УДК 004.93

А. В. Шпикуляк

СКЛАДНІСТЬ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Вінницький національний технічний університет

Анотація

Дана робота розглядає різні аспекти використання технологій розпізнавання обличчя в сучасному світі. Обговорюються питання приватності та зберігання даних, захисту від зловживань, автентифікації та можливих помилок. Обговорюється важливість відповідального використання та прозорості у впровадженні цих технологій.

Ключові слова: розпізнавання обличчя, приватність, безпека, захист даних, відповідальне використання, комп'ютерний зір.

Abstract

This research considers various aspects of the use of facial recognition technologies in the modern world. Issues of privacy and data storage, protection against abuse, authentication and possible errors are discussed. The importance of responsible use and transparency in the implementation of these technologies is discussed.

Keywords: facial recognition, privacy, security, data protection, responsible use, computer vision.

Вступ

Комп'ютерний зір — це галузь штучного інтелекту та обробки зображень, яка зосереджена на тому, як комп'ютери можуть розуміти, інтерпретувати та взаємодіяти із зоровою інформацією, схожою на те, як це роблять люди. Ця область включає в себе розпізнавання обличчя, визначення об'єктів, відслідковування рухів, розпізнавання образів та інші завдання, пов'язані з обробкою візуальної інформації.

Результати дослідження

Система розпізнавання облич – це технологія, здатна зіставляти людське обличчя з цифровим зображенням або відеокадром з базою даних осіб, зазвичай використовується для автентифікації користувачів за допомогою служб перевірки особистості, працює шляхом точного ви-значення і вимірювання рис обличчя по даному зображенню.Розробка подібних систем почалася в 1960-х роках, почавшись як форма комп'ютерного додат-ка. З моменту свого створення системи розпізнавання осіб останнім часом стали ширше використо-вуватися на смартфонах і в інших технологіях, таких як Робототехніка. Оскільки комп'ютеризоване розпізнавання обличчя включає в себе вимірювання фізіологічних характеристик людини, системи розпізнавання обличчя класифікуються як біометричні.[1,с.7].

В сучасному світі забезпечення високого рівня приватності є першочерговим завданням для систем розпізнавання обличчя. Щоб гарантувати конфіденційність біометричних даних, важливо використовувати сучасні методи шифрування на всіх етапах обробки і зберігання. Введення алгоритмів шифрування з високим ступенем захисту та безпечних протоколів зберігання є ключовим для забезпечення, що чутливі дані залишаються недоступними для несанкціонованих осіб чи систем.

Автентифікація в системах розпізнавання обличчя є ключовою функцією для підтвердження особистості користувача. Проте, існують можливі проблеми та помилки, які можуть виникнути при цьому процесі. Одна з основних проблем полягає у точності розпізнавання. Системи можуть допускати помилки при ідентифікації особи через різні фактори, такі як зміна взаємного розташування об'єктів на зображенні, освітлення, зміни в зовнішності чи якості зображення. Ці помилки можуть призвести до невірної ідентифікації особи, що може мати серйозні наслідки в контексті безпеки та автентифікації. Крім того, можлива проблема спроб обману системи, так званого "обхідного шляху". Це може включати в себе використання фальшивих зображень або об'єктів для спроб обійти процес автентифікації. Удосконалення точності ідентифікації та зменшення помилок вимагає поєднання передових алгоритмів машинного навчання та глибокого аналізу зображень, а також постійного оновлення та покращення апаратно-програмних засобів систем розпізнавання обличчя.

Також причинами несанкціанованого доступу третіх осіб до конфіденційної інформації часто стає робота інсайдерів і хакерів. Тому проблеми ідентифікації та автентифікації особистості мають велике значення. У багатьох комп'ютерних системах перевірка особи користувача все ще здійснюється за

допомогою введення логіна і пароля, але набирають популярності і методи біометричної автентифікації, які, потенційно більш надійні. [2,с.85]

Механізми захисту від зловживань включають у себе ретельну авторизацію доступу та контроль за використанням біометричних даних. Розробники повинні вдосконалювати алгоритми захисту, а також впроваджувати моніторингові системи для вчасного виявлення та реагування на будь-які спроби несанкціонованого доступу чи використання. Крім того, стандарти безпеки повинні бути постійно оновлюваними для врахування нових загроз та вразливостей.

Відповідальність розробників систем розпізнавання обличчя включає у себе не лише технічну, але й етичну складову. Вони повинні приділяти увагу розробці та впровадженню адекватних політик приватності, які визначають, як дані будуть використовуватися та зберігатися. Прозорість відносно цих процесів є ключовою для підтримання довіри. Розробники повинні надавати користувачам доступ до інформації про те, як їхні біометричні дані використовуються, і забезпечувати можливість відмовитися від використання чи видалити свої дані з системи.

Висновки

Розпізнавання обличчя, як важлива складова біометричних технологій, має значний потенціал у різних аспектах, від безпеки до зручності користувачів. Однак питання, пов'язані з приватністю, захистом від зловживань та автентифікацією, стають важливими факторами, які потрібно враховувати та вдосконалювати для успішного впровадження цих технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ВАКАЛЮК, Т., ІЛЮЩЕНКО, С., ЄФРЕМОВ, Ю., ВЛАСЕНКО, О., & ЛИСОГОР, Д. (2022). ТЕОРЕТИЧНІ АСПЕКТИ РОЗРОБКИ СИСТЕМИ РОЗПІЗНАВАННЯ ЛЮДСЬКОГО ОБЛИЧЧЯ. Інформаційні технології та суспільство, (1 (3), 6-15. https://doi.org/10.32689/maup.it.2022.1.1
2. Ляшенко Г.Є., Даниленко О.І. Дослідження методів розпізнавання облич // Міжнародна науково-практична конференція High-Technologies in infocommunications 23-25 травня 2019 р., Харків – Кам'янець-Подільський, Украї-на. https://openarchive.nure.ua/bitstreams/59672ce4-6381-4009-a26f-a6a3ae2738b5/download

Шпикуляк Андрій Віталійович – студент групи 2СП-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: andrii.sk2003@gmail.com

Shpykuliak Andrii Vitaliiovych - student of group 2SP-21b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: andrii.sk2003@gmail.com