DOI 10.34185/1562-9945-5-162-2026-16
УДК 004.8:621.391

К.Ю. Островська, В.П. Борисюк

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ГЕНЕРАЦІЇ ЗОБРАЖЕНЬ З МОЖЛИВІСТЮ ФЕДЕРАТИВНОГО НАВЧАННЯ ТА ДОНАВЧАННЯ ГЕНЕРАТИВНИХ МОДЕЛЕЙ

Анотація. У роботі розглянуто розробку та дослідження інформаційної системи для генерації зображень на основі сучасних генеративних моделей штучного інтелекту з підтримкою федеративного навчання та механізмів донавчання. Запропонована система орієнтована на забезпечення ефективної генерації візуального контенту з одночасним збереженням конфіденційності даних користувачів, що є особливо актуальним в умовах обмеженого доступу до централізованих наборів даних.

Метою роботи є розробка інформаційної системи для генерації зображень з можливістю федеративного навчання та донавчання генеративних моделей.

Розроблена інформаційна система може бути використана у завданнях, де важливо навчати генеративні моделі без передачі даних на сервер, що забезпечує захист конфіденційною інформації.

У майбутньому планується розширення функціональності системи, у тому числі додавання повноцінної реєстрації та авторизації, можливість застосовувати кілька LoRA-адаптерів одночасно, збільшення доступних для навчання та генерації моделей і реалізація додаткових алгоритмів для федеративного навчання.

Ключові слова: машинне навчання, дифузійні моделі, нейромережа, генеративно-змагальні мережі, тестування, варіаційні автокодувальники, федеративне навчання.

Вступ. Актуальність цієї теми обумовлена стрімким розвитком області машинного навчання і штучного інтелекту, а також зростаючими вимогами до захисту персональних даних.

- Сучасні генеративні моделі потребують великих обсягів даних та обчислювальних потужностей, що ускладнює централізоване навчання.
- Федеративне навчання дає можливість навчати моделі безпосередньо на пристроях користувачів, забезпечуючи захист даних.
- Розподілений підхід зменшує навантаження на центральні сервери.

Метою роботи є розробка інформаційної системи для генерації зображень з можливістю федеративного навчання та донавчання генеративних моделей.

Викладення основного матеріалу. Генеративно-змагальні мережі (Generative Adversarial Networks, GANs), являють собою моделі, у яких дві нейронні мережі (генератор та дискримінатор) навчаються у процесі змагання [1].

GAN - один із алгоритмів класичного машинного навчання, навчання без учителя.

Суть ідеї в комбінації двох нейромереж, при якій одночасно працює два алгоритми "генератор" і "дискрімінатор".

Завдання генератора – створювати образи заданої категорії.

Завдання дискриминатора – намагатися розпізнати створений образ.

Таким чином генератор генерує певні образи. Наприклад, картинки, схожі на обличчя, а дискрімінатор намагається визначити обличчя це було чи ні. І з часом мережа навчається настільки, що генератор генерує досить реалістичні обличчя.

Дискрімінатор. Для розпізнавання використовуються згорткові нейронні мережі (CNN). CNN може розпізнавати образи на картинках, наприклад, виділяти з усього зображення обличчя, цифри тощо Щоб нейронна мережа навчилася щось розпізнавати, їй потрібно обробити велику кількість зображень, де містяться образи, потрібні для пошуку.

Дифузійні моделі (Diffusion Models) – це клас генеративних моделей, заснованих на процесі додавання шуму до даних та навчання нейромережі відновлювати вихідний розподіл [2].

Latent Diffusion Models (LDM) використовує енкодер для перетворення даних більш компактне латентне простір. LDM дозволяє працювати з меншими обсягами даних, що суттєво скорочує обчислювальні витрати [3].

Вихідне зображення x_0 за допомогою енкодера E перетворюється на латентний вектор ознак z_0 згідно з формулою (1):

$$z_0 = E(x_0), \quad (1)$$

де x_0 - зображення;

z_0 – латентне уявлення, що містить основні характеристики зображення 0;

E – енкодер.

