Впровадимо оптимізації до штучного інтелекту за допомогою мутацій та схрещувань. Проженемо отриману мережу ще раз, проаналізуємо отримані результати.

Висновки

В результаті отримаємо навчений штучний інтелект та отримаємо ефективність навчання за допомого генетичного алгоритму. Візуалізуємо результати в розробленій програмі. Запишемо вихідні дані та проаналізуємо їх.

Список використаної літератури

1. Баранов, О. А. (б.д.). ІНТЕРНЕТ РЕЧЕЙ І ШТУЧНИЙ ІНТЕЛЕКТ: ВИТОКИ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ. Получено из APhD: http://aphd.ua/publication-376/
2. Глибовець, М. М., & Гороховський, С. С. (2011). Гібридний генетичний алгоритм вирішення задачі оптимізації структури інтегральної схеми. Харків. Отримано з https://core.ac.uk/download/pdf/296368997.pdf
3. Троцько, В. В. (2020). Методи штучного інтелекту. Київ. Отримано з https://library.krok.edu.ua/media/library/category/navchalni-posibniki/trotsko_0001.pdf

УДК 519.6

Парамонова К.О., *студентка 4 курсу спеціальності 124 «Системний аналіз»*
Шевченко Н.Ю., *к.е.н., доцент, доцент кафедри інтелектуальних систем прийняття рішень*

ПРОЕКТУВАННЯ МОДУЛЯ ДЛЯ ГЕНЕРАЦІЇ ОКРЕМИХ ЕЛЕМЕНТІВ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ

Донбаська державна машинобудівна академія, м. Краматорськ

Для вирішення проблеми захисту інформації від несанкціонованого доступу виділяють два основних шляхи: криптографію й стеганографію. На відміну від криптографії, яка приховує вміст секретного повідомлення, стеганографія приховує сам факт його існування в деякому контейнері.

Для забезпечення надійності даних, що передаються, доцільно забезпечити не тільки їх шифрування, але й приховування. Надійність передачі даних через відкритий канал зв’язку може бути забезпечена використанням стеганографічної системи.

В загальному випадку стеганосистему можна представити як сукупність $\sum(C, M, S, E, D)$ – контейнерів, повідомлень та перетворень, що їх зв’язують. Припустимо, що в якості повідомлення передаються згенеровані випадковим чином дані: логін і пароль. Завжди контейнери обираються таким чином, щоб заповнений контейнер майже не відрізнявся від порожнього контейнера. В якості візуальних контейнерів можуть використовуватися фрактали. Серед поширених

фракталів виділяють три основні групи [1]: алгебраїчні фрактали, геометричні фрактали, стохастичні фрактали.

Для забезпечення більшої надійності поряд з приховуванням даних доцільно застосувати ще шифрування даних, наприклад, методом RSA. Далі зашифроване повідомлення ховається в молодших бітах зображення-фрактала.

Отже, алгоритмічна модель програми для безпечної передачі даних через відкритий канал зв'язку передбачає реалізацію п'яти етапів:

1. Генерація логіна і пароля.
2. Побудова стохастичного фрактала «Плазма».
3. Шифрування логіна і пароля алгоритмом RSA.
4. Приховування зашифрованого повідомлення в молодших бітах зображення-фрактала методом LSB – Least Significant Bits.
5. Відправлення зображення на електронну адресу користувача.
6. Розшифрування та витягування логіну та паролю з фрактала «Плазма».

Для побудови стохастичного фракталу «Плазма» найбільш підходить алгоритм Diamond Square. Спочатку чотирьом кутам квадрата присвоюються випадкові величини. Після того, як задані кордони квадрата, він розбивається на чотири рівних квадрати, в кожному з яких відомо значення одного з кутів. Значення висоти центральної точки – сума усереднення висот всіх чотирьох кутових точок і випадкового значення (шуму).

Виростання стохастичних фракталів дозволяє кожен раз отримувати унікальний стегоконтейнер для приховування інформації, яка передається відкритими каналами зв'язку.

Сутність методу заміни найменш значущого біта LSB полягає в приховуванні інформації шляхом зміни останніх бітів зображення, які кодують колір на біти приховуваного повідомлення.

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів. Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі – відкритий (public) і закритий (private), разом відкритий і відповідний йому закритий ключі утворюють пари ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним закритим ключем.

Діаграма варіантів використання модуля для генерації окремих елементів стеганографічної системи наведена на рис. 1.

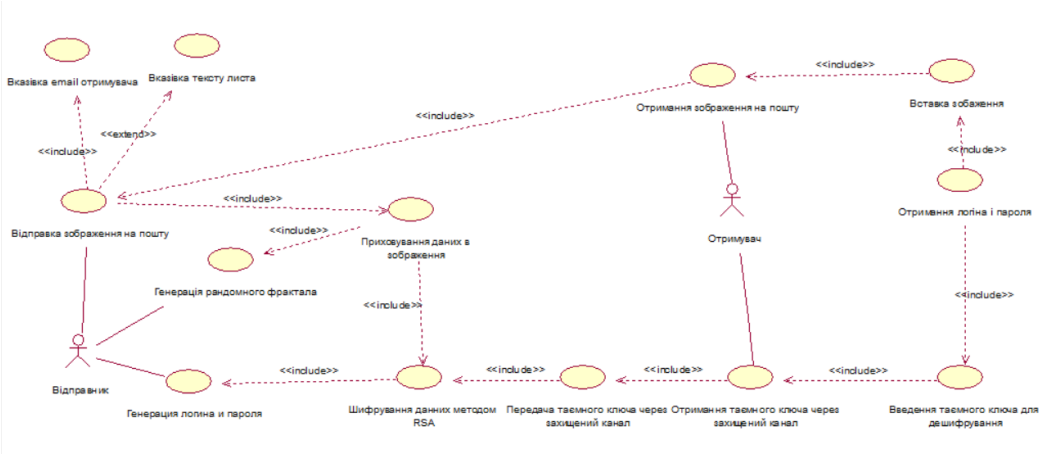

Рисунок 1 – Діаграма варіантів використання

На даній діаграмі дійовими особами або акторами є відправник та отримувач таємного повідомлення, варіанти використання показують, які дії може виконувати актор, лінії і стрілки, що з'єднують прецеденти –різного роду зв'язки між користувачем і варіантами використання.

