COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.165

УДК 004.75; 004.8

ЗАСТОСУВАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ В АНАЛІЗІ ДАНИХ МОБІЛЬНИХ ПРИСТРОЇВ ДЛЯ ВИЯВЛЕННЯ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ОСІБ

Т. О. Фединишин, О. О. Михайлова

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: taras.o.fedynyshyn@lpnu.ua, olha.o.mykhailova@lpnu.ua

У статті розглянуто методи ідентифікації потенційно небезпечних осіб (ПНО, також об'єкт оперативної зацікавленості або Person-Of-Interest) за даними мобільних пристроїв. Проблема є актуальною і не розв'язаною в діяльності правоохоронних, розвідувальних та інших органів, які провадять оперативно-розшукову діяльність, через велику кількість даних, що зберігаються на мобільних пристроях. З урахуванням складності й обсягу мобільних даних традиційні методи аналізу часто недостатньо ефективні. У статті пропонується використання штучного інтелекту (ШІ), зокрема машинне навчання та обробку природної мови, для покращення ефективності та швидкості аналізу даних мобільних пристроїв. Такий підхід спрямований на подолання обмежень ручного аналізу даних та покращення процесу ідентифікації ПНО в додержанні принципів криміналістичної достовірності.

Основною метою роботи є дослідження та демонстрація ефективності застосування штучного інтелекту у процесі ідентифікації ПНО з використанням даних мобільних пристроїв. Дослідження пропонує підходи на основі штучного інтелекту, зокрема машинного навчання та обробки природної мови, які можуть значно підвищити ефективність, точність та глибину аналізу у мобільних форензичних дослідженнях, таким способом розв'язуючи проблеми обробки великих обсягів даних та складності сучасних цифрових доказів. У дослідженні, зокрема, продемонстровано, як машинне навчання може бути використане для пошуку ПНО в даних месенджера WhatsApp.

Результат експерименту показує, що використання штучного інтелекту для розпізнавання облич може призводити до виникнення помилкових позитивних результатів, що означає, що людей не можна повністю замінити на поточному етапі еволюції штучного інтелекту. Водночас застосування глибокого навчання показало 88-відсоткову ефективність у розпізнаванні облич. Отримані результати підкреслюють трансформаційний потенціал штучного інтелекту в мобільній форензиці, виокремлюючи його здатність підвищувати точність та ефективність аналізу даних мобільних пристроїв.

Ключові слова: штучний інтелект, мобільний форензик, криміналістичний аналіз даних, ios, whatsapp.

Вступ

У динамічному ландшафті цифрової форензики експоненційний ріст використання мобільних пристроїв спричинив як непередбачувані можливості, так і виклики для правоохоронних органів, експертів з кібербезпеки та форензичних розслідувачів. Зі зростанням обсягу мобільних даних стає

нагальною потреба в інноваційних методах, які допоможуть ефективно аналізувати та інтерпретувати це величезне сховище інформації. Поява штучного інтелекту (ШІ) як потужного інструменту в різних галузях викликала зміни у сфері цифрової форензики, відкриваючи нові можливості для підвищення ефективності аналізу даних.

Об'єктом дослідження цієї праці є виявлення потенційно небезпечних осіб (ПНО) у форензичних даних мобільного пристрою. Предметом дослідження є аналіз застосування методів штучного інтелекту для розпізнавання облич у даних месенджера WhatsApp. Завдання цієї роботи – дослідити ефективність розпізнавання облич розшукуваних осіб у даних месенджера WhatsApp резервної копії мобільного пристрою на основі операційної системи iOS.

У цій статті досліджено методи пошуку потенційно небезпечних осіб у даних із мобільних пристроїв та описано трансформаційний потенціал підходів, що базуються на застосуванні штучного інтелекту в цьому контексті. Виявлення та відстеження ПНО відіграє важливу роль у вирішенні кримінальних справ, заходах протидії тероризму та забезпеченні громадської безпеки. Використовуючи передові техніки штучного інтелекту, такі як машинне навчання та глибоке навчання, це дослідження має на меті використати обчислювальні можливості цих технологій для знаходження значущих висновків з даних мобільних пристроїв, таким способом оптимізуючи процес розслідування.