Після завершення генерації, підсумковий латентний вектор $\hat{zt}$ декодується в зображення з допомогою декодера D згідно формулою (2):

$$\hat{x_0} = D(\hat{z_0}), \quad (2)$$

де $\hat{x_0}$ - відновлене зображення;

$\hat{z_0}$ - відновлене латентне уявлення;

D - Декодер.

Використання латентного простору дозволяє зменшити розмір даних, що скорочує час навчання та обсяг необхідної пам'яті. Крім того, латентні уявлення більш стійкі до шуму, що покращує якість відновлених зображень на виході.

Stable Diffusion представляє собою реалізацію LDM, розроблену для генерації високоякісних зображень на основі текстових описів [4].

Архітектура Stable Diffusion включає три компоненти – варіаційний автокодувальник (VAE), текстовий енкодер та UNet (рисунок 1).

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

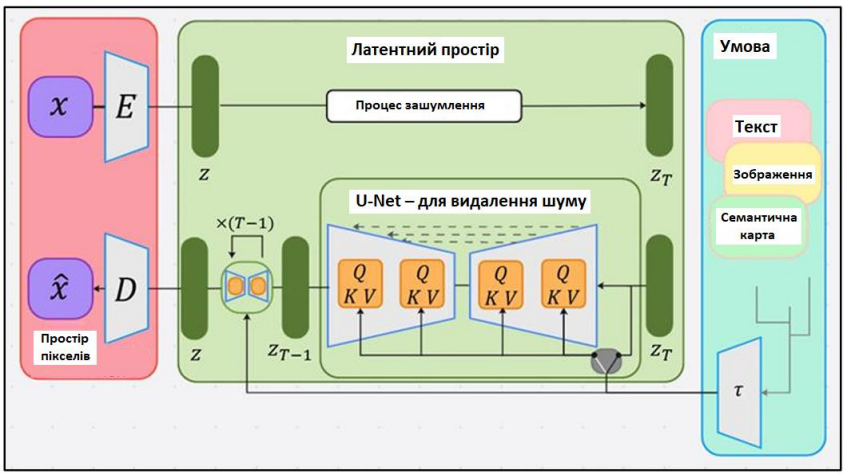

Рисунок 1 - Архітектура Stable Diffusion

Варіаційний автокодувальник (VAE) використовується для перетворення зображень x_0 в латентну виставу z_0 та навпаки.

Текстовий енкодер перетворює текстову підказку c в ембедінг $\tau(c)$, який є числовим вектором, що відображає семантичний зміст тексту. Цей ембеддинг використовується для кожного кроку зворотного дифузійного процесу як умова генерації.

UNet – дифузійна нейронна мережа, що навчається передбачати доданий шум ϵ на кожному кроку t.

Stable Diffusion є гнучкою та потужною архітектурою для генерації зображень. Завдяки відкритому вихідному коду і інтеграцією з LoRA, вона може ефективно використовуватися при розподіленому навчанні, де особливо важливими є економія ресурсів та захист даних. Це робить її оптимальним вибором для застосунку, що розробляється.

Незважаючи на високу якість генерованих зображень, дифузійні, мають велику кількість параметрів, що робить їх навчання на нових даних вкрай ресурсомісткими. Для вирішення цієї проблеми використовується метод LoRA (Low-Rank Adapatation) [5].

Основна ідея LoRA полягає в тому, щоб залишити вихідні ваги моделі незмінними (замороженими) і додати до них низькорангове доповнення. Замість оновлення повної матриці, LoRA навчає дві значно менші матриці.

Даний процес представлений формулою (3):

$$W = W_0 + \Delta W, \tag{3}$$

де W - підсумкова вагова матриця шару;

W_0 - заморожена матриця ваг, отримана з передбаченої моделі;

ΔW - низькорівневе адаптивне додавання до ваг (LoRA-ін'єкція), виражене через матриці A і B;

$A \in \mathbb{R}^{r \times k}$, $B \in \mathbb{R}^{d \times r}$ - учні матриці адаптації;

r - ранг адаптації;

d - розмірність вихідного простору шару;

k - розмірність вхідного простору шару.

