо в рамках атак на рівні зображення на підставі відомої стеганопрограми.

Розробники стеганографічних алгоритмів намагаються реалізувати вкладення з якнайменшим спотворенням статистичних властивостей зображення. Особливо це стосується стеганоалгоритмів, що модифікують кілька бітових площин, а не тільки площину *LSB*. Наприклад, *BPCS*-стеганографія (*Bit Plane Complexity Segmentation steganography*) використовує для ухвалення рішення про впровадження даних оцінку складності зображення, для чого здійснюють декомпозицію бітових зрізів на блоки 8x8, підрахунок числа переходів між чорним та білим значенням у кожному рядку та стовпці для блоку. Підхід заснований на особливостях людського зору, яке сприйнятливе до внесення змін до низькочастотних областей зображення, але не може розрізнити зміни у високочастотних (шумових) областях.

Суть методу полягає у заміні шумових блоків на блоки з приховуваною інформацією, з урахуванням їхньої складності. Якщо блок недостатньо складний, то на нього накладається висококонтрастна маска (рис.2, 3,4).

Рис. 2. Модифікація зображення програмою Cryptarkan 1.0

Рис. 3. Модифікація зображення програмою The Third Eye 1.0

Рис. 4. Модифікація зображення програмою Qtech-Hide&View v02

Достовірність висновків забезпечена формуванням зображень безпосередньо за допомогою стеганографічного додатку, значним обсягом тестової вибірки, використанням програмного середовища *Matlab*.

Список використаних джерел

1. Шніперов А.М., Прокоф'єва А.В. Метод стеганоаналізу статичних зображень формату JPEG на основі штучних імунних систем // Питання кібербезпеки. 2020. № 2 (36). З. 22-31. DOI: 10.21681/2311-3456-2020-2-22-31.

2. Башмаков Д.А. Точність передбачення пікселів фонових областей цифрових зображень у задачі стеганоаналізу методом Weighted Stego // Кібернетика та програмування. 2018. №2. З. 38-47.
3. Сівачов А.В., Прохожев Н.М., Михайличенко О.В., Башмаков Д.А. Ефективність стеганоаналізу на основі методів машинного навчання// Питання кібербезпеки. 2017. №2 (20). 3. 53-60. DOI: 10.21681/2311-34562017-2-53-60.
4. Макаренко С.І. Еталонна модель взаємодії стеганографічних систем та обґрунтування на її основі нових напрямків розвитку теорії стеганографії// Питання кібербезпеки. 2014. №2 (3). С. 24-32.
5. Парасич А. В., Парасич В. А., Парасич І. В. Формування навчальної вибірки в завданнях машинного навчання // Інформаційно-керуючі системи. 2021. № 4. С.61-70.
6. Atlasov I., Solodukha R. Cample Representativeness Estimation як Preliminary Stage of Statistical Steganalysis / 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), 2021, pp. 78-84.

УДК 004.056.53:621.39(043.2)

Ласкавчук М.А.
здобувач вищої освіти
Зелінська О.В.,к.т.н., доцент
доцент кафедри інформаційних технологій

ЗАСОБИ ТА ЗАХОДИ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

Фізичні засоби захисту - це засоби, необхідні для зовнішнього захисту обчислювальної техніки, об'єктів на базі ПК, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищається [1].

Надійним і простим заходом, щоб захистити інформацію від загроз несанкціонованого доступу є режим автономного використання комп’ютера одним користувачем у спеціально виділеному приміщенні, доступ до якого наданий лише одній особі. Замкненим контуром захисту є виділене приміщення, а захистом фізичним - підлого, вікна, стеля, стіни та двері. Якщо стеля, стіни, двері і підлога міцні, вікна і двері обладнані сигналізацією, підлога не має люків, які з'єднуються з іншими приміщеннями, то стійкість захисту визначається технічними характеристиками сигналізації при відсутності користувача в неробочий час.

Більш складні засоби контролю доступу включають технологічний підхід. Сканери ідентифікаційних карток і ідентифікаційні картки - це методи фізичної аутентифікації, які служби безпеки можуть використовувати для перевірки осіб, які входять і виходять з різних об’єктів. Використовуючи тактично встановлені перешкоди, організації можуть ускладнити зловмисникам доступ до цінних