УДК 004.056:[004.62:61] DOI: https://doi.org/10.30837/IYF.IIS.2024.099

АНОНІМІЗАЦІЯ ДАНИХ В ІНТЕЛЕКТУАЛЬНИХ МЕДИЧНИХ СИСТЕМАХ

Воронова Д. С.
Наукові керівники – к.т.н., доцент каф. ШІ Чала Л. Е., к.т.н., доцент каф. ШІ Головянко М. В.
Харківський національний університет радіоелектроніки, каф. ШІ, м. Харків, Україна
e-mail: daria.voronova@nure.ua

The importance of digitizing the medical sector and anonymizing medical data for safeguarding patient privacy cannot be overstated. This work explores machine learning methods for anonymizing medical data, focusing on techniques like Generative Adversarial Networks (GANs) and Perturbation Methods. It emphasizes the automated nature of these methods and their ability to maintain data utility while preserving patient confidentiality.

Specifically, the application of GANs, such as medGAN, demonstrates their effectiveness in generating synthetic medical data and addressing data imbalance issues while ensuring patient privacy.

Діджиталізація медичної галузі передбачає перехід від паперових записів до електронних систем зберігання медичної інформації, впровадження телемедицини, розробку програмних засобів для моніторингу здоров'я та використання алгоритмів машинного навчання для аналізу, прогнозування та підтримки прийняття рішень. Це сприяє покращенню доступності та ефективності медичних послуг, але вимагає уваги до захисту даних, конфіденційності та етичних аспектів.

Зберігання та обробка медичних даних відповідно до встановлених стандартів конфіденційності та безпеки є критично важливою. Етичні стандарти визначають правила поведінки та взаємодії в медичній сфері, гарантуючи захист конфіденційності та прав пацієнтів, а також етичне використання їхніх особистих даних. Хакерські атаки на медичні системи призводять до витоку конфіденційної інформації, яку зловмисники можуть використати для різних видів шахрайства та блокування роботи важливих медичних систем, створюючи пряму загрозу безпеці пацієнтів. Один зі способів захисту медичних даних – анонімізація, іншими словами, видалення ідентифікаторів особи, а також узагальнення будь-яких ознак, які можуть бути використані для встановлення зв'язку з конкретною людиною.

Важливими аспектами анонімізації є збереження: корисності даних (вимірюється кількістю втрат, спричинених технікою анонімізації, наприклад, втратою інформації), конфіденційності (вимірюється відповідністю даних обмеженням моделі конфіденційності) та правдивості

даних (кожен анонімізований запис відповідає єдиному запису в оригінальній таблиці).

Традиційно для анонімізації використовують такі методи [1], [2]:

1) слайсинг – поділ даних на групи за допомогою вертикального та горизонтального розбиття для групування атрибутів з високою кореляцією;

2) узагальнення – замінює значення атрибутів, що можуть ідентифікувати особу, менш специфічними значеннями;

3) приховування та переміщення – полягають у видаленні або зміні пропущених значень квазіідентифікаторів;

4) пертурбація – додавання шуму;

5) бакетизація – відокремлює чутливі атрибути від квазіідентифікаторів шляхом випадкової перестановки або заміни місцями значень чутливих атрибутів;

6) мікроагрегація – заміна значень груп з k-найближчих записів кластеру їхнім центроїдом;

7) маскування даних.

Традиційні методи анонімізації часто ведуть до втрати важливих властивостей даних, що може позначитися на ефективності подальшого використання анонімізованих даних, зокрема, в інтелектуальних системах. Наприклад, для систем, які навчаються на даних, для високої точності майбутніх прогнозів важливим є збереження оригінального розподілу даних.

Саме тому, було обрано методи машинного навчання для анонімізації даних, які набувають все більшої популярності. Їхньою перевагою є автоматичність анонімізації без необхідності ручного втручання. Ці методи доцільно використовувати, коли необхідно поєднати конфіденційність даних (неможливість ідентифікації особи) із збереженням структури та статистичних властивостей даних для ефективного навчання інтелектуальних моделей. Серед обраних методів:

– Генеративно-адверсаріальні мережі (GAN), які генерують реалістичні анонімізовані дані, зберігаючи структуру оригінальних даних, які не можуть бути використані для встановлення зв'язків з конкретною людиною. Ці моделі складаються з двох нейронних мереж – генератора і дискримінатора, які змагаються між собою. Генератор вчиться створювати нові синтетичні (анонімізовані) дані, максимально подібні на навчальні, тоді як дискримінатор використовується для оцінки того, наскільки оригінальні дані відрізняються від синтетичних.

– Методи Пертурбацій (Perturbation Methods), які переважно використовуються для анонімізації числових або текстових даних.

В роботі запропоновано поєднання GAN та реалістичних синтетичних даних в медичних системах на основі мережі medGAN [2]. Її впроваджено для генерації дискретних записів пацієнтів із декількома мітками за допомогою комбінації автокодувальника та GAN. Така мережа підтримує

генерацію як двійкових, так і числових змінних (тобто медичних кодів, таких як діагноз, ліки та коди процедур) і розташування записів у матричному форматі, де кожен рядок відповідає пацієнту, а кожен стовпець представляє конкретний медичний код. Крім того, GAN також використовувалися для сегментації медичних зображень (тобто сканування магнітно-резонансної томографії головного мозку), одночасно справляючись із захистом конфіденційності та дисбалансом набору даних. Іншими словами, мережі GAN довели свій потенціал у розширенні даних для незбалансованих наборів даних і анонімізації даних для збереження конфіденційності.

Таким чином, методи навчання на основі генеративно-адверсаріальних мереж мають великий потенціал, з урахуванням зростання важливості цифрових систем у сфері охорони здоров'я та необхідності захисту конфіденційної інформації пацієнтів. Ці методи не лише сприяють створенню синтетичних медичних даних, але й вирішують проблеми дисбалансу даних, відкриваючи шлях до комплексної анонімізації даних. Завдяки подальшим дослідженням і майбутнім розробкам цей підхід може забезпечити ще кращу анонімізацію, ніж найсучасніші методи.

Список використаних джерел:

1. A Review of Anonymization for Healthcare Data / I. E. Olatunji et al. Big Data. 2022. URL: https://doi.org/10.1089/big.2021.0169.
2. Data Anonymization for Pervasive Healthcare: A Systematic Mapping Study (Preprint) / N. Al Moubayed et al. JMIR Medical Informatics. 2021. URL: https://doi.org/10.2196/29871.