Даний підхід дозволяє значно знизити кількість параметрів, що навчаються з $d \times k$ до $r \times (d + k)$, що критично важливо при використанні дифузійних моделей в умовах обмежених обчислювальних ресурсів або для персоналізованої генерації.

Федеративне навчання – це метод машинного навчання, у якому моделі навчаються на розподілених пристроях, без передачі локальних даних на централізований сервер [6].

Процес федеративного навчання має ітеративну процедуру взаємодії між центральним сервером і множеною клієнтів, які мають власні набори даних. На першому етапі сервер ініціалізує глобальну модель і відправляє її параметри всім підключеним клієнтам. Отримавши модель, кожен клієнт проводить локальне навчання на своїх приватних користувальницьких даних, не передаючи самі дані, а лише використовуючи їх для оновлення локальних копій моделі. Після завершення локального навчання клієнти надсилають на сервер оновлені параметри своїх моделей для агрегації, після чого процес повторюється (рисунок 2).

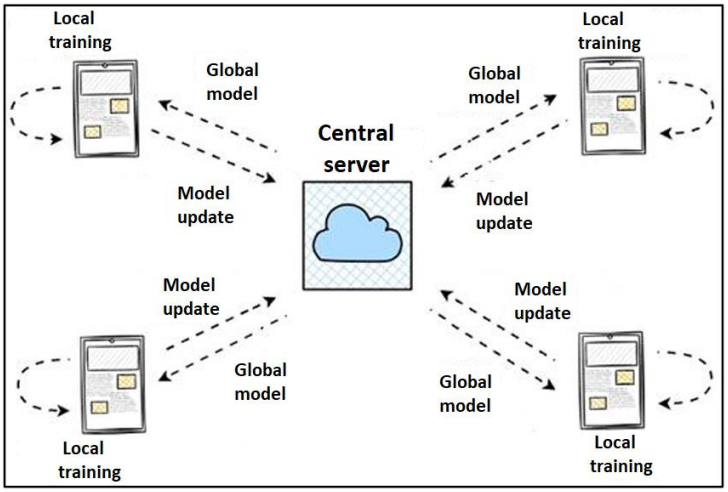

Рисунок 2 - Схема федеративного навчання

Федеративне навчання дифузійних моделей.

FedAvg – це один із найпопулярніших алгоритмів федеративного навчання, заснований на усереднення локальних оновлень моделей, навчених на даних клієнтів [6]. Глобальна модель представлена параметрами, які оновлюються згідно з формулою (4).

$$\omega^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_k^{(t+1)}, \tag{4}$$

де: $\omega^{(t+1)}$ - параметри глобальною моделі на ітерації $t + 1$;

$\omega^{(t+1)}$ - параметри локальною моделі на клієнта k на ітерації $t + 1$;

n_k - кількість даних на клієнта k ;

n - загальне кількість даних;

K - загальне кількість клієнтів.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Незважаючи на свою простоту та ефективність в умовах однорідних даних, FedAvg стикається з труднощами при роботі з неоднорідними даними. У таких ситуаціях локальні моделі можуть сильно відхилятися від глобальної, що сповільнює збіжність або наводить до нестійких результатів.

Як базовий алгоритм федеративного навчання у своєму зостасунку обрано FedAvg – надійне і поширене рішення, яке відрізняється простотою реалізації.

LoRA – це метод донавчання великих моделей, який додає до вихідних лінійних шарів низькорангові матриці $A \in \mathbb{R}r\times k$ та $B \in \mathbb{R}d\times r$, де r – ранг, а k та d – розміри вихідних шарів моделі Замість донавчання всіх ваг, LoRA навчає матриці A і B залишаючи ваги фіксованими.

Алгоритм FedEx-Lora [7], розроблений для роботи з великомасштабними мовними моделями, вирішує проблему за допомогою залишкового оновлення, як показано у формулі (5):

$$W_0^{(t+1)} = W_0^t + \underbrace{\left(\frac{1}{K}\sum_{k=1}^{K} B_k^t A_k^t\right) - \left(\frac{1}{K}\sum_{k=1}^{K} B_k^t\right)\left(\frac{1}{K}\sum_{k=1}^{K} A_k^t\right)}_{\Delta W^t}, \quad (5)$$

де: $W_0{}^{(t+1)}$ – оновлені параметри замороженої моделі для $t + 1$

$W_0{}^t$ – параметри замороженої моделі на ітерації t

$B_k{}^t$ та $A_k{}^t$ – локальні матриці на клієнті k

ΔW^t – коригуюче оновлення, яке компенсує різницю між усередненим твором та твором усереднених матриць

K– кількість клієнтів

У FedEx-LoRA параметри базової моделі W_0 оновлюються на кожному раунді навчання, що фактично означає часткове навчання базової моделі.

Враховуючи особливості та переваги даного підходу, для реалізації федеративного навчання LoRA в зостасунку був обраний алгоритм FedEx-LoRA – як оптимальне рішення для коректної агрегації та підвищенні якості моделі.

Система, що розробляється, є клієнт-серверним застосунком, призначеним для генерації, донавчання та агрегації генеративних моделей і LoRA-адаптерів у рамках федеративного навчання. Система складається з серверної та клієнтської частин, що взаємодіють між собою по мережі через API. Сервер здійснює управління моделями, зберігання та агрегацію оновлень, а також координацію обміну даними. Клієнтська частина забезпечує взаємодію користувача з системою, а також виконує донавчання моделей та роботу з даними.

Діаграма послідовності, представлена на рисунку 3, ілюструє взаємодія користувача, клієнтської і серверна частин додатки у процесі федеративного навчання. На діаграмі відображено ключові етапи роботи системи: отримання моделі, локальне донавчання, надсилання оновлень та їх агрегація на сервері.