В статті запропоновано потенційні напрями застосування ШІ для покращення ефективності аналізу даних мобільних пристроїв. Наведено результати застосування глибокого навчання для розпізнавання облич із даних додатку WhatsApp.

1. Аналіз останніх досліджень та публікацій

Сучасні методології та інструменти, що використовуються у форензиці мобільних пристроїв, значно змінили стратегії, які використовують дослідники та правоохоронні органи. Мобільні пристрої часто стають основним елементом у розслідуваннях, а ці інноваційні підходи дають покращені можливості одночасно швидкого та ефективного аналізу великої кількості даних. Сучасні техніки також дають змогу долучати в аналіз ширший спектр інформації з мобільних пристроїв. Широке використання мобільних пристроїв як у сфері бізнесу, так і в особистих цілях [7], призвело до накопичення величезної кількості даних, які є більш доступними, ніж будь-яке інше джерело даних. Наведений факт у поєднанні з високою частотою використання та впевненості користувачів у захищеності і недоступності даних на їх пристроях робить мобільні пристрої вкрай цінними для аналізу.

Після отримання так званих сирих даних з мобільного пристрою можуть використовуватися різноманітні інструменти для їх аналізу. У простих випадках з обмеженим набором пристроїв та відомими проблемами може бути достатньо ручного аналізу за допомогою електронних таблиць або традиційних платформ перегляду документів. Однак у певних ситуаціях потрібний комплексний підхід до аналізу, який використовує складніша техніка аналізу даних. Цей підхід містить видобуток конкретних типів даних та інтеграцію даних з кількох додатків чи мобільних пристроїв в єдину базу даних, що сприяє узагальненому аналізу.

Наступні етапи, а саме аналіз та звітність, зазвичай забирають більше часу і можуть потребувати кількох ітерацій, а також можливого додаткового збору даних чи коригування аналізу. Конкретні типи аналізу можуть варіюватися, але загальною метою є застосування технік, що ґрунтуються на встановлених фактах, для прискорення процесу аналізу та зменшення часу, витраченого на просіювання неактуальних даних. Фаза аналізу передбачає кілька ітерацій, кожна з яких адаптує або вдосконалює аналіз на основі отриманих висновків попередніх аналізів.

Аналіз даних мобільних пристроїв містить одночасне дослідження різних типів даних із різних додатків та служб операційної системи. Використання передових інструментів, таких як штучний інтелект та машинне навчання, дає можливість дослідникам проводити цей аналіз швидше та більш комплексно, ніж традиційні інструменти для перегляду документів.

Використання штучного інтелекту в аналізі форензичних даних та діяльності правоохоронних та інших органів стає все більш поширеним в епоху четвертої промислової революції, в яку входить світ.

Одним з таких піонерських прикладів є розпізнавання облич у системах спостереження. Танг та інші [8] (2004) пропонують перетворити фотографічне зображення на ескіз, що значно зменшує різницю між фото та ескізом і дає змогу ефективно виконувати відповідність між ними. Зафар та інші [9] (2019) – використовувати глибокі згорткові нейронні мережі та метод для підвищення ефективності систем розпізнавання облич за допомогою розв'язання проблеми помилкових позитивних результатів за допомогою використання невизначеності моделі для розпізнавання облич для стійких систем спостереження. Авайс та інші [10] (2019) пропонують використовувати ознаки гістограми орієнтованих градієнтів та класифікатор передання нейронної мережі для покращення продуктивності систем спостереження реального часу. Дослідники у [11, 12, 13] також подають різні методи та алгоритми, пов'язані з розпізнаванням облич у системах спостереження.

Хан та інші [1] (2018) пропонують метод для відстеження та розпізнавання татуювань на тілах людей на зображеннях з відеоспостереження для виявлення ПНО і їх пошуку у соціальних медіа.

Богер та Озер [5] (2023) подають теоретичну основу для використання пристроїв для виявлення ДНК для пошуку зниклих осіб, розшукуваних злочинців та ПНО в густонаселених районах через моніторинг стічних вод. Запропонована система містить комп'ютерний додаток для введення інформації про зниклих осіб, а отримані системою дані можуть бути використані для уточнення їх місця перебування для порятунку чи затримання.

