УДК 004.8

К. В. Івченко

Когнітивні обчислення та безпека населення

Вінницький національний технічний університет

Анотація

Стаття розповідає про розвиток технологій машинного навчання, когнітивних обчислень, інтелектуального аналізу даних, а також ризики та вигоду для безпеки суспільства, що може завдати використання цих технологій.

Ключові слова: машинне навчання, когнітивне обчислення, інтелектуальний аналіз даних, інформаційна безпека, штучний інтелект, теорія розпізнавання образів.

Abstract

The article tells about the development of technologies of machine learning, cognitive computing, data mining, and public safety risks that may be caused by these technologies and benefits of using them.

Keywords: machine learning, cognitive computing, data mining, information security, artificial intelligence, pattern recognition.

Сучасні інформаційні технології розвиваються з незбагненною швидкістю. Прогрес спостерігається у всіх сферах, починаючи від того, чим ми користуємося у повсякденному житті, закінчуючи космічними технологіями. Щоразу з'являються якісь нові розробки, що досить швидко знаходять застосування і впроваджуються в наше життя. Останніми такими сучасними трендами стали машинне навчання, штучний інтелект, віртуальна та доповнена реальність. Як правило, всі ці технології в певній мірі пов'язані між собою, і заглибившись в одну, можна поверхнево розглянути інші.

Розвиток інформаційних технологій має на меті створити засоби, що будуть полегшувати життя: удосконалювати виробництво, урізноманітнювати дозвілля, розвивати медицину, тощо. Усі проблеми розділяються на певні задачі, кожну з яких беруться вирішувати науковці за допомогою різноманітних засобів.

Щоб вирішити задачу за допомогою комп'ютера, необхідно використати певний алгоритм – набір інструкцій, що виконуються та обробляють вхідні дані для отримання вихідних. Є задачі, для вирішення яких алгоритму немає. Це задачі, в яких програміст не може описати ланцюжок дій та умов, при яких отримуються правильні вихідні дані, за умови будь-яких вхідних. Наведемо простий приклад з фільтруванням спаму в електронній скриньці. Листи, що повинні потрапити під категорію спаму, мають різний характер. Крім того, це залежить від власних уподобань особи – власника поштової адреси. Щоб машина - комп'ютер – могла відрізняти корисну кореспонденцію від сміття, її треба навчити. Найпростіший спосіб – це дати на аналіз велику кількість листів, відібраних користувачами як спам, і позначити їх. Таким чином машина буде знаходити певні закономірності та правила, виробляючи алгоритм самостійно [1]. Таким чином працює багато прикладного програмного забезпечення, що не має чіткого визначеного алгоритму, але має певні дані-приклад. Отже, машинне навчання (Machine Learning) – це підрозділ комп'ютерних наук, що забезпечує комп'ютери можливістю самостійно вчитися і виконувати певні дії без чітко вказаних програм. Навчання відбувається за допомогою нейронної мережі, генетичних алгоритмів.

Машинне навчання настільки проникло в наше повсякденне життя що люди навіть і не підозрюють того, що користуються ним десятки разів в день. Багато дослідників впевнені, що машинне навчання - це найкращий шлях до створення штучного інтелекту людського рівня.

Щоб досягти рівня людського мислення, комп'ютер повинен навчитися думати як людина. Обчислення, що імітують свідому розумову діяльність людини, таку як мислення, розуміння, навчання та запам'ятовування, називають когнітивними обчисленнями (Cognitive Computing). Когнітивні обчислення та когнітивні системи прискорюють, покращують та масштабують людський досвід шляхом навчання та побудови знань, розуміння природної мови та взаємодії з людиною більш природно, ніж традиційні програмовані системи. Згодом, когнітивні системи будуть імітувати більше

того, як насправді працює мозок, і допомагатимуть вирішувати найскладніші проблеми в світі, проникаючи в складність великих даних (Big Data).

Основними задачами машинного навчання є: розпізнавання, сортування, знаходження регресії. Кожна з цих задач знаходить своє застосування у різних сферах.

Застосування методів машинного навчання на великих базах даних називається інтелектуальним аналізом даних (Data Mining – з англ. «видобуток даних»). Така назва може пояснюватися аналогією з видобуванням дорогоцінних металів на шахті, коли викопується великий обсяг землі і сировини, а при обробці призводить до невеликої кількості дорогоцінного матеріалу. Аналогічним чином, в інтелектуальному аналізі даних великий обсяг даних обробляють, щоб побудувати просту модель з використанням цінних даних, які, наприклад, мають високу точність прогнозування. На практиці аналіз даних використовується у різних галузях. Наприклад, в сфері фінансів банки аналізують свої минулі дані для побудови моделі для використання кредитних заявок, виявлення шахрайства і на фондовому ринку. В обробній промисловості, моделі використовуються для оптимізації, управління та усунення неполадок. У медицині, машинне навчання використовується для медичної діагностики. У науці великі обсяги даних в галузі фізики, астрономії та біології можуть бути проаналізовані досить швидко лише за допомогою комп'ютерів. Світова павутина величезна, і вона стає дедалі більшою, а пошук відповідної інформації не може бути здійснений вручну.