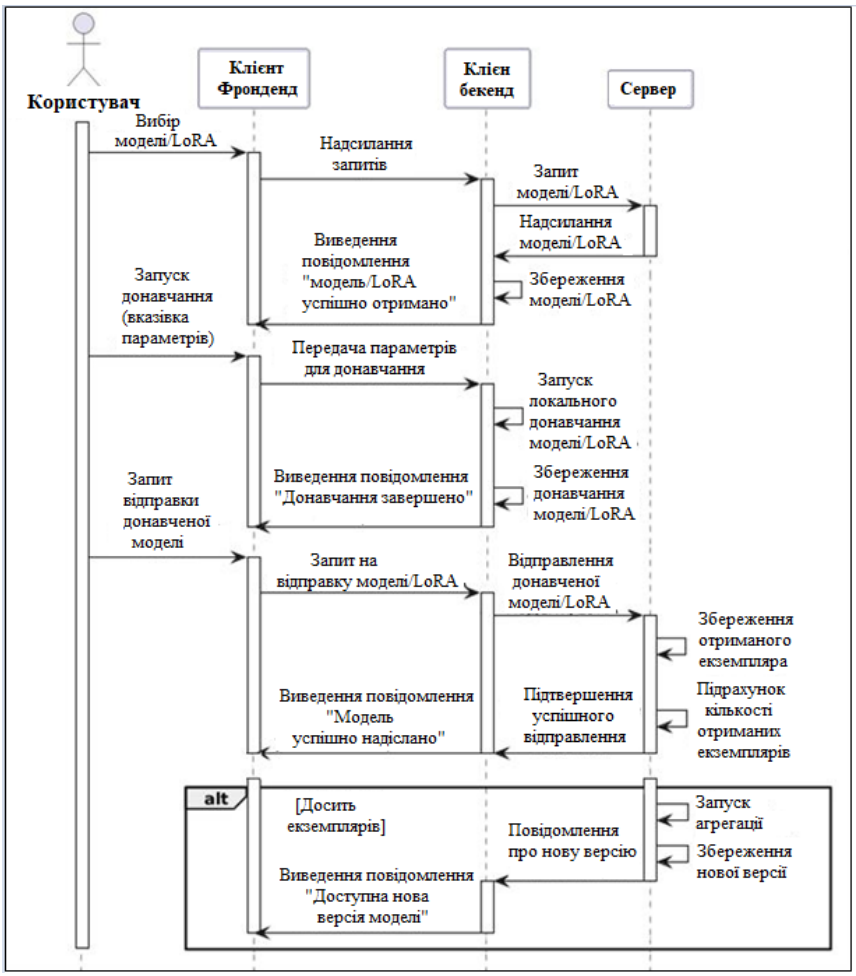

Рисунок 3 - Діаграма послідовності федеративного навчання

FedFlowServer є застосунком з використанням фреймворку Flask, що реалізує роботу сервера [8]. Сервер організований за модульним принципом з використанням окремих сервісів, кожен з яких відповідає за виконання конкретного завдання - генерацію UUID (Universally Unique Identifier), агрегацію моделей, роботу з файлами. Такий підхід забезпечує масштабованість, читаність коду та спрощує супровід системи.

FedFlow є клієнтським додатком, який забезпечує зручний інтерфейс для взаємодії з сервером, отримання інформації про моделі та LoRA-адаптери, а також дозволяє користувачам працювати з локальними даними.

Забезпечує:

- Взаємодію з сервером.
- Роботу з датасетами.
- Генерацію зображень.
- Навчання моделей і LoRA- адаптерів.
- Реалізацію користувальницького інтерфейсу.

Приклади текстового опису представлено на рисунку 4.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

```
"Van_Gogh, outdoors, sky, cloud, "
"signature, no_humans, night, traditional_media, "
"moon, night_sky, scenery, full_moon, "
"mountain, crescent_moon, acrylic_paint_(medium)"
```

Рисунок 4 - Приклади текстового опису

Тестування і аналіз результатів. Для оцінки якості федеративного навчання використовувалась метрика FID, що порівнювала розподіли згенерованих зображень та реальних даних. Як датасет використовувалися зображення Сема Альтмана - генерального директора OpenAI. Модель Stable Diffusion 1.5 з донавчаням через LoRA навчалася на п'яти клієнтах з нерівномірним розподілом даних: 20, 40, 60, 40 і 40 зображень. Навчання проходило у три раунди, кількість кроків на кожному клієнті розраховувалася на основі обсягу даних, розміру батча та числа епох, за однакових параметрів. Після кожного раунду за допомогою поточної версії моделі генерувалися зображення, на основі яких розраховувалося значення FID щодо тестової вибірки. Для порівняння також проводилося централізоване навчання моделі на повному наборі з 200 зображень. Значення метрики FID для централізованого навчання - 124,34.

Результати всіх проведених експериментів наведено в таблиці 1.

Таблиця 1

Результати експериментів

Раунд	Клієнт 1	Клієнт 2	Клієнт 3	Клієнт 4	Клієнт 5	Агрегована модель
1	178,39	165,66	147,22	166,21	175,23	150,51
2	168,57	155,09	140,83	150,42	162,77	138,04
3	160,48	150,5	135,77	152,39	157,26	133,85

Експерименти показали стійке покращення якості моделі з кожним раундом федеративного навчання, незважаючи на відмінності в обсягах даних клієнтів. Значення FID агрегованої моделі стабільно знижуються, що свідчить про зростання якості зображень. Хоча централізоване навчання на повному наборі даних дає кращі результати, федеративний підхід з використанням LoRA залишається ефективним при обмежених обчислювальних ресурсах та гетерогенності даних, забезпечуючи при цьому гідну якість зображень та знижуючи ризик витоку даних. Також проведено функціональне тестування системи за 14 основними сценаріями. Усі тести успішно пройдено, що підтверджує коректну роботу реалізованих компонентів [9].

Висновки. В результаті було розроблено інформаційну систему для генерації зображень з можливістю федеративного навчання та донавчання генеративних моделей.

Розроблена інформаційна система може бути використаа у завданнях, де важливо навчати генеративні моделі без передачі даних на сервер, що забезпечує захист конфіденційної інформації.