Зв'язком простої асоціації актор «Відправник» пов'язаний з прецедентами «Генерація рандомного фрактала» і «Генерація логіна і пароля». Це говорить про те, що при першому запуску програми маємо дві головні послідовності сценарію. При виборі «Генерація рандомного фрактала» відправник може приховувати дані в зображення, відправляти зображення на пошту. При цьому вказівка електронної пошти отримувача є обов’язковою дією, а вказівка тексту листа – ні. При виборі «Генерація логіна і пароля» відправник може шифрувати дані та відправити таємний ключ отримувачу.

Слід зазначити, що приховування інформації в зображення неможливо без шифрування даних, які були згенеровані на етапі зв’язку простої асоціації «Генерація логіна і пароля».

Зв'язком простої асоціації актор «Отримувач» пов'язаний з прецедентами «Отримання зображення через пошту» і «Отримання таємного ключа через захищений канал». Отримання зашифрованих даних включає в себе введення таємного ключа та вставку зображення.

Приклад роботи модуля наведений на рис. 2.

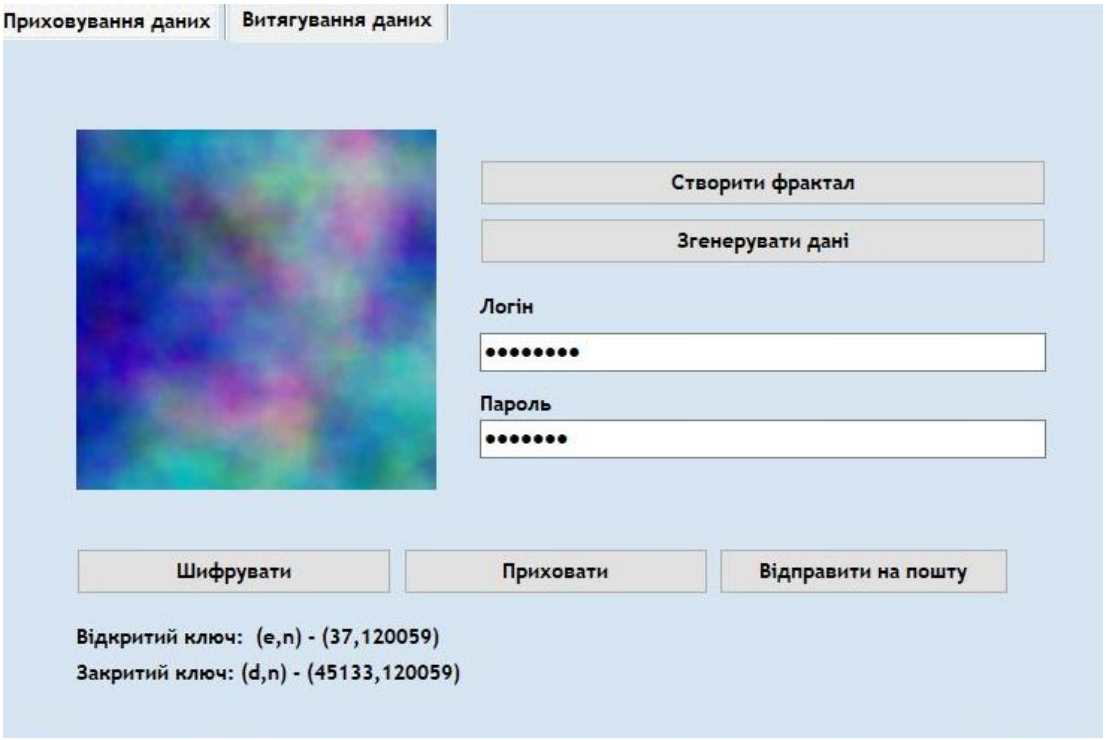

Рисунок 2 – Приклад роботи програми. Приховування даних

Список літератури

1. Фрактали [Електронний ресурс]. – URL: http://www.kpi.kharkov.ua/archive/microcad/2011/%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9.pdf

УДК 004.912

Петричко М.В., *аспірант 1 курсу спеціальності 126 «Інформаційні системи та технології»*
Штовба С.Д., *д.т.н., професор кафедри комп'ютерних наук та інформаційних технологій*

ІДЕНТИФІКАЦІЯ НАУКОВИХ СПЕЦІАЛЬНОСТЕЙ ДОСЛІДНИКІВ НА ОСНОВІ ЇХ ІНТЕРЕСІВ В GOOGLE SCHOLAR

Вінницький національний технічний університет, м. Вінниця
Донецький національний університет імені Василя Стуса, м. Вінниця

Сьогодні професійні спільноти людей взаємодіють в різноманітних онлайнових мережах. Не виключенням є і спільнота дослідників. Найбільшою онлайновою мережею дослідників є Google Scholar. В ній, зокрема, у відкритому доступі є понад 50 тисяч профілів українських дослідників. Такий величезний ресурс виглядає привабливим для розробки технологій аналітичного опрацювання накопиченої в ньому інформації з метою ідентифікації лідерів – статей, науковців, університетів, журналів, виявлення тенденцій наукових