Задача розпізнавання, в свою чергу, має також певний поділ: розпізнавання зображень, звуку, символів тощо. Машинне навчання допомагає нам знайти рішення багатьох проблем в баченні, розпізнаванні мови і робототехніці. Приведемо приклад з розпізнаванням облич: це завдання, яке ми робимо без особливих зусиль, адже кожен день ми розпізнаємо членів сім'ї та друзів, дивлячись на їхні обличчя або фото, незважаючи на відмінності в позі, освітленні, зачісці, одязі тощо. Але ми робимо це несвідомо і не в змозі пояснити, як ми це робимо. Неможливо написати алгоритм і програму для цього, тому що людина не може пояснити свій досвід і перевести його у цифри і чітку логіку. У той же час, ми знаємо, що зображення особи не просто випадковий набір пікселів: особа має структуру. Обличчя є симетричним. Є очі, ніс, рот, розташовані в певних місцях на обличчі. Обличчя кожної людини являє собою шаблон, що складається з певної комбінації. Аналізуючи такі зразки зображень облич людини, програма навчання фіксує шаблон, специфічний для цього конкретного обличчя, а потім розпізнає, шляхом перевірки цієї моделі в даному зображенні. Це один із прикладів теорії розпізнавання образів (Pattern Recognition) [1]. Розпізнавання образів є галуззю машинного навчання, яка зосереджується на розпізнавання шаблонів і закономірностей в даних, хоча в деяких випадках вважаються майже синонімом машинного навчання [2]. Системи розпізнавання образів у багатьох випадках навчені з мічених даних «навчання» (Supervised Learning – «навчання з учителем»), але коли немає мічених даних, то використовуються інші алгоритми, щоб виявити невідомі раніше закономірності (Unsupervised Learning – «навчання без учителя»).

Розглянемо ж механізм розпізнавання зображень, а саме облич. Один з видів розпізнавання облич - система розпізнавання облич - програмне забезпечення, що здатне ідентифікувати або верифікувати людину і відділити від цифрового зображення, або відеокадру із джерела відеосигналу. Один із способів зробити це - шляхом порівняння вибраних рис обличчя з зображення і бази даних особи. Вона зазвичай використовується в системах безпеки і може бути порівняний з іншими засобами біометрії, такими як відбитки пальців або райдужної оболонки ока. Останнім часом така система також стала популярною в якості комерційної ідентифікації та інструменту маркетингу. Для такого розпізнавання не потрібне використання машинного навчання, а достатньо лише набору даних для порівняння і актуальної вхідної інформації. Щоб розпізнати обличчя, або виділити його серед інших об’єктів на фото чи відео, потрібно використовувати вже засоби машинного навчання та теорії розпізнавання образів.

А наскільки безпечним є використання такої системи? Кожен користувач соціальної мережі Facebook, якщо завантажував фото з друзями, міг побачити, що система автоматично розпізнає обличчя людей, зображених на фото з дуже високою точністю. Іноді виходить плутанина, але при цьому люди дійсно повинні бути схожі між собою за певними ознаками, на які звертає увагу комп’ютер. При цьому обличчя, які система не знайшла в свої базі, пропонується «підписати» вручну самому користувачеві. Не задумуючись, користувач сам надає таким чином додаткові дані для навчання системи. Чим більше даних у системі, тим потужнішою і точнішою вона стає.

Але розпізнавання облич використовується не лише у соціальних мережах і має на меті не посягання на особисте життя, а навпаки – захист населення. Найбільше досліджень в галузі аналізу

мультимедіа та створення систем захисту населення проводить компанія IBM. На рисунку 1 можна побачити приклад розпізнавання об’єктів на вулиці міста на знімку, зробленому вуличною камерою. При цьому люди, автомобілі та інші об’єкти розпізнаються окремо, як наведено для прикладу на рисунку 2. Тут зображено розпізнавання перехожих (жовтий чотирикутник), облич (фіолетовий чотирикутник), автомобілів (червоний чотирикутник). Уся ця інформація збирається та оброблюється. Всі зафіксовані об’єкти заносяться до бази даних, при чому кожному з них присвоюється певний індекс та ярлик.