ЛІТЕРАТУРА / REFERECES

1. Goodfellow I. Pouget-Abadie J. Mirza M. et al. Generative Adver- sarial Networks. Electronic resource] // arXiv.org. 2014 року. URL:https://arxiv.org/pdf/1406.2661
2. Ho J., Jain A., Abbeel P. Denoising Diffusion Probabilistic Модель. [Electronic resource] / / arXiv.org. 2020. URL: https://arxiv.org/pdf/2006.11239
3. Rombach R., Blattmann A., Lorenz D., et al. High-Resolution Image Synthesis with Latent Diffusion Models. [Electronic resource] // arXiv.org. 2022. URL: https://arxiv.org/pdf/2112.10752
4. Xiang C., Wang L., Zhou M. Comparative Analysis of Generative Models: Enhancing Image Synthesis with VAEs, GANs, and Stable Дифузія. [Electronic resource] // arXiv.org. 2023. URL: https://arxiv.org/pdf/2408.08751
5. Stable Дифузія. [Electronic resource] URL: https://hugging-face.co/blog/stable_diffusion
6. Hu EJ, Shen Y., Wallis P., et al. LoRA: Low-Rank Adaptation of Large Language Models. [Electronic resource] // arXiv.org. 2021. URL:https://arxiv.org/pdf/2106.09685
7. Yao Y., Gao T., Li W., et al. FedEx-LoRA: Exact Aggregation for Federated and Efficient Fine-Tuning of Foundation Models. [Electronic resource] // arXiv.org. 2025. URL:https://arxiv.org/pdf/2410.09432
8. Kairouz P., McMahan HB, Avent B., та інші. Advances and Open Problems in Federated Learning. [Electronic resource] // arXiv.org. 2021. URL: https://arxiv.org/pdf/1912.04977
9. Ostrovska K., Borysiuk V. «IMAGE GENERATION WITH THE ABILITY TO ENABLE FEDERATED TRAINING AND FURTHER TRAINING OF GENERATIVE MODELS» // the 3rd International Scientific and Practical Conference. International Scientific Unity. November 12-14, 2025. Lisbon, Portugal. P 203-206.

Received 14.01.2026.
Accepted 16.01.2026.

Information system for image generation with the possibility of federated learning and further training of generative models

The paper discusses the development and research of an information system for image generation based on modern generative artificial intelligence models with support for federated learning and retraining mechanisms. The proposed system is focused on ensuring effective generation of visual content while maintaining the confidentiality of user data, which is especially relevant in conditions of limited access to centralized data sets.

The research analyzes the architecture of the information system, the principles of integration of generative models, as well as approaches to organizing federated learning, in which model parameters are updated on local nodes without transmitting the output data to the central server. Particular attention is paid to methods of retraining models, which allow the system to adapt to new types of images, styles and user requirements during operation.

The performance and efficiency of the proposed system are evaluated in terms of the quality of generated images, learning speed and resistance to changes in input data. The results obtained confirm the feasibility of using a federated approach and further training of generative models to create scalable, adaptive, and secure image generation information systems.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

In the future, it is planned to expand the functionality of the system, including adding full registration and authorization, the ability to use multiple LoRA adapters simultaneously, increasing the number of models available for training and generation, and implementing additional algorithms for federated learning.

Островська Катерина Юріївна – доцент, к.т.н., доцент кафедри інформаційних технологій і систем ННІ ДМетІ Українського державного університету науки і технологій.
ORCID: https://orcid.org/0000-0002-9375-4121
Борисюк Володимир Петрович - магістр кафедри інформаційних технологій і систем ННІ ДМетІ Українського державного університету науки і технологій.
ORCID: https://orcid.org/0009-0008-0696-6523

Ostrovska Kateryna - – Associate Professor, Candidate of Technical Sciences, Associate Professor of the Department of Information Technologies and Systems, NNI DMetI, Ukrainian State University of Science and Technology.
ORCID: https://orcid.org/0000-0002-9375-4121
Borysiuk Volodymyr - Master of the Department of Information Technologies and Systems, NNI DMetI, Ukrainian State University of Science and Technology.
ORCID: https://orcid.org/0009-0008-0696-6523