Сахуліду в [4] (2023) досліджує тенденцію зростання використання автоматизації в правоохоронних органах. Акцент зроблено на інструментах та технологіях, які працюють на основі штучного інтелекту, використовуються для передбачення людської поведінки та полегшення прийняття рішень щодо того, кому треба присвятити більше уваги у правоохоронній діяльності.

Автори в [3] описують ділянки технологій, де штучний інтелект має значення в діяльності правоохоронних органів, зокрема обробку аудіо, обробку візуальних даних, оптимізацію ресурсів та обробку природної мови. Також наводять випадки використання правоохоронними органами, зокрема системи спостереження в Норвегії, блокування даних та визначення шкідливих матеріалів в Австралії, системи рекомендацій в Німеччині та скринінг, спостереження та інші заходи безпеки на масових заходах в Японії.

Автори в [2] досліджують вплив впровадження штучного інтелекту в правоохоронній діяльності на реалізацію фундаментальних прав громадян, порівнюючи очікування та цілі політики з фактичною практикою, фінансовими проєктами та оперативною реальністю в правоохоронних органах.

2. Постановка завдання

З огляду на нагальність проблеми виявлення потенційно небезпечних осіб, актуальним завданням є розробка та тестування ефективності системи виявлення осіб, у цьому випадку тих, які розшукуються правоохоронними органами, у форензичних даних месенджера WhatsApp. Система має обробляти дані резервної копії операційної системи iOS.

3. Напрями використання штучного інтелекту

Штучний інтелект (ШІ) – це імітація процесів людського мислення у комп'ютеризованій моделі. ШІ охоплює самонавчальні системи, які використовують техніки, такі як видобуток даних, розпізнавання шаблонів та обробка природної мови для реплікації когнітивних функцій людського мозку [14].

Опрацьовуючи великі обсяги інформації, маючи зачатки елементарного мислення та здатність спілкуватися із людьми природною мовою, системи ШІ відіграють важливу роль у

вдосконаленні процесу ухвалення рішень, подібно до того, як пошук покращує отримання інформації. Властиво, ШІ допомагає експертам у прийнятті більш обґрунтованих рішень. Ми визначаємо штучний інтелект за чотирма основними ознаками:

1. Розуміння – ШІ досягає глибокого розуміння у певній сфері, головно завдяки обробці даних у різноманітних формах, чи це структуровані або неструктуровані, текстові, чи дані із сенсорів. Це відбувається в конкретному контексті, водночас можуть швидко оброблятися великі обсяги даних.

2. Аргументація – ШІ мислить для досягнення заданих цілей, демонструючи здатність генерувати гіпотези за допомогою обґрунтованих аргументів та надавати пріоритетні рекомендації. Ці здібності допомагають у прийнятті рішень людьми.

3. Навчання – ШІ постійно навчається з досвіду, засвоюючи і накопичуючи дані та уявлення з кожної взаємодії. Його не програмують, а навчають експерти, які розвивають, масштабують та прискорюють свою експертизу, що призводить до постійного покращення цих систем з часом.

4. Взаємодія – ШІ працює на стику між людьми та складними системами та спрощує цю взаємодію.

Напрями ШІ, які можуть бути цінними в процесі виявлення ПНО:

1) комп'ютерний зір – область ШІ, яка надає комп'ютерам можливість видобувати цінну інформацію з цифрових фото, відеозаписів та інших візуальних даних. Він допомагає приймати рішення або надавати рекомендації на основі інтерпретованої візуальної інформації. ШІ дає можливість комп'ютерам мислити, комп'ютерний зір надає їм здатність бачити, спостерігати та розуміти візуальні дані [15];

2) обробка природної мови (NLP) – це технологія машинного навчання, яка дає комп'ютерам можливість інтерпретувати, маніпулювати та розуміти людську мову [16]. У сучасних організаціях широкомасштабні голосові та текстові дані генеруються за допомогою різноманітних комунікаційних каналів, таких як електронні листи, текстові повідомлення, стрічки соціальних мереж, відео, аудіо та інше. Програмне забезпечення NLP використовується для автоматичної обробки цих даних, аналізує наміри або настрій, що виражені в повідомленнях, та дає оперативні відповіді на людські запитання. Ця технологія інтегрує обчислювальну лінгвістику, моделі машинного навчання та глибокого навчання для обробки людської мови;

3) обробка аудіо – це технологія машинного навчання, яка працює на основі процесу, який називається вилученням ознак. Це передбачає перетворення сирого авдіосигналу у набір ознак або точок даних, які піддаються аналізу [17]. Першим кроком є розбиття сирого авдіо на менші сегменти, які зазвичай тривають кілька мілісекунд кожен;

4) експертні системи – це комп'ютерні системи, які емулюють прийняття рішень людиною-експертом. Ці системи призначені для розв'язання складних проблем аргументуванням на основі знань системи, переважно представлених у вигляді правил на кшталт "якщо-то", а не традиційного процедурного коду. Експертні системи є прикладами систем на основі знань [18]. Зазвичай експертна система складається з кількох компонентів, зокрема бази знань, модуля виведення, модуля пояснення аргументів, засобу накопичення знань та користувацького інтерфейсу [19].

4. Приклади використання ШІ для пошуку ПНО за даними мобільного пристрою

У цьому розділі описано категорії інформації, яку можна знайти в даних мобільного пристрою під час форензичного аналізу та яку можна використовувати для ідентифікації та пошуку ПНО. Основна ідея полягає в тому, що використання штучного інтелекту в аналізі даних мобільних пристроїв забезпечує додаткові знання про користувача мобільного пристрою. І ці знання можна отримати автоматично або напівавтоматично.

1. Виявлення документів, що посвідчують особу [20]. Особа може зберігати фотографії документів, що посвідчують особу, у галереї свого мобільного телефону чи пересилати фото таких документів у месенджерах. У деяких випадках ці фотографії документів можуть бути використані для ідентифікації особи в процесі розслідування. Також можливе зберігання особою фотографій документів інших осіб. Правоохоронні органи можуть розглядати цю дію як потенційне порушення

прав на конфіденційність, незаконне володіння особистою інформацією або навіть крадіжку особистості, залежно від обставин та наміру.

2. Розпізнавання людських облич. Зображення облич можна знайти на фотографіях та відео в галереї пристрою, на аватарах у месенджерах, фотографії з обличчями можуть бути відправлені через месенджери або електронну пошту. Зображення облич можуть порівнюватися з різними базами даних, наприклад, зі списками розшукових оголошень поліції/спецслужб, списками зниклих осіб, списками осіб під санкціями і т. ін. Те, що деяка особа із вище перелічених списків є на фотографії в галереї чи месенджерах пристрою [21], може означати, що пристрій потребує детальнішого дослідження щодо виявлення ПНО.

3. Розпізнавання номерних знаків транспортних засобів. Автоматизоване визначення номерних знаків використовується майже у всіх країнах для щоденного життя, наприклад, для правоохоронних органів, контролю на дорогах, доступу до обмежених зон, електронного збору плати за проїзд або для перевірки на парковках [22]. Визначення номерних знаків може дати додаткову цінну інформацію під час застосування в аналізі даних мобільної форензики. Його застосування може допомогти виявити викрадені транспортні засоби або транспортні засоби, що брали участь у якихось подіях, з якими правоохоронні органи можуть працювати.

4. Розпізнавання фінансової інформації. Виявлення фінансової інформації під час криміналістичного аналізу даних мобільного пристрою є важливим з кількох причин: така інформація є основною у розслідуванні фінансових злочинів, таких як шахрайство, відмивання грошей, розкрадання та інші нелегальні діяльності [23]. Операції та інформація про рахунки дають можливість здійснити аналіз потенційно незаконної фінансової діяльності. Фінансова інформація є цінним джерелом даних для правоохоронних органів [24]. Аналіз фінансових операцій може виявити зв'язки між особами, організаціями та злочинними мережами, допомагаючи збирати інформацію для широкомасштабних розслідувань.

5. Розпізнавання квитків. Авіа, залізничні чи автобусні квитки надають дані про подорожі особи. Ця інформація може бути використана для встановлення часових меж, відстеження руху та ідентифікації місць, пов'язаних з ПНО.

6. Виявлення іменованих сутностей. Виявлення іменованих сутностей – це процес ідентифікації інформації, як імена людей, назви організацій, місця, дати, числа тощо. Застосування методів виявлення іменованих сутностей у мобільній форензиці підвищує ефективність дослідників, автоматизуючи ідентифікацію та витягування критичної інформації з різних джерел даних на мобільних пристроях [25, 26].

7. Резюмування та пошук за документами. Мобільні пристрої часто містять велику кількість текстових даних, зокрема повідомлення, електронну пошту, документи та нотатки. Резюмування допомагає скоротити довгі документи, даючи можливість дослідникам ефективно сконцентруватися на найбільш актуальній інформації.

8. Розпізнавання голосу. Розпізнавання голосу допомагає ідентифікувати голоси на записі на основі їхніх унікальних голосових характеристик. Це може бути вирішальним у випадках, коли потрібно встановити походження голосового повідомлення чи розмови. Так само, як і з обличчями, голос особи може бути знайдений у відео чи голосових нотатках у галереї пристрою, в месенджерах або електронній пошті. Голос може бути порівняний з різними базами даних.

5. Кейс-стаді – застосування машинного навчання для пошуку ПНО із даних месенджера WhatsApp

У цьому розділі описано експеримент, проведений з використанням даних мобільної форензики – у цьому випадку дані додатку WhatsApp – та технології розпізнавання облич для виявлення фото осіб, які є у списку розшуку.

Під час підготовки до експерименту було зроблено такі кроки:

1. Написано скрипт, який завантажує із сайту розшуку Служби безпеки України імена та фото розшукуваних осіб [31]. Приклад фото зображено на рис. 1.

Рис. 1. Приклад фото осіб із розшуку Служби безпеки України

2. Проведено пошук додаткових фото осіб із попереднього кроку на сайті [32].

3. Фото із кроку 2 відправлено месенджером WhatsApp [33] із пристрою iPhone 13 mini, який використовує операційну систему iOS 17.3.1.

4. Зроблено резервну копію даних (“backup”) пристрою iPhone за допомогою програмного забезпечення iMazing [34], використовуючи опцію “Export raw files”. Структура файлів резервної копії додатку WhatsApp зображена на рис. 2.

Наступним етапом є застосування методів штучного інтелекту. Цей експеримент проводився за допомогою бібліотеки dlib [29], написаної мовою програмування C++, та обгортки для Python – пакету face_recognition [30]. Dlib – це сучасний набір інструментів мовою програмування C++, що реалізує алгоритми машинного навчання, а також містить додаткові засоби створення складного програмного забезпечення на C++, яке розв’язує реальні проблеми. Вона використовується як в промисловості, так і в академічній сфері, у широкому спектрі галузей, наприклад, у робототехніці, вбудованих пристроях, мобільних телефонах та великих обчислювальних середовищах високої продуктивності. Dlib є універсальною бібліотекою крос-платформенного програмного забезпечення, яка написана мовою програмування C++. Бібліотека реалізує численні алгоритми машинного навчання, зокрема метод опорних векторів (SVM), кластеризацію K-середніх, баєсівські мережі та інші.

Для виконання цього етапу експерименту було написано скрипт мовою програмування python:

1) кожне фото зі списку осіб із розшуку подається у простір 128-вимірного вектору, де зображення однієї й тієї ж людини перебуває близько одне до одного, а зображення різних людей віддалені одне від одного;

2) для кожного фото із даних додатку WhatsApp також генерується 128-вимірний вектор із чисел із рухомою крапкою;

3) для кожного фото із даних додатку WhatsApp розраховується евклідова відстань між його вектором та векторами всіх фото із бази рошуку;

4) для кожного фото із даних додатку WhatsApp розраховані відстані сортуються за зростанням;

5) результати зберігаються у файл.

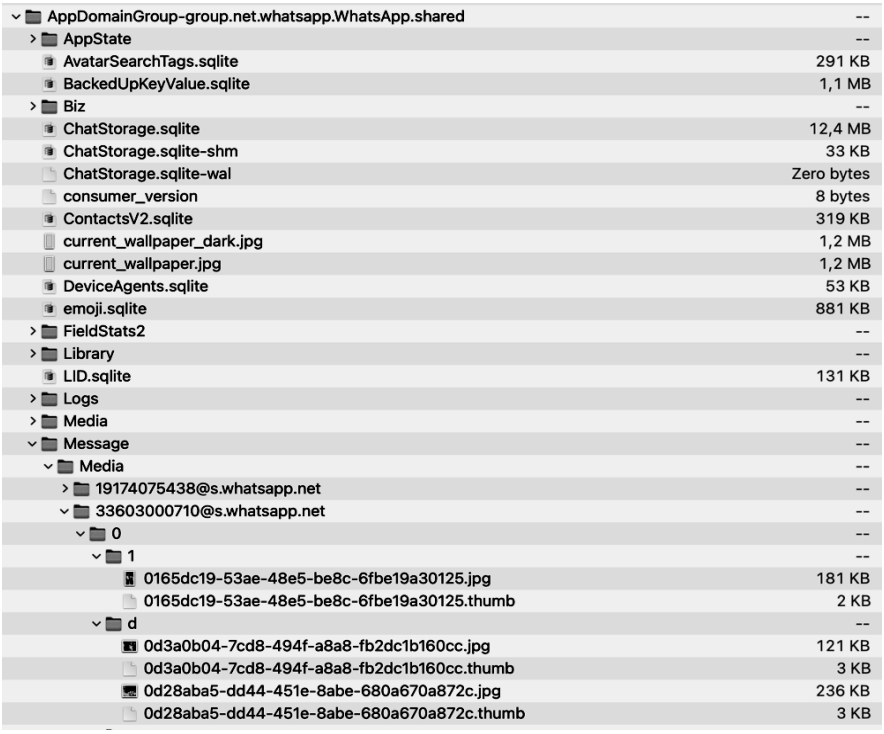

Рис. 2. Структура файлів додатку WhatsApp резервної копії операційної системи iOS

Далі відбувається ручна перевірка людиною, чи збігаються особи, вектори яких максимально близькі.

Внаслідок проведення експерименту було розпізнано 24 з 27 (88 %) осіб, чиї фотографії відправлено через WhatsApp. На рис. 3 та 4 показані обличчя, які успішно визнано.

Рис. 3. Приклад № 1 успішного розпізнавання облич

Рис. 4. Приклад № 2 успішного розпізнавання облич

На рис. 5 показано обличчя, які були визнані з помилкою.

Рис. 5. Приклад неуспішного розпізнавання облич

6. Результати дослідження

Запропонований у роботі метод імплементований мовою Python, а для розпізнавання облич було використано бібліотеку face_recognition, яка є Python обгорткою бібліотеки dlib. Тестування розробленого методу пошуку ПНО у форензичних даних мобільного пристрою, а саме додатку WhatsApp, показало 88-відсоткову ефективність – 24 із 27 осіб було розпізнано за фото.

Висновки

Розглянуто проблему аналізу форензичних даних мобільного пристрою в контексті пошуку ПНО. Запропоновано напрями застосування ШІ для аналізу даних мобільних пристроїв, а також подано приклад застосування. Показано, що використання методів машинного навчання, обробки природної мови та інші техніки ШІ можуть посилити можливості форензичних аналітиків у виявленні та видобуванні критично важливої інформації з обширних та складних наборів даних на мобільних пристроях.

Виявлені результати свідчать, що ШІ поки не може повністю замінити людину в криміналістичному аналізі даних, але може спростити роботу людини.

Список літератури

1. Han H., Li J., Jain A. K., Shan S. and Chen X. Tattoo Image Search at Scale: Joint Detection and Compact Representation Learning in: IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 41, No. 10, pp. 2333–2348, 1 Oct. 2019, doi: 10.1109/TPAMI.2019.2891584

2. Sanz-Urquijo B., Fosch-Villaronga E. & Lopez-Belloso M. The disconnect between the goals of trustworthy AI for law enforcement and the EU research agenda. AI Ethics 3, 1283–1294 (2023), https://doi.org/10.1007/s43681-022-00235-8

3. Towards responsible ai innovation second interpol-unicri report on artificial intelligence for law enforcement, 2020, Available at: https://www.interpol.int/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf (Accessed: 15 February 2024).

4. Sachoulidou A. Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence. Artif Intell Law (2023). https://doi.org/10.1007/s10506-023-09347-w

5. Boger Nathaniel, Ozer Murat. Monitoring sewer systems to detect the eDNA of missing persons and persons of interest, Forensic Science International, Vol. 349, 2023, 111744, ISSN 0379-0738, https://doi.org/10.1016/j.forsciint.2023.111744

6. Fedynyshyn T., Mykhaylova O., Opirskyy I., 2023. Method to detect suspicious individuals through mobile device data, doi: https://doi.org/10.18372/2225-5036.29.18075

7. Forensic Data Analysis of Mobile Devices: A Primer | Kroll. Available at: https://www.kroll.com/en/insights/publications/forensic-data-analysis-of-mobile-devices (Accessed: 15 February 2024).

8. Xiaoou Tang and Xiaogang Wang. Face sketch recognition, in: IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 50–57, Jan. 2004, https://doi.org/10.1109/TCSVT.2003.818353

9. Zafar U., Ghafoor M., Zia T. et al. Face recognition with Bayesian convolutional networks for robust surveillance systems. J Image Video Proc. 2019, 10 (2019). https://doi.org/10.1186/s13640-019-0406-y

10. Awais M. et al. Real-Time Surveillance Through Face Recognition Using HOG and Feedforward Neural Networks, in: IEEE Access, Vol. 7, pp. 121236–121244, 2019, https://doi.org/10.1109/ACCESS.2019.2937810

11. Melnyk R. A., Kvit R. I., Salo T. M. Face image profiles features extraction for recognition systems, 2021, doi: https://doi.org/10.36930/40310120

12. Jose E. G. M., Haridas M. T. P. and Supriya M. H. Face Recognition based Surveillance System Using FaceNet and MTCNN on Jetson TX2, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 608–613, https://doi.org/10.1109/ICACCS.2019.8728466

13. Chawla Dimple & Munesh Trivedi (Dr.) (2019). Face Recognition under Partial Occlusion for Security Surveillance Using Machine Learning.

14. IBM Design for AI, Fundamentals, 2022. Available at: https://www.ibm.com/design/ai/fundamentals/. (Accessed: 15 February 2024).

15. IBM, What is computer vision?, 2022. Available at: https://www.ibm.com/topics/computer-vision. (Accessed: 15 February 2024).

16. AWS What is Natural Language Processing (NLP)? 2024. Available at: https://aws.amazon.com/what-is/nlp/. (Accessed: 15 February 2024).

17. How Does Audio AI Work? (A guide for beginners), 2024. Available at: https://engineeryoursound.com/how-does-audio-ai-work-a-guide-for-beginners/. (Accessed: 15 February 2024).

18. Expert system, 2024. Available at: https://en.wikipedia.org/wiki/Expert_system. (Accessed: 15 February 2024).

19. Lea Andrew S. (2023). Digitizing Diagnosis: Medicine, Minds, and Machines in Twentieth-Century America. Johns Hopkins University Press. pp. 1–256. ISBN 978-1421446813

20. Adawadkar Amrin, Maria Khan, Kulkarni Nilima. Cyber-security and reinforcement learning – A brief survey, Engineering Applications of Artificial Intelligence, Vol. 114, 2022, 105116, ISSN 0952-1976, https://doi.org/10.1016/j.engappai.2022.105116

21. Alsayaydeh Jamil Abedalrahim Jamil, Irianto, Azwan Aziz, Xin Chang Kai, Hossain A. K. M. Zakir and Herawan Safarudin Gazali. Face Recognition System Design and Implementation using Neural Networks. International Journal of Advanced Computer Science and Applications (IJACSA), 13(6), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130663

22. Salimah U. et al. 2021 IOP Conf. Ser.: Mater. Sci. Eng. 1115 012023, https://doi.org/10.1088/1757-899X/1115/1/012023

23. Sukardi Sukardi. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. Unnes Law Journal. 8. 133–158. https://doi.org/10.15294/ulj.v8i1.53059.

24. Lagerwaard Pieter & Goede Marieke. (2023). In trust we share: The politics of financial intelligence sharing. Economy and Society. 52. 1–25. https://doi.org/10.1080/03085147.2023.2175451.

25. Rodrigues F. B., Giozza W. F., Albuquerque R. de Oliveira and Villalba L. J. García. Natural Language Processing Applied to Forensics Information Extraction With Transformers and Graph Visualization, in: IEEE Transactions on Computational Social Systems, https://doi.org/10.1109/TCSS.2022.3159677.

26. Studiawan H., Hasan M. F. and Pratomo B. A. Rule-based Entity Recognition for Forensic Timeline, 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2023, pp. 1–6, https://doi.org/10.1109/ICTAS56421.2023.10082742.

27. Gaby G. Dagher, Benjamin C. M. Fung. Subject-based semantic document clustering for digital forensic investigations, Data & Knowledge Engineering, Volume 86, 2013, P. 224–241, ISSN 0169-023X, https://doi.org/10.1016/j.datak.2013.03.005

28. Shevchuk Denys, Harasymchuk Oleh, Partyka Andrii, Korshun Nataliia. Designing Secured Services for Authentication, Authorization, and Accounting of Users (short paper). CPITS II 2023: 217–225.

29. King Davis. dlib. Version 19.22, dlib.net, 2022. https://dlib.net. (Accessed: 15 February 2024).

30. Geitgey A. (2023). face_recognition (Version 1.3.0) [Software]. Available at: https://github.com/ageitgey/face_recognition. (Accessed: 15 February 2024).

31. Security Service of Ukraine, Wanted Persons, https://ssu.gov.ua/u-rozshuku. (Accessed: 15 February 2024).

32. Non-government Center for Research of Elements of Crimes against the National Security of Ukraine, Peace, Humanity, and the International Law Information for law enforcement authorities and special services about pro-Russian terrorists, separatists, mercenaries, war criminals, and murderers, https://myrotvorets.center/. (Accessed: 15 February 2024).

33. WhatsApp | Secure and Reliable Free Private Messaging and Calling. Available at: https://www.whatsapp.com. (Accessed: 15 February 2024)

34. iMazing | iPhone, iPad & iPod Manager for Mac & PC. Available at: https://imazing.com. (Accessed: 15 February 2024).

ARTIFICIAL INTELLIGENCE TECHNIQUES APPLICATION IN THE MOBILE DEVICE DATA ANALYSIS TO IDENTIFY PERSON-OF-INTEREST

T. Fedynyshyn, O. Mykhaylova

Lviv Polytechnic National University,
Information Protection Department

The methods for identifying persons of interest (POI) based on mobile device data has been considered. The problem is relevant and unresolved in the activities of law enforcement, intelligence, and other agencies involved in operational search activities due to the large amount of data stored on mobile devices. Given the complexity and volume of mobile data, traditional analysis methods are often insufficiently effective. The authors propose use of artificial intelligence (AI), including machine learning and natural language processing, to improve the efficiency and speed of mobile device data analysis. This approach aims to overcome the limitations of manual data analysis and enhance the process of identifying POIs while adhering to the principles of forensic integrity. The research specifically demonstrates how machine learning can be utilized to search for persons of interest in WhatsApp messenger data.

A method has been developed for decentralized control of adaptive data collection processes using the principle of equilibrium and reinforcement learning using the normalized exponential function method. The developed method allows for efficient operation of autonomous distributed systems in conditions of dynamic changes in the number of data collection processes and limited information interaction between them.

The results of the experiment indicate that using artificial intelligence for facial recognition may result in false positive outcomes, implying that humans cannot be entirely replaced at the current stage of AI evolution. However, the application of deep learning showed an 88 % success rate in facial recognition. These findings underscore the transformative potential of artificial intelligence in mobile forensics, highlighting its capacity to enhance the accuracy and efficiency of data analysis in mobile devices.

Keywords: artificial intelligence, mobile forensics data analysis, ios, whatsapp.