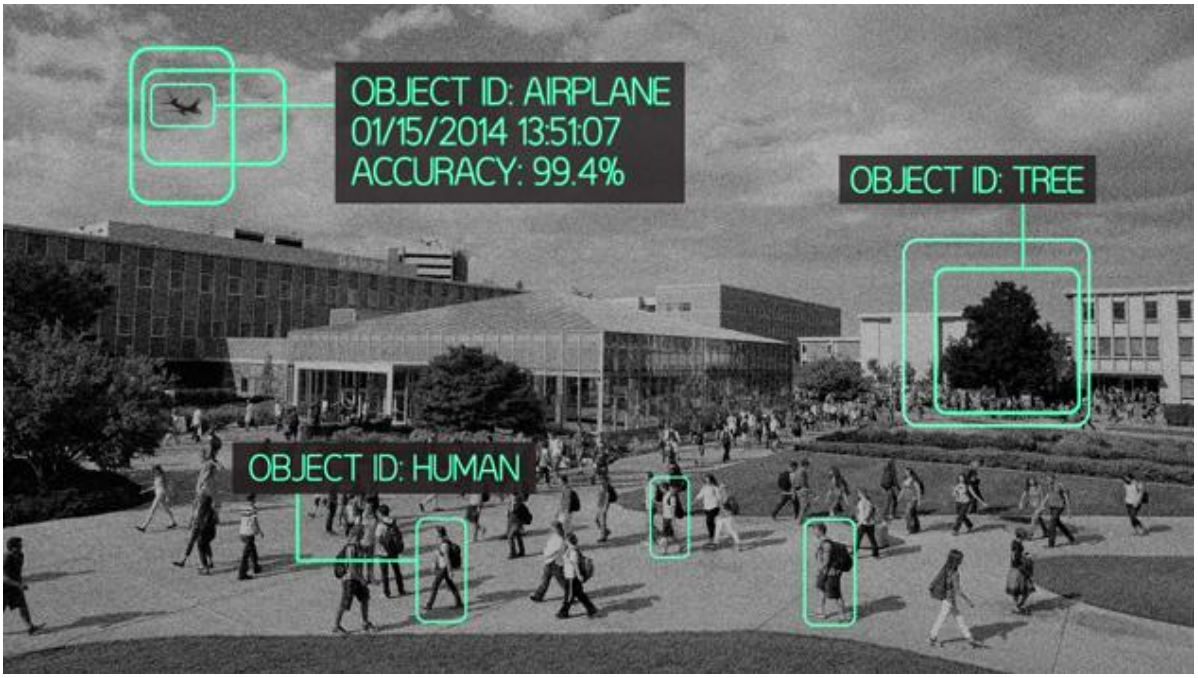

Рисунок 1 – Розпізнавання об’єктів з камери спостереження на вулиці міста.

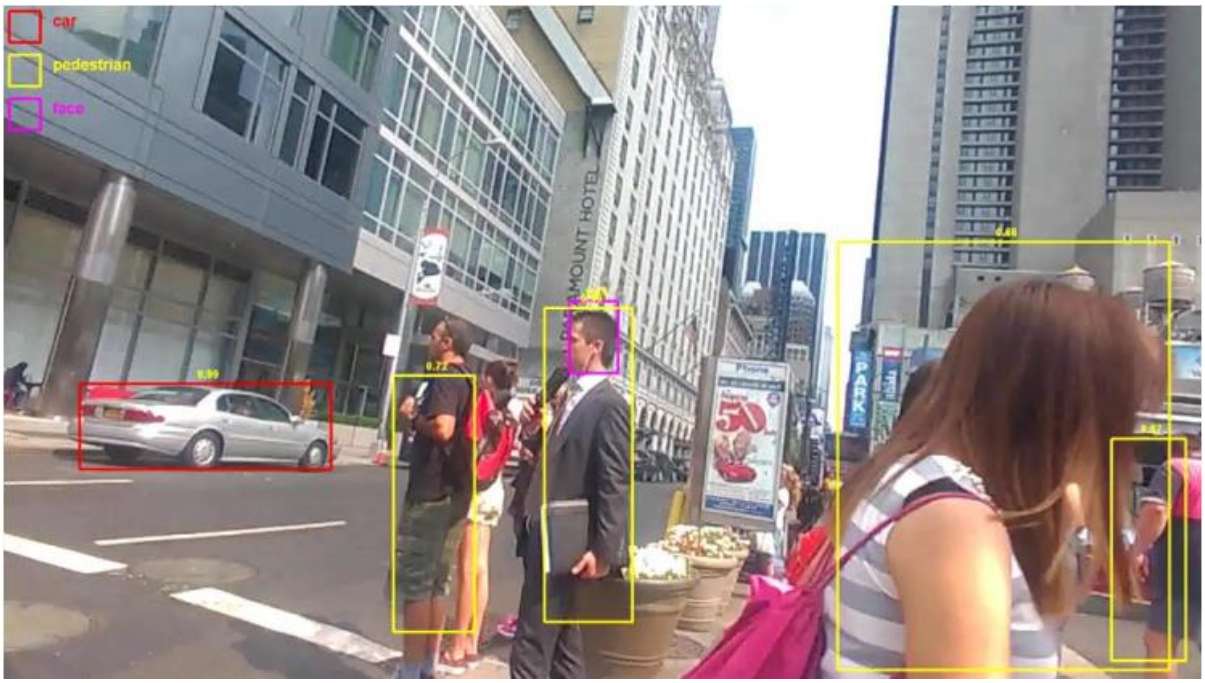

Рисунок 2 – Розпізнавання об’єктів з камери на Тайм Сквер у Нью-Йорку.

Всі камери логічно об’єднуються в системи спостереження. Сьогодні у світі використовується близько 845 мільйонів камер спостереження. 2,4 мільйони нових камер встановлюються щорічно.

Близько 10 мільярдів годин відео записується щотижня. Лише 3% цих камер і сенсорів обладнані певними інтелектуальними системами. При цьому очевидно, що ніхто не переглядає всі відзняті відео, а, відповідно, немає кому слідкувати за безпекою людей [3]. Зазвичай такі записи використовують у тому випадку, коли вже трапився певний інцидент, тоді записи допомагають відтворити хід подій та дають змогу відстежити пересування злочинців, винуватця дорожньо-транспортної пригоди тощо.

Щоб обробити таку величезну кількість інформації за короткий період, недостатньо лише людських ресурсів. Тому наразі стоїть завдання розвитку когнітивних обчислень, що діятимуть як людина, або навіть краще, при цьому зі швидкістю, яку ми не можемо собі уявити. Застосування таких технологій дозволить скоротити пошуки злочинця від місяців до годин, або навіть хвилин, відстежити пересування автомобіля, при цьому чим більше камер буде працювати у системі, тим краще. Інше застосування – попередження нещасних випадків: наїздів, аварій, пожеж, зіткнень. Комп'ютер зможе розпізнати і характеризувати натовп та окремих осіб у ньому, що може бути корисним під час мітингів, демонстрацій, неконтрольованих скупчень людей. За допомогою цієї системи можна знайти серед перехожих озброєних людей, при цьому швидко та вчасно передати інформацію до найближчого відділення чи посту поліції.

Використання ярликів та індексів допоможе знайти і відслідкувати осіб за певними характеристиками. Ярлики можуть бути різноманітними: стать, колір шкіри, раса, вік, одяг, зачіска, аксесуари, тощо, а також поєднання декількох з них. Наприклад, стався злочин, злочинець не потрапив у камери, але свідки описали його зовнішність як білий лисий чоловік у синьому верхньому одязі. Оператор заносить дані до системи пошуку: «світлошкірий», «лисий», «синій верх», а система шукає особу за даними мітками на всіх камерах. Результат буде приблизно такий, як на рисунку 3.

Рисунок 3 – Результати пошуку за мітками «світлошкірий» + «лисий» + «синій верх».

Таким чином можна значно підвищити рівень захисту населення, передбачити та запобігти нещасним випадкам та аваріям, розкрити злочин. Застосування таких систем повинно стати новим слово у технічній і суспільній революції.

Отже, розвиток машинного навчання, когнітивних обчислень, теорії розпізнавання образів та інтелектуального аналізу даних є актуальною проблемо сучасності. А застосування цих технологій

може змінити представлення про майбутнє нашого суспільства, поліпшуючи безпеку населення до якісно нового рівня.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Alpaydın Ethem. M. Introduction to Machine Learning/ Ethem Alpaydın.– London:. The MIT Press, 2010. - 579 p. – ISBN 978-0-262-01243-0.
2. Bishop Christopher. M. Pattern Recognition and Machine Learning / Christopher M. Bishop.– New York:. Springer-Verlag, 2006. - 738 p. – ISBN 978-0-387-31073-2.
3. Russo St. IBM Multi-Media Analytics & Cognitive Computing for Safer Cities / Stephen Russo // Lviv IT Arena: міжнародна конф. з інф. технологій, 30 вер. — 2 жовт. 2016 р.: презентації, доповіді.

Івченко Ксенія Володимирівна – студентка групи 1ПЗ-16м Факультету інформаційних технологій і комп'ютерної інженерії Вінницького національного технічного університету, м. Вінниця, e-mail: ksenon.madpainter@gmail.com.

Ivchenko Kseniia V. – student of the group 1ПЗ-16м, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ksenon.madpainter@gmail.com.