техніки, електротехнік, розробник додатків для телефонів, програміст з робототехніки, спеціаліст з 3D (візуалізатор і модельєр), педагог за напрямом «Робототехніка».

А. Штундер
Науковий керівник – д.т.н., проф. Дудикевич В. Б.

СИСТЕМИ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON

Розпізнавання обличь – технологія, яка на сьогодні є наявною в більшості сфер нашого життя. В роботі наведено огляд основних біометричних методів ідентифікації людини а також інструментів , за допомогою яких можна реалізувати систему. Було створено систему розпізнавання обличь за допомогою мови програмування Python та підключених зовнішніх бібліотек OpenCV, Face_Recognition, dlib проекту Open Face, які є у вільному доступі на GitHub. Класифікація обличь здійснювалась звичайним перебором циклом for по базі даних відомих обличь. Реалізовано функціонал для реєстрації людини в базі даних, для порівняння двох зображень людей, для пошуку людини на фотографії, а також розпізнавання людини на відео в «прямому ефірі». Розглянуто переваги та недоліки реалізованого методу розпізнавання людини. Для подальшого розвитку методу доцільно застосувати досконаліші алгоритми класифікації ніж простий перебір, наприклад, Random Forest та метод опорних векторів. Архітектура розробленої програми дозволяє легко заміняти окремі модулі, що відкриває широкі можливості для подальшого розвитку системи.

Для того, щоб реалізувати розпізнавання обличчя з використанням Python, необхідними є всього 4 кроки.

1. Пошук усіх обличь

Для того, щоб знайти усі обличчя на зображенні, використовується алгоритм HOG – гістограма направлених градієнтів.

Це метод, який підраховує напрямки градієнтів в локальних точках зображення, створює простий “макет”, та шукає всі фрагменти зображення, схожі на шаблон обличчя.

2. Розміщення обличчя

Для цього використовується алгоритм, який називається – оцінка орієнтирів лиця. Ідея проста – на обличчі виділяють 68 орієнтирів, які є на кожному обличчі, наприклад, кутики очей, губ, кінчик носа тощо.

Далі методом афінних перетворень треба вирівняти лице так, щоб рот та очі були приблизно по центру.

3. Кодування лиця

Для реалізації цього кроку треба використати глибинне машинне навчання. Вхідні дані для навчання – 3 фото: 2 з них належать одній людині, та інше – іншій. На виході ми маємо отримати 128 вимірів кожного обличчя (карта лиця).

4. Пошук людини в базі

Цей крок найпростіший – за отриманою картою лиця треба знайти в базі відповідне ім'я людини. Тут можна використовувати будь-який алгоритм, який в певних умовах буде давати задовільні результати по швидкості пошуку.

Н. Швець
Науковий керівник – д. т. н., проф. Ромака В. А.

ДОСЛІДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ШЛЯХОМ ПОРІВНЯННЯ ТЕХНІК МОНІТОРИНГУ ТА АНАЛІЗУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Інформаційний простір охоплює всі сфери діяльності сучасної людини, тому актуальною є безпека інформаційних ресурсів, яка потребує розвитку та вдосконалення. Сучасні загрози інформаційної безпеки виникають у різних формах та спрямованні на широкий спектр вразливостей. Запобігання загрозам та виявлення атак на систему є одним з найголовніших завдань для забезпечення цілісності, доступності та конфіденційності інформації.

Головним напрямком даної роботи є моніторинг інформаційної системи та реагування на порушення даних та кібер-атак, які стають більш поширеними. Для виявлення шкідливого програмного забезпечення та спроб компрометації пристроїв інформаційної системи використовують різні техніки моніторингу. Одним із ключових факторів успішного виявлення атаки та перешкоди реалізації конкретної загрози є вибір інструментарію.

В даній роботі представлено дослідження по аналізу вірусу за допомогою двох наборів інструментів. Це дозволить оцінити ефективність використання конкретних програм та технік. Критеріями ефективності є досягнення поставленої мети по виявленню та запобіганню загрози, затрачений час та складність використання.