АНАЛІЗ ВРАЗЛИВОСТЕЙ БІОМЕТРИЧНИХ СИСТЕМ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ ДО АТАК ІЗ ЗАСТОСУВАННЯМ ГЕНЕРАТИВНО-ЗМАГАЛЬНИХ МЕРЕЖ

Олешко І.В., Луценко В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Біометричні системи автентифікації використовують унікальні фізіологічні або поведінкові характеристики людини такі, як відбитки пальців, обличчя чи голос для ідентифікації особи.

Системи біометричної автентифікації порівнюють біометричні дані користувача з даними, що зберігаються в базі шаблонів і, якщо зразки збігаються, автентифікація вважається успішною і доступ надається [1].

Прогрес у сфері штучного інтелекту створює принципово нові загрози для біометричних систем автентифікації.

Генеративні змагальні мережі синтезують біометричні зразки даних, здатні обходити захисні механізми [2].

Генеративно-змагальні мережі є архітектурою глибокого навчання, яка включає дві нейромережі.

Генеративна мережа створює нові зразки, схожі на реальні дані. Дискримінаторна мережа вчиться відрізняти справжні дані від синтезованих. Під час спільного навчання дискримінатор забезпечує генеративну мережу зворотним зв'язком, що допомагає удосконалювати якість створених зразків [3].

Одним з найпоширеніших методів біометричної автентифікації наразі є автентифікація за відбитком пальця. Штучне відтворення відбитків пальців має на меті відтворити розташування та розподіл дрібних деталей оригінального відбитку.

Сучасні схеми штучного відтворення складаються з двох етапів: спочатку реконструюється поле орієнтації на основі дрібних деталей, а потім відтворюється папілярний візерунок за допомогою реконструйованого поля орієнтації [3].

$$o(z) = \left[o_\infty + \frac{1}{2} \times \left(\sum_{i=1}^{\mathrm{K}} \arg(z - z_{ci}) - \sum_{j=1}^{\mathrm{L}} \arg(z - z_{dj}) \right) \right] mod\ \pi \quad (1)$$

Поле орієнтації відтворюється з використанням моделі нуль-полюс. У цьому підході кожне ядро у відбитку пальця розглядається як нуль, а кожна дельта як полюс.

У наведеній формулі (1) z_{ci} та z_{dj} є відповідно і-та ядра та j-та дельти відбитка пальця, а o_∞ є константним корекційним членом. У точці z вплив ядра z_{ci} дорівнює $\frac{1}{2} \times \arg(z - z_{ci})$, а вплив дельти z_{dj} дорівнює $\frac{1}{2} \times \arg(z - z_{dj})$ [4].

Генеративно-змагальна мережа для штучного відтворення відбитків пальців включає три основні компоненти: генератор, що створює синтетичні

зображення, кодувальник, який реконструює відбитки на основі карт дрібних деталей для забезпечення точної структури, та редактор атрибутів, що модифікує візуальні характеристики.

Для оцінки ефективності запропонованого підходу було проведено штучне відтворення відбитків пальців з бази даних NIST SD4.

Для імітування автоматичного розпізнавання відбитків пальців у системах, використовувалось відкрите програмне забезпечення Bozorth3 [5].

Система біометричної автентифікації помилково прийняла як істинні 97 % зразків, створених генеративно-змагальною мережею.

Метою доповіді є аналіз вразливостей сучасних біометричних систем автентифікації за відбитками пальців до атак, які використовують методи та технології штучного інтелекту.

Розглянуто методи створення синтетичних зразків, що можуть імітувати реальні біометричні дані та проходити автентифікацію в системах захисту.

В доповіді наводяться результати вимірювань ефективності атак на біометричні системи автентифікації за відбитками пальців з використанням генеративних моделей штучного інтелекту.

Наведені дані показують, що системи автентифікації за відбитками пальців виявили вразливість до синтетичних шаблонів, створених за допомогою генеративно-змагальних мереж.

Список літератури

1. Shoroog Albalawi, Lama Alshahrani, Nouf Albalawi,Reem Kilabi, and A'aeshah Alhakamy. A comprehensive overview on biometric authentication systems using artificial intelligence techniques. International Journal of Advanced Computer Science and Applications, 13(4):1–11, 2022. DOI: http://dx.doi.org/10.14569/IJACSA.2022.0130491

2. Bontrager, P.; Roy, A.; Togelius, J.; Memon, N.D.; Ross, A. DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9. DOI: http://dx.doi.org/10.1109/BTAS.2018.8698539

3. Bouzaglo, Rafael, and Yosi Keller. Synthesis and reconstruction of fingerprints using generative adversarial networks. arXiv preprint arXiv:2201.06164, 2022. DOI: https://doi.org/10.48550/arXiv.2201.06164

4. Fan, L.L.; Wang, S.G.; Wang, H.F.; Guo, T.D. Singular Points Detection Based on Zero-Pole Model in Fingerprint Images. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, no. 6, pp. 929-940, June 2008 . DOI: https://doi.org/10.1109/TPAMI.2008.31

5. NIST Biometric Image Software (NBIS). – 2010. – Режим доступу до ресурсу: https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis