ВСТУП

Актуальність дослідження В наші дні однією з головних проблем на підприємстві, виробництві є незаконне проникнення на об'єкт з метою нанесення шкоди майну або розкрадання секретної інформації.

У зв'язку з цим необхідно контролювати всіх відвідувачів будівлі і припиняти спроби незаконного проникнення зловмисників. Так як всі об'єкти розрізняються за своїми конструкторським параметрам, створити одну універсальну систему не можна. Тому вкрай важливо спроектувати найбільш правильну для відповідного об'єкта систему контролю і управління доступом (СКУД), а також систему відеоспостереження. Але не можна забувати і про фінансову складову цього питання.

Для того щоб вибрати найбільш підходящий набір приладів необхідно проаналізувати не тільки їх технічні характеристики, але і їх вартість, щоб вартість спроектованої системи не перевищувала вартість об'єкта, що захищається майна та інформації.

Беручи до уваги швидкий розвиток нейронних мереж – їх використання в цій області – питання часу. На ринку з’являються нові ефективніші алгоритми, більші набори даних, певні оптимізаційні підходи, тож в сукупності з наявністю вже встановлених камер на підприємствах нейромережа може бути дуже оптимальним та зручним засобом для побудування СКУД.

Актуальність такої технології як нейромережа та ріст потреби в безпеці підприємств без додаткових зовнішніх засобів роблять цю роботу вкрай актуальною.

Мета та завдання дослідження. Метою дослідження є створення ефективного комплексу контролю доступу людини до об’єкту використовуючи останні досягнення в галузі обробки та ідентифікації людини по зображенню. Завдання – дослідити існуючі нейроні моделі та використовуючи сучасні архітектурні підходи та канали обміну створити зручну розширювану

архітектуру екосистеми по авторизації використовуючи відео канал як основний потік вхідної інформації.

Об'єкт та предмет дослідження. Об'єктом роботи є згорткові нейроні мережі.

Предметом є процес удосконалення пошуку обличчя на фотографії та класифікації його рис за допомогою загорткових нейронних мереж.

Наукова новизна та практична значущість результатів роботи полягає в тому, що вперше було використано передову версію нейронної мережі Массачусетского технічного університету, а також запропоновано новий спосіб навчання цієї нейронної мережі для підвищення якості роботи класифікаторів. Крім того було створено з нуля архітектуру системи контролю доступу в якій значно пришвидшено час ідентифікації користувача.

Отримана система може бути використані будь-де де необхідно обмежити доступ до об'єкту та забезпечити контроль за переміщенням персоналу. Крім того система може бути допрацьована та розширена модулем обліку часу на робочому місці або в робочому модулі.

Структура роботи. Структуру роботи складають перелік ключових слів, вступ, три розділи, висновки, список використаної літератури.

В першому розділі проаналізовано існуючих системи контролю доступу, визначено основні недоліки та переваги та критерії для оцінки майбутньої системи.

В другому розділі обґрунтовано використання основної технології майбутньої системи – аналізатора зображень – нейронної мережі. Досліджено наявні нейронні моделі та етапи аналізу зображення на предмет наявності зображення особи.

Третій розділ присвячений безпосередньо побудові архітектури системи, визначення фізичних та програмних властивостей майбутнього продукту та тестуванню результатів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ОБ'ЄКТУ

1.1 Опис та вимоги до системи контролю доступу

Системи контролю доступу (СКД) це системи в яких використовують спеціальне обладнання завдяки якому можна визначити повноваження доступу осіб на територію, що охороняється. Вони також забезпечують можливість контролю переміщення людей та машин по територіях організації. При переміщенні об'єкта (людина, машина, і т.п.) через пункти контролю доступу дані про проходження записуються в базу даних. Надалі ці дані доступні для аналізу та статистики.

Системи контролю доступу застосовуються може застосовуватись в офісних будівлях, підприємствах оптової торгівлі, бізнес-центрах, торгових центрах і т.п.

У найпростішій конфігурації система для авторизації особи можуть використовуватися два зчитувача – один на вхід і один на вихід. Після пред'явлення відвідувачем ІД-картки черговий на моніторі отримує фотографію та короткі деталі про власника картки. Ідентифікацію особи і визначення права на прохід пункту пропуску здійснює черговий. Складніші системи використовують фізичні бар'єри. Прохід через них в обох напрямках можливий за умови використання картки. Над фізичними бар'єрами можуть бути встановлені камери системи відеоспостереження. Прикладом фізичних бар'єрів служать турнікети, шлагбауми і т.п..

У системах контролю доступу може бути використано також спеціальні модулі для запобігання проносу або провезення заборонених предметів, в тому числі вибухових речовин, наркотичних засобів, зброї, ядерних матеріалів т.п.

Крім того СКД можуть бути інтегровані з системою відеоспостереженням чи охоронно-пожежної сигналізації, а також платіжною системою або з інформаційними системами організації [1].

Крім фізичних карток для ідентифікації можуть використовуватися біометричні дані а саме – ідентифікація за формою кисті руки, по відбитку пальця, за райдужною оболонкою ока.

Устаткування для контролю доступу можна вбудувати в двері всіх приміщень захищених областей. В таких випадках зчитувачі подвійних технології - Ргох або Smart плюс відбиток пальця здатні значно підвищити рівень безпеки завдяки додатковій ідентифікації особи.

Охоронна сигналізація зазвичай тісно інтегруються з системою контролю доступу. Навіть якщо системи контролю доступу та охоронної сигналізації були виконані різними виробниками вони можуть бути інтегровані на рівні програмного забезпечення, що дає можливість підключення вже встановленого на об'єкті обладнання до єдиного керуючого блоку.

Системи контролю доступу широко використовуються для управління рухом транспортних засобів по територіях підземних автостоянок. Ідентифікація проводиться постановкою автомобіля на індукційну петлю і пред'явленням водієм Ргох-карти на зчитувач. З урахуванням пріоритету даного користувача за допомогою світлофорів, шлагбаумів і воріт організовується траса для проїзду автомобіля. Для запобігання проривів в будівлю можуть використовуватися гідравлічні блокатори підйомного типу.

Систем контролю доступу може бути базою для створення інтегрованої охоронної системи яка і поєднує в єдиний комплекс підсистеми безпеки з різними функціями. В такому випадку здійснюється управління всіма підсистемами як єдиної багатоканальною та багатофункціональної охоронною системою а також забезпечується використання спільного протоколу подій всіх підсистем, обробка подій всіх підсистем, програмування тригерів на події, створення складних алгоритмів взаємодії підсистем. Така система має великі

вимоги до автономності та функціонуванню в надзвичайних ситуаціях, в тому числі в умовах виходу відсутності електроенергії або виходу з ладу її окремих компонентів.

Місця встановлення СКУД

- офіси компаній, бізнес-центри;
- банки;
- складські приміщення;
- заклади навчання(школи, технікуми, вузи);
- промислові підприємства;
- готелі;
- громадські заклади;
- охороняєм території;
- автостоянки, паркінги;
- місця проїзду автотранспорту;
- приватні будинки, котеджі.

Перерахуємо нижче основні можливості, які надає установка СКУД на об'єкті, що охороняється:

- Контроль і управління доступом це основна функція системи. Як вже було зазначено раніше, за допомогою даної функції проводиться поділ прав доступу співробітників в певні приміщення, а також відмова в доступі небажаним особам. Крім того, можливе дистанційне керування блокувальними пристроями (замки, турнікети і пр.). СКУД дозволяє заборонити прохід для співробітників у святкові та вихідні дні, а також після закінчення робочого дня.
- Збір і надання статистики. СКУД збирає інформацію про осіб, які пройшли через певні точки контролю доступу. По кожному співробітнику можливе отримання такої інформації: час входу та виходу, спроби доступу до заборонених для нього приміщення і зони, а також спроби проходу в недозволений час. Також можливо відстежити переміщення співробітника

по території із зазначенням місця і часу. Таким чином, всі виявлені порушення трудової дисципліни можуть бути занесені до особової справи співробітника, а керівництво порушника повідомлено в робочому порядку. Крім того, виходячи з інформації про останній точці проходу, СКУД дозволяє визначити місцезнаходження співробітника в будь-який момент часу.

- Доступ співробітника тільки за особистим ідентифікатором. При проході за допомогою ідентифікаційної карти на екрані монітора в пункті охорони може відображатися вся інформація по співробітникові і його фотографія, що виключає можливість проходу по чужому ідентифікатором. Також на рівні правил реакції СКУД можна забезпечити захист від передачі ідентифікатора іншій особі і блокувати повторний вхід на територію об'єкта з тієї ж самої карті доступу.
- Облік робочого часу. За допомогою вбудованої в СКУД системи обліку робочого часу, реєструється час виходу на роботу і час відходу з робочого місця. В результаті надається можливість визначити сумарний час перебування співробітника на робочому місці з урахуванням обідів. А на самому початку дня, наприклад, о 9:30 система обліку робочого часу, вбудована в СКУД може формувати груповий звіт про співробітників, які не пройшли через точку входу на територію. Це дозволяє в масовому порядку виявляти тих, хто запізнився або не з'явилися на робоче місце співробітників. Аналогічний звіт можна отримати і в кінці робочого дня на пункті виходу з території підприємства або офісу.
- Автономність роботи системи. СКУД оснащується системою безперебійного живлення, що дозволяє не переривати роботу в разі відключення електрики в будівлі. Також система контролю доступом завдяки функціоналу контролера має можливість продовжувати роботу, наприклад, при виході керуючого комп'ютера з ладу.

- Охорона об'єкта в реальному часі. СКДУ дає можливість ставити певні приміщення на охорону і знімати їх з охорони. Крім того, в реальному часі можна отримувати відомості про всілякі позаштатних і тривожних ситуаціях через спеціальні сповіщення відповідальних осіб. Крім цього в базі даних системи реєструються всі тривожні події і події, дає можливість доступу до цієї інформації в подальшому при необхідності. Завдяки наявним в СКУД коштів, співробітник охорони зі свого робочого місця за допомогою комп'ютера має можливість не тільки керувати дверима і турнікетами, а й подавати сигнали тривоги. У комп'ютер СКУД у співробітника охорони можуть бути занесені поверхові плани будівлі зі схемою розташування контролерів обмеження доступу.
- Віддалене управління системою через інтернет або з мобільного телефону.
- Якщо при установці підключити СКУД до мережі Інтернет, то в адміністрації з'являється можливість вести віддалене управління і контроль за роботою системи. Аналогічне можна сказати і про можливості управління СКУД зі свого мобільного телефону, правда це більше відноситься до GSM систем контролю доступу.
- Інтеграція СКУД з іншими системами безпеки і охорони. Системи контролю і управління доступом прекрасно поєднуються і вбудовуються з іншими системами безпеки: системою відеоспостереження, охоронною та пожежною сигналізацією. Так, наприклад, контроль доступом разом з відеоспостереженням забезпечують абсолютний контроль над охоронюваними приміщеннями. При виникненні нештатної ситуації така система в найкоротші терміни дозволить виявити і заблокувати порушника.
- При інтеграції СКУД і охоронної сигналізації є можливість налаштувати спільну реакцію системи на несанкціоноване проникнення в те чи інше приміщення. Наприклад, можна включити сирену на пункті охорони,

тривожною лампу або ж і зовсім заблокувати всі двері в необхідної частини будівлі.

- Інтеграція СКУД з системою пожежної сигналізації дозволяє автоматично розблокувати двері, турнікети і прохідні в разі пожежі. Всі ці заходи значно спрощують евакуацію персоналу таким важкий період.

1.2 Компоненти системи контролю доступу

Перед початком аналізу існуючих комп'ютерних систем контролю і управління доступом (СКУД), необхідно розглянути державну нормативну базу. Згідно ДСТУ IEC 60839 «Системи тривожної сигналізації та електронні системи безпеки." [2], СКУД - це сукупність засобів контролю та управління доступом, що володіють технічної, інформаційної, програмної та експлуатаційної сумісністю.

Засоби управління (ЗУ) – апаратні та програмні засоби які забезпечують установку режимів доступу, прийом і обробку інформації з зчитувачів, проведення ідентифікації і автентифікації, управління виконавчими і пристроями, що відображення і реєстрацію інформації.

Засоби контролю доступу в приміщення (засоби КУД) - механічні, електромеханічні пристрої та обладнання, електричні, електронні, електронні програмовані пристрої, програмні засоби, що забезпечують реалізацію контролю і управління доступом.

Керовані перешкоди (КП) - пристрої, що забезпечують фізичне перешкода доступу і обладнані виконавчими пристроями для управління їх станом (турнікети, прохідні кабіни, двері і ворота, обладнані виконавчими пристроями СКУД).

Пристрій зчитувач (ПС), зчитувач - це пристрій, призначений для зчитування (введення) ідентифікаційних ознак.

Пристрої виконавчі (ПВ) - це пристрої або механізми, що забезпечують приведення у відкрите або закрите стан КП (електромеханічні, електромагнітні замки, електромагнітні засувки, механізми приводу шлюзів, воріт, турнікетів і інші подібні пристрої).

Зчитувач - пристрій призначений для зчитування (введення) ідентифікаційних ознак.

Ще одним важливим поняттям СКУД є ідентифікатор користувача - унікальний ознака суб'єкта або об'єкта доступу. Як ідентифікатор може використовуватися код, біометричний ознака або фізичний ключ. Фізичний ключ - предмет, в який (на який) за допомогою спеціальної технології занесений ідентифікаційна ознака у вигляді кодової інформації (карти, електронні ключі, брелки та ін.).

1.3 Огляд альтернативних методів ідентифікації

У наш час існує велика кількість СКУД систем. Аналіз існуючих комп'ютерних систем допоможе визначити їхні переваги і недоліки. Завдяки цьому ми матимемо можливість виділити основні критерії до майбутньої системи в цілому [3].

1.3.1 Ідентифікація по геометричній будові руки і пальців

Системи контролю доступу з використанням геометрії рук мають найдовшу історію впровадження серед всіх біометричних методів. David P. Sidlauskas розробив та запатентував концепцію геометрії руки в 1981 році і протягом року з’явились перші доступні комерційні системи розпізнавання геометрії рук. Серед великих реалізацій можна виділити використання ідентифікації на Олімпійських іграх 1996 р.. Саме там реалізували авторизації за геометрією руки для контролю та захисту фізичного доступу до олімпійського села. Багато компаній реалізують системи сканування геометрію рук паралельно

з тактовими часами для контролю доступу. Уолт Дісней Світ використовував подібну "пальчикову" геометрію протягом декількох років для прискорення та полегшення входу до парку та гостей як придбали сезонний квиток. Саме ця система допомогла запобігти шахрайству з цим типом квитків.

Метод ідентифікації користувачів за геометрією руки за її технологічною структурою та рівнем надійності цілком можна порівняти із методом ідентифікації людини за відбитками пальців. Статистична ймовірність існування двох рук з однаковою геометрією надзвичайно мала. Але ознаки руки змінюються з віком, а сам прилад порівняно великий.

У біометриці виділяють два основні методи розпізнавання за геометрією руки:

Першому методу вже більше 25 років - від народження біометричних систем контролю доступу до приміщень. Він базується лише на геометричних характеристиках руки. З точки зору компактності зображення, цей клас систем є найбільш економічним. У найпростішій версії зберігається лише інформація про довжину і ширину пальців для чого потрібно лише 9 байт. Очевидно що аби обманути таку систему достатньо просто зробити картонний манекен оригінальної руки. Більш складними є системи, що вимірюють профіль руки, що включає об’єм руки, пальців, шорсткість долоні, розташування складок шкіри на руці;

Вихідними біометричними ознаками руки є радіус вписаного в долоню окружності, ширина долоні, довжини пальців (це дистанція від виділених верхніх контрольних точок до центрів ліній нижніх контрольні точки), висота та ширина пальців чи кисті руки в трьох пунктах.

Другий метод є більш сучасним, він базується на змішаних фізичних характеристиках. До них належать відносяться зображення флангів пальців в зонах згину, карта підшкірних кровоносних судин. З чотирьох характеристик що отримуються з руки 3 є скалярними і описують розмірів пальців.

Три перші характеристики

- висота вказівного пальця
- ширина вказівного пальця
- довжина середнього пальця

Згин між середньою і нижньою фалангою вказівного пальця є четвертою характеристикою. В цьому методі всі характеристики можна вмістити в 9 байтів.

Як приклад розглянемо зчитувач HandKey. Сучасні біометричні системи компанії Recognition Systems призначені для ідентифікації персоналу, що проходить на територію об'єкту, що охороняється. На відміну від традиційних систем контролю доступу, що працюють з різними електронними картами, в біометричних системах, що працюють за технологією HandKey, ідентифікатором є рука співробітника. Біометричні зчитувачі HandKey розпізнають персонал за розміром і формою кисті руки, що забезпечує високий рівень безпеки в силу унікальності будови кисті руки кожної людини.

Метод тривимірної ідентифікації HandKey передбачає звірення профілю руки вхідної людини з раніше отриманим шаблоном за розміром долоні, довжині, ширині і товщині пальців і по ряду інших параметрів. Первісна запис шаблону геометрії руки реалізується за допомогою триразового сканування кисті руки співробітника і усереднення отриманої інформації.

Для того щоб біометрична система могла призвести зчитування, людина повинна покласти долоню руки на панель пристрою, а спеціальні штирі-фіксатори допомагають скоригувати її розташування. Вбудовані світлодіоди на панелі пристрою для читання сигналізують про коректність розташування долоні, що спрощує взаємодію людини з пристроєм.

Процедура верифікації кисті руки здійснюється за допомогою інфрачервоного підсвічування і реєстрації даних спеціальної CCD-телекамерою. За рахунок бічних дзеркал, які потрапляють в огляд телекамери, пристрій також отримує інформацію про товщину і габаритах кисті руки. Отримане зображення біометричних показників перетвориться за спеціальним алгоритмом в цифрову інформацію (розмір шаблону - 9 байт), після чого відбувається порівняння даних

з шаблоном, що зберігаються в пам'яті. За результатами відповідності отриманої інформації шаблоном біометрична система приймає відповідне рішення.

Системи HandKey здійснюють процедуру ідентифікації особистості в два взаємопов'язаних етапи: набір унікального ідентифікаційного номера, що складається з 1-10 цифр, і безпосередньо сканування кисті руки на панелі пристрою для читання. У порівнянні з традиційними системами контролю доступу, що використовують зчитувачі різних електронних карт, біометричні системи вимагають тільки запам'ятовування коду. Також важливо наголосити на тому, що другий етап ідентифікації - сканування кисті руки користувача і повністю виключає несанкціонований прохід в приміщення, що охороняються за чужий або вкраденої карті доступу.

У той же час біометричні системи доступу (створені на основі біометричних зчитувачів HandKey II) передбачають можливість підключення зчитувачів карт доступу, що дозволяє використовувати різні електронні картки замість набору унікального ідентифікаційного номера на клавіатурі зчитувача. Як правило, зчитувачі карт доступу підключають до біометричних зчитувачів з метою оптимізації часу ідентифікації - при великому потоці людей не потрібно втрачати час на набір свого ідентифікаційного номера перед процедурою верифікації кисті руки.

Двоетапна процедура ідентифікації користувача з одного боку істотно підвищує рівень безпеки, а з іншого боку дозволяє практично миттєво здійснити перевірку з бази даних. Тобто, набираючи свій індивідуальний код на клавіатурі системи (або, як варіант, використовуючи карту доступу) людина, перед тим як пройти верифікацію за формою кисті руки, заздалегідь «повідомляє» біометричного зчитувача з яким саме шаблоном порівнювати отримані дані. Таким чином, час верифікації за формою кисті руки не перевищує 1 секунди, а загальний час ідентифікації в системі з урахуванням набору коду або використання електронної карти становить 1-5 секунд.

Переваги методу ідентифікації по геометричній будові руки і пальців:

- "Ключ" завжди з користувачем;
- не пред'являються вимоги до чистоти, вологості, температури;

Недоліки методу:

- громіздкість пристроїв (за деяким винятком);
- невисока складність виготовлення муляжу для пристроїв першого типу (що використовують тільки геометричні характеристики).

1.3.2 Ідентифікація на основі RFID карт

Основним елементом безконтактних ідентифікаційних засобів є обрамлена електронікою спеціально організована пам'ять, оформлена у вигляді пластикової ідентифікаційної карти або інший конструкції. Збільшення обсягу пам'яті ідентифікаційної карти, поділ цієї пам'яті на незалежні сектори перетворило її в багатофункціональну (інформаційну) карту (ІК) [4].

Можливості ідентифікаційної карти дозволяють створити єдиний багатофункціональний електронний документ для кожного об'єкта. Залежно від характеру об'єкта розрізняють два основних типи інформаційних карт:

- інформаційна карта майна (тварини, автомобіля і т.п.);
- інформаційна карта людини, виконана, як правило, у вигляді стандартної пластикової карти.

Сучасний рівень електроніки дозволяє створити багатофункціональний документ, який супроводжує людину у всіх процесах життєдіяльності і дозволяє автоматизувати всі операції його обслуговування.

При безконтактної радіочастотної ідентифікації зчитування інформації з розміщеного на об'єкті ідентифікатора виробляється без фізичного, електричного або оптичного контакту. Досить, що б ідентифікатор і зчитувач знаходилися на відстані не більше заданого (зазвичай це кілька сантиметрів, десятки сантиметрів або метрів), при чому між ними може бути будь-яка неметалічна перешкода., Наприклад стінка ящика, стрічка транспортера, стіна приміщення.

Для здійснення безконтактної радіочастотної ідентифікації потрібні три компоненти:

- Транспондер (відповідач-ідентифікатор), розміщений на об'єкті, який підлягає ідентифікації;
- Зчитувач інформації з ідентифікатора (він же, якщо передбачено, записує інформацію в транспондер);
- Одержувач інформації-додаток, комп'ютерна система обробки даних або оператор.

Зчитувач зазвичай містить радіочастотний модуль (передавач і приймач), блок управління, що включає мікропроцесор і пам'ять, і елемент зв'язку з транспондером. Крім того, багато зчитувачі обладнуються додатковим інтерфейсом (RS 232, RS 485), що б мати можливість передавати прийняті дані в іншу систему (ПК, систему обробки даних).

Транспондер являє собою пристрій, що є фактично носієм даних RFID-системи, і зазвичай включає в себе приймач, що передає схему, антену і блок пам'яті для зберігання інформації. Приймач, схема і пам'ять конструктивно виконуються у вигляді окремої інтегральної схеми. Іноді до складу конструкції радіочастотної мітки включається автономне джерело живлення. Коли транспондер, який зазвичай не має свого власного джерела напруги, що не знаходиться в зоні опитування зчитувача, він повністю пасивний. Транспондер активізується тільки тоді, коли він знаходиться в зоні опитування зчитувача. Енергія, необхідна для активізації транспондера, подається на транспондер безконтактно через блок зв'язку разом з синхроімпульсами і даними.

Процес радіочастотної ідентифікації виконується наступним чином:

- Передавач зчитувача через антену безперервно (або в заданий час) випромінює посилку радіосигналу з прийнятою в даній системі частотою;
- Транспондер, що знаходиться в зоні дії зчитувача, через свою антену приймає цей радіосигнал і використовує його енергію для електроживлення (в цьому полягає пасивність ідентифікатора - йому не

потрібно джерело живлення). Транспондер зчитує код зі свого пристрою, що запам'ятовує і моделює у відповідь радіосигнал;

- Зчитувач приймає відповідний сигнал, виділяє укладений в ньому код, проводить, якщо це передбачено, операції криптографічного захисту й процедури антіколізії (послідовної роботи з декількома ідентифікаторами, одночасно знаходяться в зоні дії зчитувача) і передає інформацію за призначенням в: додаток, систему обробки даних або оператору .

Частота електромагнітного випромінювання і зворотного сигналу, що передається транспондером, значно впливають на показники роботи RFID-системи.

Робоча частота RFID-системи визначає її сферу застосування. Низькочастотні RFID-системи використовуються там, де допустимо невелику відстань між об'єктом і зчитувачем. Звичайне відстань зчитування складає 0,5 м, а для мініатюрних тегів дальність читання, як правило ще менше близько 0,1 м. Низьку частоту використовують більшість систем управління доступом, системи управління складами і виробництвом.

RFID-системи з проміжними значеннями робочої частоти використовуються там, де необхідно передавати великі кількості даних, наприклад в системах контролю доступу, в смарт-картах.

Високочастотні RFID-системи використовуються, там де потрібна велика відстань і висока швидкість читання, наприклад при контролі дорожніх вагонів, контейнерів, автомобілів, систем збору відходів. Велика дальність дії уможливлює безпечну установку зчитувачів поза межами досяжності людей.

За допомогою RFID-систем успішно вирішується цілий ряд складних організаційно-технічних завдань:

- Скорочення витрат на введення даних і виключення помилок, пов'язаних з ручним введенням інформації.
- Повністю автоматична реєстрація ідентифікованих об'єктів з подальшою комп'ютерною обробкою результатів (приклад: система реєстрації

пасажирів маршрутного таксі або автобуса з автоматичним справлянням плати за проїзд)

- Забезпечення високої оперативності реєстраційної інформації для менеджерів і клієнтів компанії
- Високий ступінь автоматизації управління майном, складами, транспортом, доступом людей в приміщення
- Поліпшення контролю якості в виробничих, складських і транспортних операціях
- Скорочення облікового документообігу і трудовитрат.

На основі засобів безконтактної радіочастотної ідентифікації можуть бути налаштовані найрізноманітніші прикладні системи.

Переваги RFID:

- Безконтактна робота - RFID-мітка може бути прочитана без будь-якого фізичного контакту між міткою і рідером.
- Перезапис даних - дані RFID-мітки з перезаписом (RW-мітки) можуть бути перезаписані велике число раз.
- Робота поза прямої видимості - щоб RFID-мітка була прочитана RFID-рідером, в загальному випадку не потрібно її знаходження в зоні прямої видимості рідера.
- Різноманітність діапазонів читання - діапазон читання RFID-мітки може становити від декількох сантиметрів до 30 метрів і більше.
- Широкі можливості зберігання даних - RFID-мітка може зберігати інформацію обсягом від декількох байтів до практично необмеженої кількості даних.
- Підтримка читання декількох міток - RFID-рідер може автоматично читати кілька RFID-міток в своїй зоні читання за дуже короткий період часу.
- Міцність - RFID-мітки можуть значною мірою протистояти жорстким умовам навколишнього середовища.

- Виконання інтелектуальних завдань - крім зберігання і передачі даних, RFID-мітка може призначатися для виконання інших завдань (наприклад, для вимірювання таких умов навколишнього середовища, як температура і тиск).
- Висока точність читання - RFID є точною на 100%.

RFID-мітки практично неможливо підробити, так як при виробництві мітці присвоюється унікальне незмінне число-ідентифікатор. Цей унікальний ідентифікатор або інші дані на мітці можна зашифрувати сучасними методами зворотного шифрування. Крім того цифровий пристрій як і будь яка радіочастотна мітка може бути захищений паролем від запису чи зчитування даних. В одній мітці одночасно можна зберігати відкриті і закриті дані.

Однак RFID має недоліки:

- Необхідно забезпечувати безпеку даних так, щоб мітка не могла бути переписана або випадково (які мають на те право рідером), або навмисно (рідером, використовуваним шахраями).
- Час, необхідний для правильної передачі рідера всіх своїх бітів даних міткою з великим об'ємом пам'яті, може багаторазово перевищувати час передачі тільки унікального ідентифікатора.
- Крім того, збільшення обсягу переданих даних веде до підвищення частоти виникнення помилок передачі.
- Мітка з великим об'ємом пам'яті буде дорожче міток, які можуть зберігати лише унікальний ідентифікатор.

1.3.3 Ідентифікація за малюнком райдужної оболонки і сітківки ока

На даний момент в світі найбільш відомі дві технології, які використовують в якості ідентифікатора очей людини, вони є одними з найбільш високонадійних серед біологічних методів.

Перша заснована на ідентифікації малюнка райдужної оболонки ока. Друга технологія використовує метод сканування очного дна сітківки ока і базується на унікальності кутового розподілу кровоносних судин для кожної людини.

При ідентифікації по райдужній оболонці ока використовуються індивідуальні відмінності складних малюнків райдужної оболонки ока людини для встановлення індивідуальних особливостей. Ідентифікація по райдужній оболонці ока є найточнішою з усіх біометричних ідентифікаційних систем. Коефіцієнт помилкової ідентифікації є настільки низьким, що вірогідність помилкової ідентифікації однієї особи в якості іншої практично дорівнює нулю..

Характеристики райдужної оболонки ока:

- дуже складний малюнок, який відрізняється навіть у близнюків;
- малюнок стабілізується у віці від шести місяців до двох років і залишається незміненим протягом усього життя;

Розглянемо, як же здійснюється ідентифікація по райдужці. Першим етапом, природно, є отримання досліджуваного зображення. Робиться це за декількох різних камер. Варто відзначити що для якісної ідентифікації потрібно використовувати не один а декілька знімків.

Другий етап - виділення зображення райдужної оболонки ока. Сьогодні існує багато способів якісного отримання області райдужної оболонки за описаними ознаками.

Наступний етап ідентифікації - це приведення розміру зображення райдужної оболонки до еталонного. Для цього є дві причини.

Перша – в залежності від умов зйомки (відстань для об'єкта, освітленість) розмір зображення може змінюватися. Відповідно і елементи райдужки теж будуть виходити різними. Втім, з цим особливих проблем не виникає. Це завдання вирішується шляхом масштабування. А ось з другої причиною справи йдуть не так добре. Під впливом деяких факторів може змінюватися розмір самої райдужної оболонки. При цьому розташування її елементів відносно один одного стає трохи іншим. Спеціально розроблені алгоритми дозволяють

вирішити це завдання. Вони створюють модель райдужної оболонки ока і відтворюють можливе переміщення її елементів за певними законами.

Наступним кроком є отримання зображення райдужної оболонки ока в полярній системі координат. Це суттєво полегшує всі майбутні розрахунки адже райдужка - це майже коло, а всі основні її елементи розташовуються по колу і перпендикулярним їм прямим відрізках. Крім того в деяких системах ідентифікації цей етап неявний: він поєднаний з наступним.

П'ятий етап в процесі ідентифікації є вибірка елементів райдужної оболонки ока що можуть бути використані в біометрії. Це найскладніший етап тому що проблема полягає в відсутності на райдужній оболонці жодних характерних деталей. Тому використання не можна використовувати сталі звичними в інших біометричних технологіях значення, її розміру, відстані до інших елементів і т.д. В цьому випадку використовуються складні математичні перетворення, здійснювані на основі наявного зображення райдужної оболонки.

Ну і, нарешті, останнім етапом ідентифікації людини за райдужною оболонкою ока є порівняння отриманих параметрів з еталонами. І в цій дії є одна відмінність від багатьох інших подібних завдань. Справа в тому, що при виділенні унікальних характеристик необхідно враховувати закриті області. Крім того, частина зображення може бути спотворена століттями або відблисками від зіниці. Таким чином, деякі параметри можуть істотно відрізнятися від еталонного. Втім, ця проблема досить легко вирішується завдяки надмірного вмісту на райдужній оболонці ока унікальних для кожної людини елементів. Як вже було сказано, збіги 40% з них досить для надійної ідентифікації особистості. Решта ж можуть вважатися "зіпсованими" і просто-напросто ігноруватися.

Цей вид біометричного розпізнавання є одним з найнадійніших. Причиною тому - генетично обумовлена унікальність райдужної оболонки ока, яка відрізняється навіть у близнюків.

Сітка кровоносних судин сітківки ока також унікальна для кожної людини. Вона не зумовлена генетично і, тому, різна навіть у близнюків. У той же час вона стабільна протягом усього життя людини, що робить її надзвичайно зручним ідентифікатором. У терміналах для ідентифікації по сітківці використовується спеціальна камера з електромеханічним сенсором що реєструє, відображає та поглинає характеристики сітківки з відстані. Випромінююча лампа має малу потужність, виключає будь-який негативний вплив на людину і не викликає дискомфорту. Перед процесом ідентифікації клієнт вводить свій PIN-код і дивиться в спеціальний окуляр. Імовірність помилки другого роду (помилковий допуск) FAR = одна мільйонна (при будь-яких обставинах).

З точки зору зручності самого процесу, технологія ідентифікації по райдужній оболонці ока має істотну перевагу в порівнянні з сітківкою, оскільки немає необхідності дивитися в "очок" з відстані 3 см, а досить просто підійти до зчитувача на відстань близько 25 см.

Переваги методу ідентифікації по сітківці і райдужну оболонку ока:

- статистична надійність методу;
- захоплення зображення райдужної оболонки можна проводити на відстані від декількох сантиметрів до декількох метрів, при цьому фізичний контакт людини з пристроєм не відбувається;
- райдужна оболонка захищена від пошкоджень рогівкою (наприклад, відбитки пальців легко псуються подряпинами або брудняться)

  велика кількість методів протидії підробкам.

Недоліки методу:

- ціна системи для захоплення райдужної оболонки перевищує номінальну вартість сканера відбитка пальця і камери для захоплення 2D зображення особи;
- ідентифікацію по сітківці ока цілком можна обдурити

- необхідно відзначити деякі труднощі психологічного характеру - не всі люди спокійно ставляться до самої процедури сканування сітківки, хоча з медичної точки зору вона нешкідлива.

1.4 Визначення основних вимог та обмежень

Згідно нормативних документів загальні вимоги до систем контролю і управління доступом полягають в наступному:

- забезпечення захисту від несанкціонованого доступу на об'єкт, що охороняється (приміщення, зону) в режимі зняття їх з охорони;
- контроль і облік доступу персоналу (відвідувачів) на об'єкт, що охороняється (приміщення, зону) в режимі зняття їх з охорони;
- автоматизація процесів взяття / зняття об'єкта, що охороняється (приміщення, зони) за допомогою засобів ідентифікації СКУД в складі пристроїв і приладів охоронної сигналізації;
- захист і контроль доступу до комп'ютерів автоматизованих робочих місць (АРМ) пультового обладнання систем охоронної сигналізації;
- захист від несанкціонованого доступу до інформації.

СКУД в робочому режимі повинна забезпечувати автоматичну роботу. Режим ручного або автоматизованого управління (за участю оператора) повинен забезпечуватися тільки при виникненні надзвичайних, аварійних або тривожних ситуацій, або при наявності відповідних вимог в технічному завданні.

Проектована СКУД повинна також забезпечувати:

- видачу сигналу на відкриття КУД при зчитуванні зареєстрованого в пам'яті системи ідентифікаційна ознака;
- заборона відкриття КУД при зчитуванні незареєстрованої в пам'яті системи ідентифікаційна ознака;
- запис ідентифікаційних ознак в пам'ять системи;

- захист від несанкціонованого доступу при записі кодів ідентифікаційних ознак в пам'яті системи;
- збереження ідентифікаційних ознак в пам'яті системи при відмові і відключенні електроживлення;
- ручне, напівавтоматичне або автоматичне відкриття КУД для проходу при аварійних ситуаціях, пожежі, технічні несправності відповідно до правил встановленого режиму і правил протипожежної безпеки;
- автоматичне формування сигналу закриття на КУД при відсутності факту проходу;
- видачу сигналу тривоги при аварійному відкритті УПУ для несанкціонованого проникнення.

Режим контролю доступу розробляється СКУД - односторонній, з ідентифікацією при вході і вільним виходом.

Також розробляється СКУД повинна забезпечувати можливість безперервної роботи з урахуванням проведення регламентного технічного обслуговування.

Крім того, при проектуванні СКУД слід врахувати наступні моменти:

- зчитувач повинен бути відділений від контролера, щоб ланцюги, по яких проводиться відкриття замку, були недоступні;
- переважно використовувати обладнання в антивандальному виконанні з урахуванням кліматичних вимог;
- система повинна мати мінімальну надмірністю обладнання;
- система повинна бути легко масштабується;
- система повинна мати запас масштабованості;
- система повинна легко інтегруватися з іншими системами;
- система повинна мати резервне джерело живлення на випадок зникнення мережі або навмисного його відключення.

Вимоги до методу ідентифікації:

- низька вартість радіочастотного зчитувача;

- звичність і зрозумілість самої процедури і правила ідентифікації для персоналу.

1.5 Економічні переваги пункту пропуску з використанням відеоспостереження

Процес виробництва ґрунтується на взаємодії трьох основних елементів: основних виробничих фондів, оборотних коштів і робочої сили. При використанні засобів виробництва (знаряддя і предмети праці) працівниками матеріальної сфери забезпечується випуск продукції. Ефективність виробництва визначається шляхом зіставлення кінцевого результату господарської діяльності підприємства (ефект) з витратами живої і уречевленої праці на його досягнення.

Ефект, або кінцевий результат, господарської діяльності характеризують різними вартісними і натуральними показниками, наприклад обсяг виробництва, прибуток, економія по окремих елементах витрат, загальна економія від зниження собівартості продукції.

Всі витрати, пов'язані з досягненням ефекту, підрозділяються на поточні (оплата живої праці, вартість спожитих матеріалів, сировини та інших матеріальних ресурсів, амортизаційні відрахування, витрати на підтримку основних виробничих фондів в стані (витрати на ремонт) та інші витрати, що включаються в повну собівартість промислової продукції). І одноразові (витрати, авансовані для розширеного виробництва основних виробничих фондів, вдосконалення їх структури з метою підвищення конкурентної можливості і т.п.).

Рівень ефективності виробництва оцінюється за допомогою системи загальних (прибуток і рентабельність виробництв) і приватних показників (продуктивність праці, капіталомісткість (фондомісткість), матеріаломісткість продукції і т.п.).

Продуктивність праці це співвідношення вироблення продукції подальшого року до вироблення попереднього, тобто її фактичної величини до планової і т. д.. Зростання продуктивності праці буде спостерігатися, коли співвідношення перевищить одиницю.

Матеріаломісткість - це вартість матеріальних витрат, певна шляхом віднесення до собівартості або вартості валової або товарної продукції. Зниження матеріаломісткості - один із напрямів підвищення ефективності промислового виробництва.

Фондомісткість продукції відображає вартість основних виробничих фондів, що припадає на один рубль вартості валової або товарної продукції. Питома фондомісткість продукції - вартість основних виробничих фондів, що припадає на одиницю виробленої продукції. При зниженні фондоємність підвищується ефективність виробництва.

Основні фонди підприємства є найбільш значущою складовою частиною майна підприємства і його необоротних активів.

Основні засоби – це засоби праці, які неодноразово беруть участь у виробничому процесі, зберігаючи при цьому свою натуральну форму, а їх вартість переноситься на вироблену продукцію частинами в міру зношування.

Таблиця 1.1 - Основні фонди

Назва ОПФ	Характеристика ОПФ	Ціна, грн.
комп'ютер	Intel Pentium 5 3GHz; 1024 DDR4; HD 256 Gb;	15000
відео монітор	HD монітор	5000
IP-відеокамера (5 шт)	З кольоровим зображенням	5*2000 = 10000
сервер обробки інформації	Intel Pentium 7 3GHz; 2048 DDR4; SSD 512 Gb; MSI PCI-Ex GeForce GTX 1660 6G 6GB GDDR5	30000

Основне завдання на підприємстві повинна зводитися до того, щоб не допускати надмірного старіння основних виробничих фондів (ОПФ) (особливо активної частини), так як від цього залежать рівень їх фізичного та морального зносу, але і результати роботи підприємства.

Отже вартість враховуюи основні фонди: 60 000 грн.

Розрахуємо амортизаційні відрахування, так як вони знадобляться нам для подальшого розрахунку, для цього візьмемо прискорену норму амортизації, яка дорівнює 10%, тобто $Н_а = 0,1$.

Прискорена амортизація поширюється тільки на основні фонди, які використовуються при виробництві нових прогресивних видів матеріалів, обчислювальної техніки, приладів і обладнання. Це дозволяє накопичити достатні кошти для технічного переозброєння і реконструкції виробництва, прискорити процес оновлення активної частини основних виробничих фондів на підприємстві, уникнути морального і фізичного зносу активної частини основних виробничих фондів, зменшити податок на прибуток. Підтримка основних фондів на високому технічному рівні крім того створює хорошу основу для збільшення обсягу виробництва, випуску більш якісної продукції і зниження її собівартості. Розрахувати можна за формулою 2.1.

$$A = \text{ВОФ} * H_a \qquad (2.1)$$

де А - амортизаційні відрахування,

ВОФ - вартість основних фондів,

$Н_а$ - норма амортизації,

В результати отримуємо 6000 гривень як амортизаційні вимоги.

Підсумовуючи все вище пораховане отримуємо вартість в 66000 гривень в перший рік використання. Переваги цього методу полягають в тому що не потрібно витрачати надалі ресурси на випуск фізичних карток чи інших елементів доступу. Крім того відеокамери можуть працювати в режимі запису

що дозволить підвищити рівень безпеки на підприємстві, а враховуючи що вони вже встановлені в багатьох пунктах пропуску – ціна запуску системи різко знижується.

Основна перевага перед іншими біологічними системами – відсутність необхідності в придбанні специфічних пристроїв для отриманні біологічної інформації. Камери давно зайняли місце на підприємствах і в багатьох випадках їх якість дозволяє уникнути придбання нових апаратів.

Висновки до розділу

В першому розділі було розглянуто альтернативні методи ідентифікації. В результаті чого було визначено основні характеристики майбутньої системи а також переваги та недоліки існуючих, з якими потрібно буде конкурувати. Було розглянуто питання економічної вигоди від використання СКУД на основі відеоспостереження.

РОЗДІЛ 2. АНАЛІЗ ВИКОРИСТАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ

2.1 Обґрунтування використання нейронної мережі як аналізатору зображень

Сьогодні існують системи які здатні позмагатись з людським мозком в плані швидкості виконання різних операцій, але повністю зімітувати принцип роботи мозку обчислювальною машиною ще не вдалось. Саме це спонукає і направляє роботи вчених з усього світу у створення і дослідження штучних нейронних мереж.

Перших спробами розкрити секрет високої ефективності мозку можна вважати роботу Рамон-і-Кахаля (1911), де висловлено ідею про нейрон як структурну одиниці мозку. Однак нейрон має на 5-6 порядків меншу швидкість спрацьовування, ніж напівпровідниковий логічний елемент. Майбутні дослідження показали що секрет високої продуктивності мозку полягає у величезній кількості нейронів і масивних взаємозв'язках між ними [5].

Мережа нейронів що утворює людський мозок, є високоефективною, комплексною, нелінійною та багатопоточною системою обробки інформації. Вона здатна організувати свої нейрони таким чином, щоб реалізувати сприйняття образу, його розпізнання або управління рухом, у багато разів швидше, ніж ці завдання будуть вирішені найсучаснішими комп'ютерами.

ІНС є спрощеною моделлю мозку. Вона будується на основі штучних нейронів, які володіють тим же рівнем пластичності що живі нейрони. Використання структури мозку і пластичності нейронів робить ІНС універсальною системою обробки інформації. У загальному випадку ІНС - це машина, що моделює спосіб роботи мозку. Зазвичай ІНС реалізуються у вигляді електронних пристроїв чи комп'ютерних програм [6]. Серед багатьох можна виділити визначення ІНС як адаптивної машини, дане в: штучна нейронна

мережа - це істотно паралельно розподілений процесор, який володіє природною схильністю до збереження досвідченого знання і можливістю надання його нам. Вона схожа з мозком в двох аспектах: знання здобувається мережею в процесі навчання, для збереження знання використовуються сили міжнейронних з'єднань, звані також синаптическими вагами [7-8].

Процедура, яка використовується для здійснення процесу навчання, називається алгоритмом навчання. Її функція полягає в модифікації синаптичних ваг ІНС певним чином так, щоб вона набула необхідних властивості.

Модифікація ваг є традиційним способом навчання ІНС. Такий підхід близький до теорії адаптивних лінійних фільтрів, які вже давно і успішно застосовуються в управлінні. Однак для ІНС існує ще і можливість модифікації власної топології, яка ґрунтується на тому факті, що в живому мозку нейрони можуть з'являтися, вмирати і змінювати свої зв'язки з іншими нейронами.

Дві властивості ІНС дозволяють реалізують свою обчислювальну потужність, а саме: паралельно-розподілена структура нейронної мережі та вміння навчатися і узагальнювати отримані навички. Під властивістю узагальнення мається на увазі вміння ІНС генерувати правильні шари та виходи для вхідних сигналів, які ще не були створенні в процесі навчання (тренування). Ці дві властивості роблять ІНС системою переробки інформації, яка вирішує складні багатовимірні завдання, непосильні іншим технікам.

З точки зору машинного навчання нейронна мережа являє собою окремий випадок набору методів по розпізнаванню образів, методів кластеризації дискримінантного аналізу, і т.п. З математичної точки зору, навчання нейронних мереж це багатопараметричне завдання нелінійної оптимізації. Кібернетика розглядає нейронну мережу в рамках задачі адаптивного управління і як алгоритми для робототехніки. З точки зору розвитку обчислювальної техніки та програмування, нейронна мережа - спосіб вирішення проблеми ефективного паралелізму. Для штучного інтелекту ІНС є основним напрямком в структурному підході з вивчення можливості побудови (моделювання)

природного інтелекту за допомогою комп'ютерних алгоритмів та основою філософської течії коннектівізма [9].

Штучна нейронна мережа (ІНС, нейронна мережа) - це набір нейронів, з'єднаних між собою. Як правило, передавальні функції всіх нейронів у нейронної мережі фіксовані, а ваги є параметрами нейронної мережі і можуть змінюватися. Деякі входи нейронів позначені як зовнішні входи нейронної мережі, а деякі виходи - як зовнішні виходи нейронної мережі. Подаючи будь-які числа на входи нейронної мережі. Ми отримуємо якийсь набір чисел на виходах нейронної мережі. Таким чином робота нейронної мережі полягає в перетворенні вхідного вектору у вихідний вектор, причому це перетворення задається вагами нейронної мережі [10].

Штучна нейронна мережа це сукупність нейронних елементів та зав’язків між ними.

Основу кожної штучної нейронної мережі складають відносно прості, в більшості випадків - однотипні, елементи (комірки), що імітують роботу нейронів мозку (далі під нейроном ми будемо мати на увазі штучний нейрон, осередок штучної нейронної мережі).

Нейрон має групу синапсів - односпрямованих вхідних зав’язків, з'єднаних з виходами інших нейронів. Кожен синапс характеризується величиною синоптичної зв'язку або її вагою.

Кожен нейрон має поточний стан, яке зазвичай визначається, як зважена сума його входів:

Нейрон має аксон - вихідну зв'язок даного нейрона, з якої сигнал (збудження або гальмування) надходить на синапси наступних нейронів. Вихід нейрона є функція його стану: = F (s) [11]

Функція активації може мати різний вигляд:

- пороговий,
- кусочно-лінійний,
- пігмоїд;

Безліч всіх нейронів штучної нейронної мережі можна розділити на підмножини - шари. Взаємодія нейронів відбувається пошарово.

Шар штучної нейронної мережі - це безліч нейронів, на які в кожен такт часу паралельно надходять сигнали від інших нейронів даної мережі

Вибір архітектури штучної нейронної мережі визначається завданням. Для деяких класів задач вже існують оптимальні конфігурації. Якщо ж завдання не може бути зведена ні до одного з відомих класів, розробнику доводиться вирішувати задачу синтезу нової конфігурації. Проблема синтезу штучної нейронної мережі сильно залежить від завдання, дати загальні докладні рекомендації важко. У більшості випадків оптимальний варіант штучної нейронної мережі виходить дослідним шляхом.

Штучні нейронні мережі можуть бути програмного і апаратного виконання. Реалізація апаратна зазвичай являє собою паралельний обчислювач, що складається з безлічі простих процесорів.

Обличчя – це найстійкіше зображення у зоровій системі людини. Тож не дивно, що ми володіємо чудовою здатністю до їх розпізнавання. Як правило, нам потрібен лише один погляд на обличчя щоб ми запам’ятали цю людину. Таким чином, не дивно, що у нас є виділена область в мозку виключно для обробки обличчя, а також для їх розпізнавання.

Обличчя також підходить гарно підходить для ідентифікації особи – риси лиця без хірургічного втручання змінити майже не можливо. А завдяки новітнім камерам з можливістю глибинного зчитування використати зображення для підробки також стає не можливим.

2.2 Етапи розпізнавання обличь

Вважається що мозок запам’ятовує найважливіші деталі, такі як форма та колір очей, форма носу, чола, щік та щелепи. Навіть більше, людський мозок

може впоратися зі значними коливаннями в освітленні, міміці, а також обличчях, що спостерігаються здалеку.

На жаль для комп'ютера мінливість зовнішнього вигляду обличчя впливає на його здатність до розпізнавання. Наприклад, зміни освітленості, інший вираз обличчя, поза, додаткові атрибути такі як окуляри або борода, можуть мати величезний вплив на швидкість розпізнавання. Враховуючи це машинне розпізнавання було поділено на три етапи [12]. Перший етап – виділення обличчя, другий – виділення частин обличчя та третій етап - їх порівняння.

2.2.1 Етап виділення обличчя на фотографії

Завдання виявлення особи на зображенні є першим кроком в процесі рішення задачі розпізнавання обличь.

Існуючі алгоритми для виявлення осіб можна розділити на чотири категорії:

- розпізнавання за допомогою шаблонів, заданих розробником [13];
- емпіричний метод;
- метод характерних симетричних ознак;
- метод виявлення за зовнішніми ознаками, які навчаються системи.

Емпіричний підхід «базується на знаннях зверху-вниз» (knowledge based top-down methods) передбачає створення алгоритму, який реалізує набір правил, яким повинен відповідати фрагмент фотографії, для того щоб вважатися людським обличчям. Даний набір правил - це спроба формалізувати емпіричні знання про те, як виглядає обличчя на зображенні і чим керується людина для прийняття рішення: бачить він обличчя або ні [14].

Основні правила:

- центральна частина особи має однорідну яскравість і колір;
- у центральній і верхньої частин особи різна яскравість;
- лице містить ніс, рот і два симетрично розташованих очі, різко відрізняються за яскравістю щодо іншої частини особи.

Метод стискання зображення використовується для того, щоб згладити перешкоди і зменшити обчислювальні операції. На такому зображенні простіше виявити зону з рівномірним розподілом яскравості, а потім перевірити наявність різко відрізняються за яскравістю областей всередині [15].

Метод побудови гістограм будує горизонтальну і вертикальну гістограми. А в областях-кандидатах відбувається пошук рис обличчя. Такий підхід використовувався в самому початку розвитку комп'ютерного зору через те, що він не був вимогливим до обчислювальної потужності процесора. Методи, розглянуті вище, мають непогані показники по виявленню осіб на зображенні з нескладним однорідним фоном і легкі в реалізації. Пізніше було розроблено безліч схожих алгоритмів. Але всі ці методи абсолютно непридатні для обробки зображень, з великою кількістю осіб або зі складним фоном. Також дані методи дуже чутливі до повороту і нахилу голови.

Методи характерних симетричних ознак, що базуються на знаннях знизу-вгору (Feature invariant approaches) є другим сімейством засобів для виявлення лиць. У цих методах проблема розглядається з іншого боку: немає спроби в явному вигляді формалізувати процеси, які відбуваються в людському мозку. Прихильники цього підходу намагаються виявити властивості і закономірності зображення особи неявно, знайти інваріантні особливості особи, незалежно від положення або кута нахилу.

Основні етапи алгоритмів цієї групи методів:

- виявлення на зображеннях явних ознак особи: рота, носа, очей;
- виявлення кордону, форми, кольору, текстури, яскравості лиця;
- об'єднання всіх знайдених ознак, потім їх верифікація.

Метод виявлення обличь в складних сценах це пошук правильного геометричного розташування рис обличчя при великій кількості поміх. Для цих цілей краще використовувати Гауссовский фільтр з безліччю різних орієнтацій і масштабів. Після цього виконується пошук відповідності знайдених рис і їх взаємного положення випадковим перебором.

Суть методу групування ознак у використанні другої похідної Гауссовского фільтра для того, щоб знайти важливі області зображення. Потім використовуючи пороговий фільтра окреслюються грані навколо кожної такої області. Після цього застосовується оцінка за допомогою байєсівської мережі для комбінування виявлених ознак - таким чином виконується вибірка рис обличчя.

Методи з цієї групи мають можливість розпізнавати обличчя в різних положеннях. Але при невеликому перекритті особи іншими об'єктами, засвітлені або виникненні шумів відсоток розпізнавання різко падає. Значний вплив має складний фон зображення. Основа розглянутих підходів - Емпірика. Вона є одночасно і сильною, і слабкою стороною. Велика мінливість об'єкта розпізнавання, залежність від умов зйомки та освітлення дозволяють віднести детектування осіб на зображеннях до завдань високої складності. Використання емпіричних правил дозволяє побудувати певну модель зображення особи і звести цю задачу до виконання кількох відносно простих перевірок. Але незважаючи на це спроби імітувати людський зір, методи з першої категорії поки дуже далекі по ефективності від свого прообразу, тому що дослідники, які обрали цей шлях, стикаються з великою кількістю труднощів. По-перше, процеси, які відбуваються в людському мозку під час розпізнавання образів, досить погано вивчені, і набір емпіричних знань про обличчя людини, доступних дослідникам на свідомому рівні, не вичерпує інструментарій, який використовує мозок підсвідомо. По-друге, досить важко ефективно перевести неформальний людський досвід і знання в набір формальних правил, тому що жорсткі рамки правил приведуть до того, що в деяких випадках особи не будуть виявлені, і, навпаки, а надто загальні правила приведуть до великої кількості випадків помилкового виявлення.

Розпізнавання за допомогою шаблонів, заданих розробником (Template Matching Methods). Шаблони задають якийсь стандартний образ зображення особи, наприклад, за допомогою опису властивостей окремих частин обличчя і

їх можливого взаємного положення. Пошук особи за допомогою шаблону складається в перевірці кожної області зображення на відповідність заданим шаблоном.

Особливості даного підходу:

- два види шаблонів;
- шаблони запрограмовані заздалегідь;
- для знаходження особи на зображенні використовується кореляція.

Метод виявлення особи за допомогою тривимірних форм використовує шаблон у вигляді пар відносин кольору шкіри в двох областях. Для виявлення особи необхідно пройти все зображення на порівняння із заданим шаблоном. Робити це треба з різним масштабом.

Моделі розподілу опорних точок є статистичними моделями, які представляють об'єкти, форма яких може змінитися. Корисна особливість методу - це здатність виділити форму змінних об'єктів в межах навчального набору з невеликою кількістю параметрів форми. Дана точна і компактна параметризація може бути використана для розробки ефективних систем класифікації [16].

Перевагами розпізнавання за допомогою шаблонів є відносна простота реалізації і хороші результати на зображеннях з не дуже складним фоном. Головний недолік - це необхідність калібрування шаблону поблизу із зображенням обличчя. А велика трудомісткість обчислення шаблонів для різних ракурсів і поворотів особи ставлять під сумнів доцільність їх використання.

Методи виявлення особи за зовнішніми ознаками (методи при яких необхідно провести етап навчання системи, шляхом обробки тестових зображень). Зображенню або фрагменту зображення ставиться у відповідність певний обчислений вектор ознак, що використовується для класифікації зображення на два класи - особа / не особа. Зазвичай пошук особи на зображенні за допомогою методів, які засновані на побудові математичної моделі зображення особи, полягає в тому, щоб перебрати всі прямокутні фрагменти

зображення всіх розмірів і перевірити кожен фрагмент на наявність особи. Але через те, що схема повного перебору має такі недоліки, як надмірність і велика обчислювальна складність, автори застосовують різноманітні методи зменшення кількості розглянутих фрагментів.

Головні принципи методів:

- Схоластика. Тобто кожне зображення сканується і представляється якимись векторами цінності.
- Блокова структура. Зображення розбивається на пересічні або непересічні ділянки різних масштабів і проводиться оцінка за допомогою алгоритмів оцінки ваг векторів.

Для того, щоб навчити алгоритми потрібно набір вручну підготовлених зображень з особами та без осіб.

Варто також відзначити, що найважливіше завдання - це виділити сильні класифікатори, так як вони будуть найбільш пріоритетними для перевірки виявлених ознак на зображенні. Кількість слабших класифікаторів варто зменшувати за рахунок їх схожості один на одного, а також видалення класифікаторів, які виникли за рахунок шумових викидів.

Основні методики виконання даних завдань:

- Штучні нейронні мережі;
- Метод головних компонент;
- Метод факторного аналізу;
- Лінійний дискримінантний аналіз;
- Метод опорних векторів;
- Наївний Байєсівський класифікатор;
- Приховані Марковские моделі;
- Метод розподілу;
- Розріджена мережа вікон;
- Активні моделі;
- Метод Віоли-Джонса та ін. [17]

Розглянемо особливості деяких з них.

Сьогодні метод штучних нейронних мереж є найпоширенішим способом для вирішення завдань розпізнавання осіб. Штучна нейронна мережа - це математична модель, яка являє собою систему з'єднаних і взаємодіючих між собою нейронів. Нейронні мережі не програмуються в звичному сенсі цього слова, вони навчаються. Технічно навчання полягає в знаходженні коефіцієнтів зав’язків (синапсів) між нейронами.

Метод опорних векторів застосовується для того, щоб зменшити розмірність простору ознак, не наводячи при цьому до істотної втрати інформативності навчального набору об'єктів. Застосування методу головних компонент до набору векторів лінійного простору, дозволяє перейти до такого базису простору, що дисперсія набору буде спрямована вздовж кількох перших осей базису, які називаються головними осями. Натягнуте на отримані таким чином головні осі підпростір є оптимальним серед всіх просторів в тому сенсі, що найкращим чином описує навчальний набір. Це набір алгоритмів схожий на алгоритми виду «навчання з учителем», які використовуються для класифікації та регресійного аналізу. Цей метод належить до сімейства лінійних класифікаторів. В основі методу опорних векторів лежить лінійне поділ класів.

Сьогодні найперспективнішим в плані високої продуктивності, малої частоти помилкових спрацьовувань і високим відсотком вірних знаходжень обличь є метод Віоли-Джонса.

Головні принципи, на яких базується метод:

- зображення використовуються в інтегральному уявленні, це дозволяє швидко знайти обличчя;
- використовуються ознаки Хаара, за допомогою цих ознак відбувається пошук особи і його характеристик;
- використовується прискорення для вибору найбільш підходящих ознак для шуканого об'єкта на зображенні;
- використовується класифікатор, який дає відповідь: обличчя / не обличчя;

- використовуються каскади ознак Хаара для швидкого відкидання областей, де особа не знайдено.

Класифікатори навчаються дуже повільно, але обличчя виявляються дуже швидко. Алгоритм демонструє хорошу роботу, якщо шуканий об'єкт знаходиться на зображенні під невеликим кутом, приблизно до 30 градусів. При більшому куті нахилу відсоток ідентифікації набагато нижче. На жаль, це не дозволяє в стандартній реалізації виявляти повернене обличчя людини під кутом більше 30 градусів, що в значній мірі ускладнює або робить неможливим використання даного алгоритму в сучасних системах виявлення осіб.

Завдання виявлення обличчя людини на цифровому зображенні виглядає наступним чином. Є зображення, на якому є особа. Воно представлено двовимірної матрицею пікселів, в якій кожен піксель має значення від 0 до 255 включно, якщо зображення є чорно-білим, від 0 до 255^3, якщо зображення кольорове. Алгоритм повинен визначити обличчя і помітити їх - пошук здійснюється в активній області зображення прямокутними ознаками, за допомогою яких і описується знайдене обличчя. Простіше кажучи, використовується підхід на основі області сканування. Зображення сканується зоною пошуку, а потім до кожного положення застосовується класифікатор.

Для того, щоб проводити будь-які дії з даними, використовується інтегральне представлення зображень в методі Віоли-Джонса. Інтегральне уявлення дозволяє швидко розрахувати сумарну яскравість довільної прямокутної області на зображенні, причому будь-якого розміру дана область була, час розрахунку статичний.

Інтегральне представлення зображення - це матриця, що збігається за розмірами з вихідним зображенням. У кожному її елементі зберігається сума яскравості всіх пікселів, які знаходяться вище і лівіше даного елемента. У стандартному методі Віоли - Джонса використовуються прямокутні ознаки, які називаються Хароподобнимі вейвлетами. Для їх обчислення використовується

поняття інтегрального зображення, яке було розглянуто вище. Ознаки Хаара дають точкове значення перепаду яскравості по осі X і Y відповідно.

Алгоритм сканування вікна з ознаками виглядає наступним чином [18]. Є досліджуване зображення, вікно сканування і ознаки що обрані для пошуку. Вікно сканування починає послідовно пересуватися по зображенню з кроком в 1 діапазон вікна. Сканування проводиться послідовно для різних масштабів, причому масштабується не саме зображення, а скануюче вікно. Всі знайдені ознаки потрапляють до класифікатору, який вирішує - знайдено обличчя чи ні.

Обчислювати всі ознаки на персональних малопотужних комп'ютерах просто нереально. Тому класифікатор повинен реагувати тільки на потрібну підмножину ознак. Отже, класифікатор потрібно навчити знаходженню осіб за певною множиною. Це можна зробити завдяки навчанню обчислювальної машини автоматично.

В контексті алгоритму, є безліч зображень, розділених на класи. Задано кілька зображень, для яких відомо, до якого класу вони відносяться, наприклад, клас «фронтальне положення носа». Ці кілька зображень - навчальна вибірка. Класова приналежність інших зображень не відома. Потрібно побудувати алгоритм, здатний класифікувати довільний об'єкт з початкової множини. Для вирішення цієї проблеми існує технологія прискорення (бустінг). Бустінг - це комплекс методів, які сприяють підвищенню точності аналітичних моделей. Модель, яка допускає невелику кількість помилок класифікації, називається «сильної». «Слабка» ж не дозволяє надійно класифікувати і робить в роботі багато помилок.

Алгоритм прискорення для пошуку обличь:

- Визначення слабких класифікаторів з прямокутним ознаками;
- Для кожного переміщення скануючого вікна обчислюється прямокутний ознака на кожному прикладі;
- Вибирається найкращий поріг для кожної ознаки;
- Відбираються кращі ознаки і кращий поріг;

- Переважується вибірка.

Каскадна модель сильних класифікаторів - це дерево прийняття рішень, в якому кожен вузол побудований таким чином, щоб виявляти всі цікаві образи і відхиляти регіони, які не є образами. Вузли дерева розміщені таким чином, що чим вузол ближче до кореня дерева, тим з меншої кількості примітивів він складається і, отже, вимагає менше часу на прийняття рішення. Цей вид каскадної моделі ідеально підходить для обробки зображень, на яких кількість шуканих образів не велика. В даному випадку метод може швидше вирішити, що даний регіон не містить образ, і перейти до наступного.

У тому випадку, якщо на вхід системи подається кольорове зображення, то можна в значній мірі збільшити швидкість роботи алгоритму, якщо попередньо обробити зображення за допомогою колірного кодування. Кольорове кодування також допомагає скоротити число помилкових спрацьовувань.

Сьогодні алгоритм Віоли-Джонса є найпопулярнішим завдяки високій точності спрацьовування і високій швидкості роботи.

2.2.2 Нормалізація обличчя

Після того, як обличчя буде знайдено на картинці (будуть отримані координати верхнього лівого кута, довжина і ширина прямокутника з особою), необхідно піддати зображення попередній обробці. З метою зниження рівня шуму можна використовувати різні фільтри (медіанний, гауссовский і ін.) [19]. Крім того, необхідно провести процедуру нормалізації зображення, тобто обрізати, масштабувати і повернути до горизонтального положення лінії, що з'єднує центри очей. Хоча в цій роботі теоретичного матеріалу про попередній обробці приділено мало уваги, слід зазначити, що якість роботи системи істотно залежить від попередньої обробки вхідних зображень. В ході виконання роботи було відзначено, що відсутність етапу фільтрації призводить до зниження ймовірності правильної верифікації.

2.2.3 Етап виділення рис обличчя та їх порівняння

Наступним кроком є обчислення рис і порівняння їх сукупностей між собою. Нижче представлено опис найпопулярніших алгоритмів.

Метод гнучкого порівняння на графах (Elastic graph matching). [20]

Суть методу полягає в тому, щоб зіставити еластичні графи, що описують риси обличчя. Обличчя подаються у вигляді графів зі зваженими ребрами і вершинами. На етапі розпізнавання еталонний граф залишається незмінним, а інший піддається деформації з метою найкращої підгонки до еталонного. У системах розпізнавання, заснованих на цьому методі, графи можуть являти собою прямокутну решітку або структуру, утворену антропометричними точками особи.

На вершинах графа обчислюються значення ознак, зазвичай за допомогою комплексних значень фільтрів Габора, шо вираховує в певній локальній області вершини графа за допомогою згортки значень яскравості пікселів з Габоровскімі фільтрами [21].

Ребра графа зважуються відстанями між суміжними вершинами. Відстань між двома графами обчислюється за допомогою деякої цінової функції деформації, яка враховує різницю між значеннями ознак, обчисленими в вершинах, і ступінь деформації ребер графа.

Граф деформується шляхом зміщення кожної його вершини на деяку відстань в певних напрямках щодо його початкового положення і вибору позиції вершини, при якій різниця між значеннями ознак у вершинах деформованого графа і відповідних вершинах еталонного графа буде мінімальним. Дана операція виконується для кожної з вершин графа до тих пір, поки не буде досягнуто найменше сумарне відмінність між ознаками еталонного і деформується графів. Значення цінової функції деформації при такому положенні, що деформується графа - це міра відмінності між еталонним графом і вхідним зображенням обличчя. Ця процедура деформації повинна виконуватися для всіх еталонних обличь що присутні в базі даних системи. В результаті

роботи даної системи розпізнавання ми отримаємо еталон з найкращим значенням цінової функції деформації.

У деяких джерелах вказується 95-97% -ва ефективність розпізнавання навіть при різній міміці на фотографіях і повороті особи до 15 градусів. Однак розробники подібних систем заявляють про те, що для роботи системи потрібні великі обчислювальні потужності.

Нейронні мережі.

У наші дні існує близько десятка різновидів нейронних мереж. Найпопулярнішою різновидом бути мережа, в основі якої лежить багатошаровий перцептрон. Вона дозволяє класифікувати вхідне зображення відповідно до попереднього її навчанням.

Нейронні мережі навчаються на наборі навчальних прикладів. Суть навчання зводиться до того, щоб налаштувати ваги міжнейронних зав’язків в процесі рішення задачі оптимізації з використанням методу градієнтного спуску. В процесі навчання нейронної мережі відбувається автоматичний витяг, визначення важливості і побудова взаємозв'язків між ключовими ознаками. Передбачається, що навчена нейронна мережа зможе застосувати отриманий під час навчання досвід на невідомі образи за рахунок здібностей до узагальнення.

Найкращі результати в розпізнаванні обличь продемонструвала Convolutional Neural Network або згорткова нейронна мережа, яка є логічним розвитком архітектури когнітрону і неокогнітрона. Успіх був досягнутий за рахунок обліку двовимірне зображення, на відміну від багатошарового перцептрона.

Згорткова нейронна мережа відрізняють від інших локальних рецепторів поля, які забезпечують двовимірну зв'язність нейронів, загальні ваги що забезпечує виявлення деяких рис в будь-якому місці зображення та ієрархічну організацію з так званим просторовим семплінгом. Завдяки даним нововведенням згорткова нейронна мережа забезпечує деяку стійкість до масштабування, зміні ракурсу, поворотам, зміщення і деяким іншим спотворень.

Тестування даної нейронної мережі на базі даних ORL (містить зображення осіб з невеликими змінами масштабу, освітлення, просторовими поворотами, емоціями) показало 96% -ву точність розпізнавання.

Згорткові нейронні мережі стали популярними завдяки розробці DeepFace, яку пізніше придбав Facebook, інформація про особливості архітектури не розголошується.

Недоліком нейронних мереж в першу чергу є їх швидкість навчання. Наприклад, додавання нового еталонного особи в БД зажадає повного перенавчання мережі на всьому наборі. Дана процедура, в залежності від обсягу вибірки, може зайняти від 1 години аж до декількох днів. Також існує кілька проблем математичного характеру, які пов'язані з навчанням. Наприклад, вибір оптимального кроку оптимізації, потрапляння в локальний оптимум, перенавчання, важко формалізується етап вибору архітектури мережі (характер зав’язків, кількість шарів, нейронів) і т.д. Беручи до уваги все вищесказане, можна зробити висновок, що нейронна мережа - це «чорний ящик» результатами роботи, важкими в інтерпретації.

Висновки до розділу

У другому розділі було обґрунтовано використання нейромережі як засобу для аналізу зображень. Етап порівняння обличь було розділено на три кроки та розглянуто теоретичну частину кожного з них.

РОЗДІЛ 3. ПОБУДОВА СХЕМИ КОНТРОЛЮ ДОСТУПУ ВИКОРИСТОВУЮЧИ НЕЙРОМЕРЕЖУ ДЛЯ ІДЕНТИФІКАЦІЇ

3.1 Архітектура системи контролю доступу за допомогою нейромережі

Основне завдання системи відеоспостереження - отримання, запис і відтворення візуальної інформації про поточні події на об'єкті, що охороняється. Пристрої, представлені сьогодні на ринку обладнання для систем безпеки, дають можливість спроектувати систему відеоспостереження з хорошими технічними характеристиками, надійну і зручну в експлуатації.

Більшість систем відеоспостереження будується на базі локальної мережі. Це пов'язано з тим, що такий підхід відносно простий і звичний, перш за все, для користувача: управління елементами системи здійснюється через ПК, підключений до мережі. Проте як і раніше поширений «класичний» варіант реалізації на базі багатоканальних відеореєстраторів зображений на рис. 3.1.

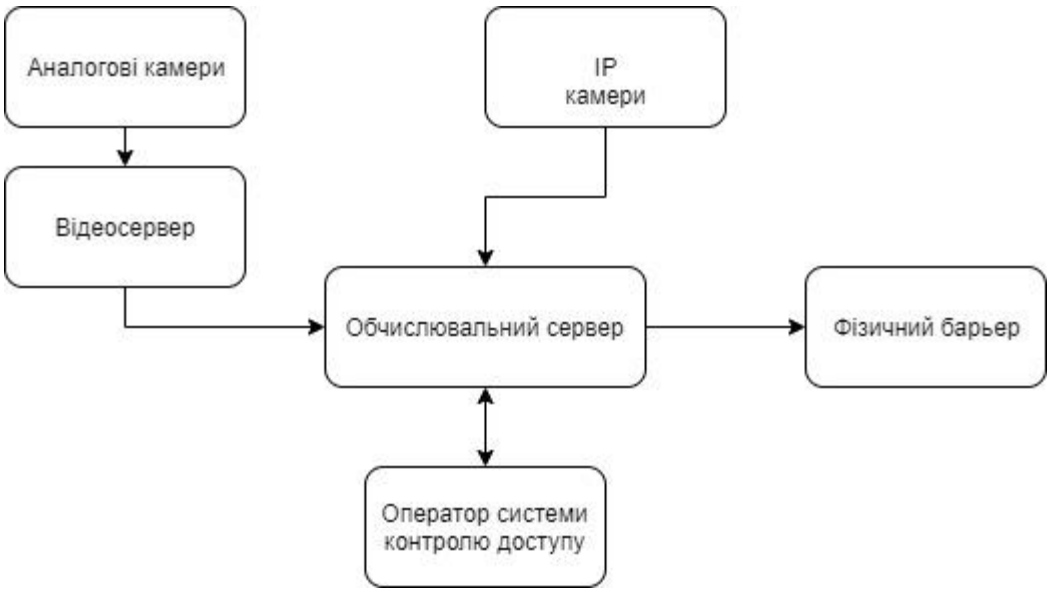

Рисунок 3.1 – Класична архітектура системи контролю доступу

3.2 Фізичне обладнання системи контролю доступу

Основний елемент системи відеоспостереження - це відеокамери. Відеокамери розрізняються і за основними параметрами, і за конструктивними особливостями, і за принципом обробки сигналу.

Таблиця 3.1 Види відеокамер

Категорія	Тип камери	Характеристики
Вихідний сигнал	Аналогова	На виході - аналоговий відеосигнал.
	Цифрова	На виході - цифровой відеосигнал.
	IP-камера	Цифровий сигнал (стиснутий в MPEG, JPEG, H-264 и т.д.), передається за допомогою TCP/IP.
Чутливий елемент	ПЗЗ матриця	Найрозповсюдженіший тип відеокамери.
	CMOS	Переваги перед ПЗЗ: мініатюрность, стабільність до засвічення. А також відносна мініатюрність відеокамери.
	Мікроболометр	Пристрій, чутливий в ІК-діапазоні. Використовується в камерах нічного бачення.
Кольоровість	Чорно-біла	Використовується якщо інформація про колір не грає ролі.
	Кольорова	В світлий час доби може бути використана, в нічний час доби працює погано.

Продовження таблиці 3.1

	«День-ніч»	Для цілодобового нагляду
	Інфочервона (з ПЗЗ чи мікроболометром)	Для відеоспостереження в умовах обмеженої видимості (чагарник, огорожі) або вночі..
Кінематика	Стаціонарна	Фіксована область огляду.
	Керована поворотна	Віддалене управління напрямком огляду. Швидкість обертання купольних камер - до 500 град. / С.
	Панорамна	За рахунок об'єктива «риб'яче око» камера постійно «бачить» весь навколишній простір. Надійніше поворотною і купольної за рахунок відсутності рухомих деталей.
	Гіростабілізована	Використовуються на транспорті для отримання стабільного зображення.

Призначення об’єктиву камер – проектування світловий потоку на чутливий елемент камери. Розрізняють об'єктиви з статичною фокусною дистанцією, варіфокальні (фокусну відстань можна налаштувати вручну), трансфокатори (фокусна відстань змінюється дистанційно). Багатокорпусні відеокамери поставляються в комплекті з об'єктивом. Часто об'єктив являє собою конструктивну складову камери. Наприклад, швидкісна купольна камера є інтегрованим пристроєм, до складу якого входить трансфокатор. У панорамних камерах об'єктив «риб'яче око» також є невід'ємною частиною.

На монітор системи відеоспостереження можна виводити зображення з однієї або декількох камер. Тому монітор повинен підтримувати багатоекранний

режим виведення відео; бажана підтримка режиму «картинка в картинці», що дозволяє негайно виводити відео з тривожного каналу. Залежно від того, де буде встановлено монітор, до його технічних характеристик (яскравості, контрастності, куту огляду) ставляться специфічні вимоги. Монітори, на які постійно виводиться рухома картинка, повинні володіти малим часом відгуку пікселя.

Мережеве і комутаційного обладнання - крім мережевого обладнання (маршрутизаторів, комутаторів, концентраторів) при побудові систем відеоспостереження використовуються спеціальні комутаційні пристрої, орієнтовані на підключення аналогових відеокамер:

- Мультиплексори - для послідовного або одночасного виведення декількох каналів відео,
- Квадратори – 4х-канальні мультиплексори
- Матричні комутатори - для виведення будь-якого з відеоканалів на будь-який з моніторів,
- Відеосервери - для перетворення, стиснення і передачі по IP-мережі аналогового відеосигналу

Додатково обладнання - якщо необхідно розширити можливості системи відеоспостереження або адаптувати існуюче обладнання до нових умов роботи, використовують додаткові пристрої:

- кожухи і кронштейни розширюють можливості монтажу камер. кронштейни бувають фіксованими і керованими поворотними (PTZ). Кожухи, крім фіксації камери в певному положенні, забезпечують також її захист від зовнішніх умов. Існують звичайні, погодозахищені (з підігрівом) або пило- та вологозахищені (IP-66/67) кожухи.
- ІК-підсвічування використовується спільно з камерами чутливими в ІК-діапазоні, для відеоспостереження в темний час доби і при недостатній освітленості.

- датчики і апаратні детектори руху підключаються до тривожних входів відеокамери і дозволяють включати запис або здійснювати поворот відеокамери в певне положення.
- зовнішні мікрофони використовуються спільно з відеокамерами для включення відео за рівнем звуку або для використання відеокамери за аналогією з відеодомофоном.

3.3 Розробка нейронної мережі

В якості нейронної моделі було вибрано VGG-Face 2. Це модель згорткової нейронної мережі запропонована K. Simonyan та A. Zisserman із Оксфордського університету в статті “Very Deep Convolutional Networks for Large-Scale Image Recognition” [22]. Модель має середню точність в 92.7% — цей показник попадає в топ-5 [23] при тестуванні на ImageNet в задаче розпізнавання обличь на зображенні. Ця нейронна модель була навчена більш ніж 3 мільйонами зображень що належать до більш ніж 9 тисячам людей.

В рамках цієї роботи було проведено декілька тестів для пошуку способів пришвидшення та підвищення якості розпізнавання. Один з тестів базувався на статті “Deep face recognition using imperfect facial data”. В ній автор запропонував провести порівняльний аналіз між двома методами класифікації зображень кожен з яких був попередньо навчений набором обличь з або без додаткового набору лише рис. Важливість цього тесту в рамках цієї роботи полягає в тому що на підприємствах досягти ідеального середовища для сканування обличчя майже не можливо. В залежності від специфіки організації працівники на ній можуть носити каски або окуляри, які будуть перекривати частину лиця, в такому випадку сканер має базуватись лише на певній його частині [24].

Для підтвердження цієї теорії було проведено додатковий тест використовуючи VGG-Face 2, а результати відображені в таблиці 3.2.

Таблиця 3.2 Результати розпізнавання обличь з додатковим навчанням

Частина лиця	Без додаткового навчання	З додатковим навчанням
Права щока	1%	14%
Рот	1%	12%
Лоб	1%	35%
Ніс	2%	13%
Очі	25%	64%
Очі та ніс	39%	90%
Лице без очей та без носа	28%	98%
Права частина	99%	99%
Нижня половина	58%	99%
Верхня половина	99%	100%
¾ лиця	100%	100%
Повне зображення обличчя	100%	100%

Як бачимо цей підхід навіть дозволив підвищити відсоток розпізнавання в декілька разів що дуже важливо при використанні системи в польових умовах.

Окрім того ще одне нововведення буде стосуватись процесу навчання. В багатьох існуючих системах використовується набір зображень працівника для подальшої ідентифікації. Ефективність цього методу різко знижує рівень розпізнавання якщо кут повороту обличчя доволі різкий. Для того аби подолати цю проблему потрібно виконувати навчання за зразком відео. Алгоритм цього навчання такий:

- працівник виконує рухи голови перед камерою в різні сторони
- відеопотік розділяється на кадри на передається серверу обробки [25]
- сервер оброки на кожному кадрі знаходить обличчя
- після виділення рис та отриманні моделі цього обличчя інформація зберігається під ідентифікатором користувача

  Переваги такого навчання очевидні – якість розпізнавання росте а алгоритм навчання мережі по відео в майбутньому буде використовуватись й надалі. Прикладом цього є випадок коли нейронна мережа не розпізнала вже існуючу в базі людину. В такому випадку використовуючи наявний відрізок відео можна покращити якість розпізнавання шляхом додаткового навчання.

3.4 Розробка програмного модуля

Програмна підсистема має забезпечити функціонування згідно з діаграмами варіантів використання системи контролю та управління доступом до об'єктів. В рамках розробки програмному модуля бути виконано роботу було виконано розробку структури бази даних, розробку web-інтерфейсу, розробку алгоритму обробки вхідного відеосигналу.

З даною системою можуть працювати оператор і користувачі. Для кожного з них надаються свої права в системі.

Користувачеві (співробітнику підприємства) доступні дві дії - ідентифікація (процес пізнання суб'єкта по властивому йому або наданим йому ідентифікаційним ознакою) і автентифікація (процес пізнання суб'єкта шляхом порівняння введених ідентифікаційних даних з еталоном).

Всі користувачі, які володіють правом доступу до охоронюваного об'єкту, попередньо повинні пройти ідентифікацію, повинен бути створений ID-номер ідентифікує користувача. Потім, коли користувач хоче отримати доступ до об'єкту, що охороняється, він проходить автентифікацію шляхом зупинки перед

фізичним барьером над яким встановлена камера. Якщо обличчя людини присутнє в базі даних - користувач отримує доступ до об'єкту (на сервер відправляється повідомлення про санкціонованому доступі), в іншому випадку - в доступі буде відмовлено, і на сервер буде відправлено повідомлення про несанкціоновану спробі отримання доступу до об'єкта.

Оператор має доступ до налаштування і управління обладнанням, перегляду поточних подій системи, управління списком об'єктів доступу, перегляду архіву, а також отримання звітів (рисунок 3.2).

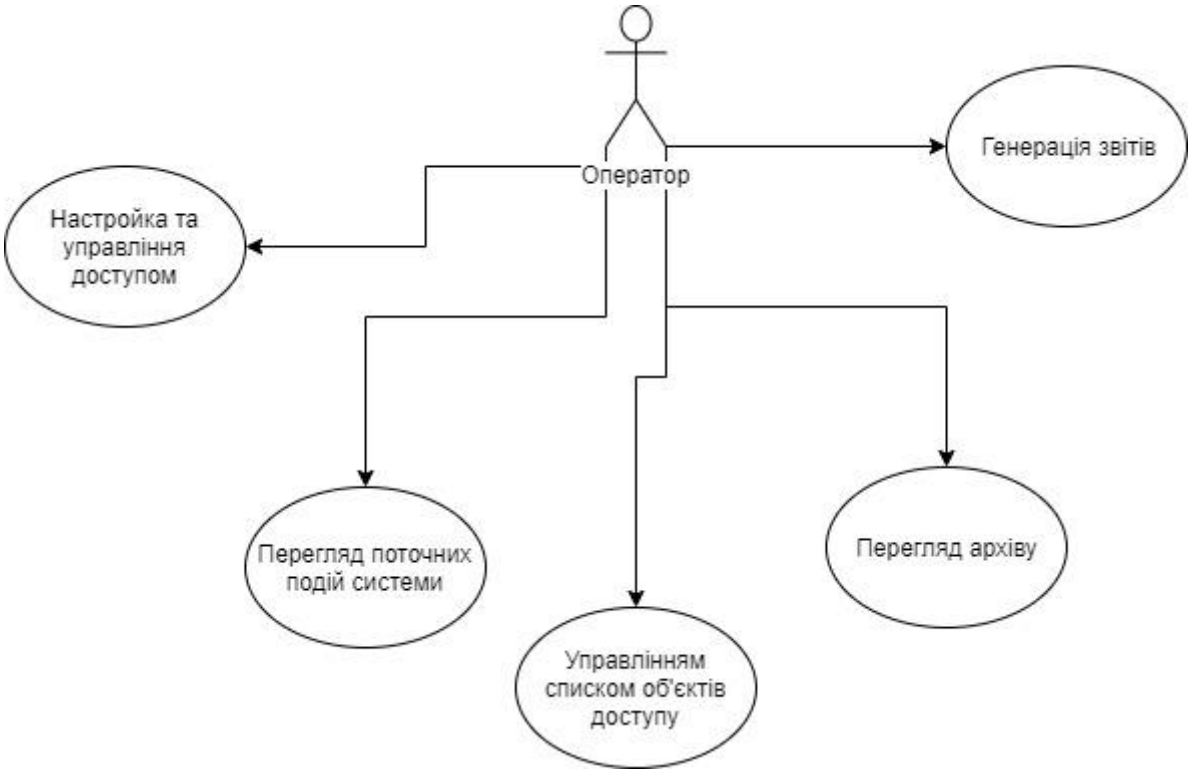

Рисунок 3.2 – Діаграма доступних дій оператора

Налагодження та управління обладнанням має на увазі під собою можливість оператора виконувати наступні дії:

- додавання нової точки доступу (ТД); точка доступу - це місце, де здійснюється контроль доступу;
- видалення існуючих ТД;

- оцінка якості зв'язку з мікро контролером;
- ручне управління точками доступу (можлива установка трьох режимів роботи - нормального, заблокованого і розблокованого);
- настройка ТД (установка IP-адреси);
- управління мікро контролером (отримання технічної інформації про МК, перегляд і реєстрація або видалення персоналу на обраної ТД).

Перегляд подій системи полягає в тому, що оператор може вибрати цікавлять його точки доступу (одну, кілька, або ж всі), налаштувати фільтр подій системи (наприклад, показувати тільки події по зареєстрованих спробах санкціонованого доступу в певний період часу) і отримати доступ до знайдених подій, що мали місце на даних точках доступу. Також, оператор може переглянути облікові картки користувачів.

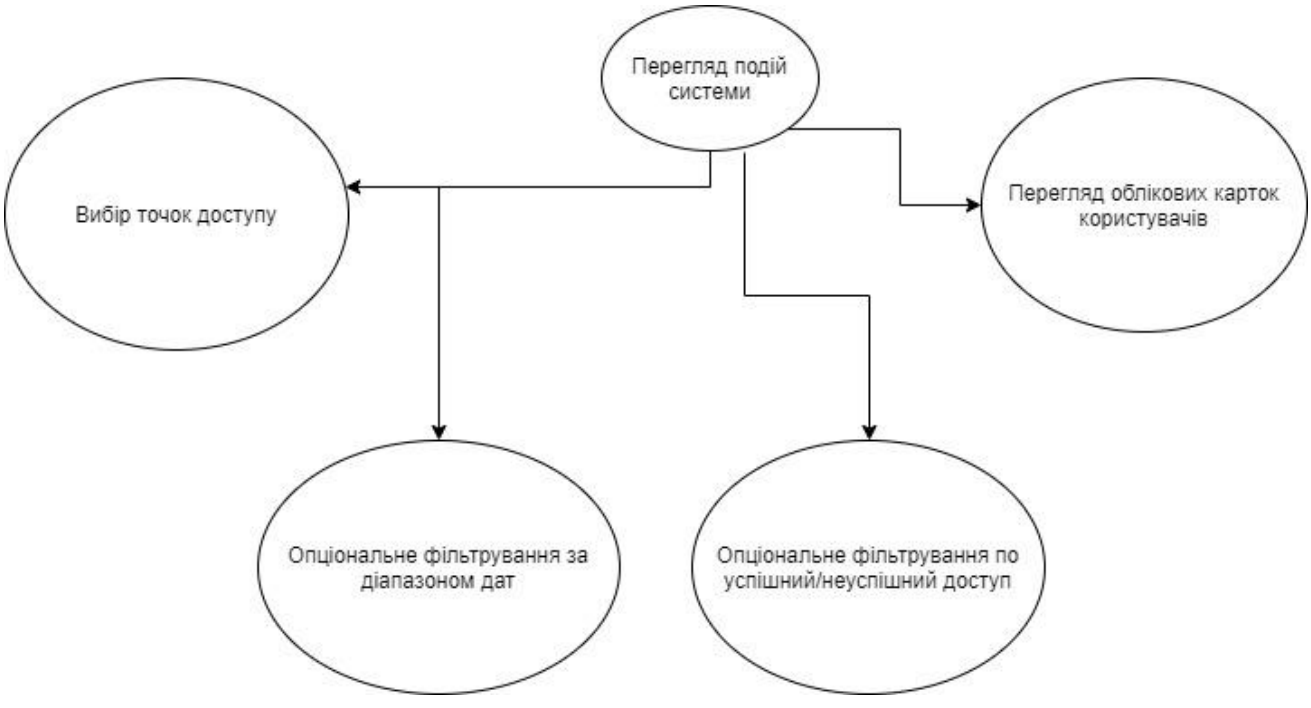

Рисунок 3.3 - Діаграма варіантів використання перегляду подій системи

Події системи - це облік успішних або невдалих спроб проходу через точку доступу, а також факти зміни (втрати або появи) зв'язку з контролерами.

Події доступу реєструються мікроконтролером автономно і незалежно від наявності зв'язку з сервером, час і дата події реєструються відповідно до вбудованим годинником реального часу.

Всі зареєстровані події зберігаються в незалежній пам'яті контролера і автоматично передаються на сервер СКУД при наявності зв'язку.

Таким чином, в базі даних сервера зберігаються всі події СКУД, за якими можна отримувати звіти за задані проміжки часу.

Система зберігає всю інформацію про зареєстрованих нею події, починаючи з моменту її першого запуску, без тимчасових обмежень. Кількість подій в системі - необмежено.

Управління списком об'єктів доступу полягає в тому, що оператор може додати або видалити відділ підприємства, і доступна можливість редагування даних облікових карток користувачів. Присутній також можливість пошуку за списком об'єктів доступу (користувачів системи).

Перегляд архіву полягає в тому, що оператор має доступ до архіву всіх подій системи. Присутня можливість використання фільтру подій (що відбулися проходи, проходи, санкціоновані оператором, заборонені проходи і зломи). Оператор також може переглянути інформацію про користувачів системи.

Отримання звітів це можливість відобразити інформацію з подій використовуючи певний шаблон попередньо налаштувавши потрібні параметри і обривши тип звіту. В результаті оператор отримає повний список подій що його цікавлять.

При виконанні будь-яких дій оператора фіксується комп'ютер, на якому проводилися ці дії, час, об'єкт над яким виконувалося дію, оператор їх виробляв. Таким чином, фіксуються всі зміни в таблицях баз даних, команди управління апаратурою, постановка і зняття з охорони, підтвердження тривоги і інші дії операторів.

Вибір СУБД для зберігання даних

Один з складних етапів в проектування програмного модулю є вибір системи управління базою даних. Обраний програмний продукт повинен задовольняти як поточним, так і майбутнім потребам, тобто мати можливість простого розширення обсягу даних. При цьому слід враховувати фінансові витрати на придбання необхідного обладнання, самої системи, розробку необхідного програмного забезпечення на її основі, а також навчання персоналу. Крім того, необхідно переконатися, що нова СУБД здатна принести реальні вигоди.

У таблиці 3.3 наведені основні переваги і недоліки трьох найбільш популярних open-source СУБД - PostgreSQL, MySQL і FirebirdSQL.

Таблиця 3.3 - Переваги і недоліки різних СУБД

СУБД	MySQL	PostgreSQL	FirebirdSQL
Переваги	- швидкодія; - безпека і надійність; - відсутність. високих вимог до апаратних ресурсів; - переносимість.	- підтримка БД практично необмеженого розміру; - потужні і надійні механізми транзакцій і реплікації; - успадкування; - легка розширюваність.	-багатошарова архітектура; - компактність (дистрибутив 5Mb); - висока ефективність та повна підтримка хранимих процедур та тригерів

Продовження таблиці 3.3

Недоліки	- відсутність транзакцій і тригерів; - відсутні збережені процедури і вкладені запити; - немає підтримки інструкції UNION; - відсутність каскадного оновлення даних.	- відносна складність інсталяції; - невірна робота оточення PostgreSQL; - відсутність Intellisense при програмуванні.	- відсутність кеша результатів запитів; - відсутність повнотекстових індексів.

З переліку вимог до СУБД можна виділити кілька груп критеріїв:

- особливості розробки додатків;
- можливість моделювання даних за допомогою діаграм;
- особливості архітектури і функціональні можливості;
- вимоги до робочого середовища;
- контроль роботи системи;
- продуктивність;
- надійність;

Бази даних мають свої особливості та відмінності. Але враховуючи що система контролю доступу потребує сховище яке дозволить швидко зберігати та зчитувати не великі об’єми - в якості СУБД для зберігання даних буде використовуватися СУБД MySQL..

Розробка класів-сутностей

При розробці системи, було прийнято рішення використовувати ORM. ORM (абревіатура від Object Relational Mapping- Об'єктно-реляційна проекція) - технологія програмування, яка зв'язує бази даних з концепціями об'єктно-

орієнтованих мов програмування, створюючи «віртуальну об'єктну базу даних». Суть проблеми, яка вирішується за допомогою ORM-шару, полягає в необхідності перетворення об'єктних структур в пам'яті програми в форму, зручну для збереження в реляційних базах даних, а також для розв'язання оберненої задачі - розгортання реляційної моделі в об'єктну, при цьому зберігаються властивості об'єктів і відносин між ними.

JPA - це технологія, що забезпечує об'єктно-реляційне відображення простих JAVA об'єктів і надає API для збереження, отримання та управління такими об'єктами.

JPA - це специфікація (документ, затверджений як стандарт, що описує всі аспекти технології), частина EJB3 специфікації.

Сам JPA не вміє ні зберігати, ні управляти об'єктами. JPA визначає інтерфейси, які повинні будуть бути реалізовані провайдерами. JPA визначає правила про те, як повинні описуватися метадані відображення і про те, як повинні працювати провайдери. Далі, кожен провайдер, реалізуючи JPA, визначає отримання, збереження і управління об'єктами. У кожного провайдера реалізація різна.

При виборі ORM не виникло особливих проблем, так як в проекті використовується синтаксис лише JPA, без доповнень унікальних функціональностей різних бібліотек ORM, тому була вибрана бібліотека «Hibernate». Варто відзначити, що можна підключити будь-яку іншу ORM бібліотеку, без внесення змін до класи-сутності. Було розроблено ряд сутностей, які розглянемо нижче.

«Рівень доступу» - Дану сутність буде створено для обмеження або ж дозволу доступу тому чи іншому співробітнику в різні приміщення.

«Група співробітників» - сутність служитиме для об'єднання співробітників з однаковими правами доступу в одне підмножина. Найчастіше персонал з одного і того ж відділу і з однієї і тієї ж посадою володіють

однаковим рівнем доступу, для об'єднання персоналу з одним і тим же рівнем доступу буде створена дана сутність.

«Користувач» - робочий персонал. Дана сутність зберігає персональні дані кожного працівника компанії, такі як П.І.Б., дата народження або посаду.

«Переходи» - сутність для контролю і зберігання всіх переходів персоналу з одного приміщення в інше. Містить інформацію про час входу в приміщенні, про місце від куди здійснений перехід. Якщо співробітник вперше за день увійшов в цю кімнату, то в поле «від куди» буде зберігатися 0. Таким чином, можна відстежити, куди в першу чергу ходив співробітник. Так само сутність зберігає дані про проведений час в тому чи іншому приміщенні.

«Кімната» - зберігає номер кімнати і необхідний рівень доступу, для здійснення позитивного переходу.

«Поверх» - служить для зберігання номера поверху і шляхи до SVG файлу (векторний малюнок), на якому зображений план приміщення поверху.

«Будівля» - сутність на випадок, якщо офіс розташований на території більш ніж 1-го будинку. Зберігає номер будівлі, адреса за яким воно розташоване і файл SVG, на якому розміщено схематичне зображення будівлі.

Алгоритми обліку доступу до приміщень

При розробці системи було реалізовано безліч алгоритмів, але не хотілося б зупинятися на всіх. Тому будуть розглянуті кілька алгоритмів основного призначення системи, а саме алгоритми обліку доступу в приміщення.

Спочатку розглянемо алгоритм обліку входу в приміщення. При здійсненні входу в приміщення, система створює об'єкт класу Transition (перехід) і в локальну змінну tempId заносяться дані з картки, а саме Id користувача, які зчитуються пристроєм читання. Далі відбувається ідентифікація користувача по обличчю та пошук відповідного в базі даних нейронної мережі. В випадку позитивного знаходження отримуємо його ID, якщо користувач не знайдений, то в поля класу Transition, «isAccessPermitted» заносяться дані булевого типу «false», а в поле «reason» - «nu» (No User), після чого відбувається

завершення методу і повернення false. В іншому випадку, тобто у разі якщо користувач з наявними ID присутній в системі відбувається запис в поля класу «toRoom» заносяться відповідні дані -Номер кімнати, в яку здійснюємо перехід, «timeIn»-час входження в кімнату. Після чого система перевіряє чи має право співробітник увійти в дане приміщення, якщо працівник не володіє таким правом, то система заносить в поля класу «isAccessPermitted» дані булевого типу «false», а в поле «reason» - «na» (No Access) і завершує метод з поверненням false. У разі позитивного результату перевірки система заносить дані в поля «isAccessPermitted» булевого типу «true», а в поле «reason» - «ok» (і завершує метод повертаючи true.

Другий алгоритм, який буде представлений нижче, забезпечує облік виходу з приміщення. При здійсненні виходу система здійснює пошук вже вчиненого входу в кімнату, необхідним співробітником. У разі повернення результату null методом пошуку, метод виходу завершується повертаючи false. В іншому випадку в поля об'єкта (об'єкт передається методом findTransition) знайденої транзакції заносяться дані, а саме в поле timeout заноситься час виходу а в поле «spendtime» вводиться число часу проведене в приміщенні.

Вибір вбудованої операційної системи (ОС) і мов програмування

На сьогоднішній день найбільш популярними вбудовуваними операційними системами є Embedded Linux і Windows Embedet compact.

Windows Embedded Compact 7 (відомої раніше як Windows Embedded CE 7.0) - сьома версія операційної системи реального часу Windows Embedded CE, що розвивається окремо від родини Windows NT, і орієнтованої на підприємства, що виготовляють промислові контролери і пристрої побутової електроніки. Windows Embedded Compact може працювати на різних мікропроцесорних архітектур і підтримує x86, SuperH і ARM.

Windows Embedded Compact 7- це компонентна, багатозадачна, багатопотокова, багатоплатформенна операційна система з підтримкою реального часу. Розробникам доступні близько 600 компонентів,

використовуючи які вони можуть створювати власні образи операційної системи, які включає тільки необхідний даному конкретному пристрою функціонал.

Windows CE надає розробникам додатків набір API, заснований на стандартному Win32 API і доповнений спеціалізованим API для вбудованих пристроїв. Оскільки CE підтримує тільки частина Win32 API і має певну специфіку, пов'язану зі вбудованої природою операційної системи, додатки, написані для настільних версій операційної системи Windows, можуть зажадати додаткової адаптації і модифікації для запуску їх на вбудованих пристроях; і в будь-якому випадку, для запуску програм на пристрої потрібно їх перекомпіляція.

Але так само, як і настільні версії Windows, Windows CE використовує стандартний формат файлу - Portable Executable (PE). Це дозволяє розробникам використовувати більшість стандартних утиліт, що працюють з форматом PE, наприклад Dependency Walker (перевірка залежностей) або DumpBin.

На базі Windows CE засновано безліч платформ, включаючи Handheld PC, Palm-size PC, Pocket PC, Windows Mobile, Meizu OS, а також безліч промислових пристроїв і вбудованих систем.

Під Embedded Linux маються на увазі різні варіанти ОС, в основі яких лежить ядро Linux, налаштовані для заданої апаратної платформи, а також вільне програмне забезпечення GNU: компілятор gcc, бібліотека GNU libc і інші програмні компоненти, що випускаються під одним з відкритих ліцензій. Embedded Linux активно використовується в проектах, пов'язаних з розробкою налагоджувальних плат і пакетів підтримки (BSP), програмно-апаратних комплексів на базі сучасних процесорів ARM, Blackfin, AVR32, MIPS, PowerPC.

Переваги Embedded Linux перед Windows CE:

- поширюється разом з вихідним кодом
- кроссплатформеність;
- велика кількість наборів розробника;

- безкоштовна;
- велике кількість матеріалів по використанню;
- використання ядра Linux дозволяє звільнитися від написання драйверів для різного роду периферії.

Як вбудованої ОС, в розроблюваної системі буде використовуватися Embedded Linux, виходячи з переваг Linux, але за бажанням можна використовувати і Windows, що ніяк не вплине на роботу системи загалом.

Для взаємодії програмного забезпечення з мікроконтролером будуть використовуватись існуючі бібліотеки та драйвера. Деякі мікроконтролери мають сервер з API у довільному форматі. Нажаль не завжди можна з'єднатись з мікроконтролером напряму, в такому випадку потрібно буде написати свій драйвер використовуючи мову низького рівня. Асемблер являє собою низькорівневий мову програмування. Він використовує напряму набір інструкцій мікроконтролера. Створення програми цією мовою потребує хорошого знання системи команд процесора. Крім того потрібно мати достатній часу на розробку програми. Асемблер програє Сі в швидкості і зручності саме розробки програм але має помітні переваги в розмірі кінцевого виконуваного коду, а відповідно, і швидкості його виконання.

Створення програми на Сі проходить з набагато більшим комфортом, надаючи розробнику всі переваги мови високого рівня. Компіляція вихідних текстів, написаних на Сі, здійснюється швидко і дає компактний, ефективний код.

Основні переваги Сі перед асемблером:

- підтримка обчислень з числами з плаваючою точкою.
- відносно висока швидкість розробки програми за допомогою існуючих IDE з підсвіткою коду та помилок;
- універсальність, яка не потребує досконального вивчення архітектури мікроконтролера;

- найкраща документовані і читаність алгоритму; наявність бібліотек функцій;

Можливості мови низького рівня гармонійно поєднуються з властивостями мови високого рівня. Можливість низькорівневого програмування дозволяє легко управляти апаратними засобами а властивості мови високого рівня дозволяють створювати легко підтримуваний програмний код. Крім того, практично всі компілятори Сі мають можливість використовувати асемблерні вставки для написання критичних за часом виконання і займаним ресурсів ділянок програми.

Проаналізувавши основні особливості мов програмування Сі та асемблера, вибір був зупинений на Сі.

Для розробки серверної частини було прийнято рішення використовувати мову високого рівня, а саме об'єктно-орієнтовану мову програмування. На розгляд було запропоновано дві мови програмування, що задовольняють умови (об'єктно-орієнтовані, з синтаксисом, успадкованим від С):

C# розроблено групою інженерів під керівництвом Андерса Хейлсберг в компанії Microsoft.

Java, розроблений компанією Sun Microsystems (в подальшому придбаної компанією Oracle). Програми Java зазвичай компілюються в спеціальний байт-код, тому вони можуть працювати на будь-який віртуальної Java-машині (JVM) незалежно від комп'ютерної архітектури.

Вирішено використовувати, як мова розробки серверної частини-Java, який, на відміну від C #, є мультиплатформним.

Для створення web-інтерфейсу буде використовуватися бібліотека Vaadin.

Vaadin - це платформа веб-додатків з відкритим вихідним кодом для створення повнофункціональних інтернет-додатків. На противагу бібліотекам JavaScript і рішенням на основі браузерів / модулів, в її склад входить архітектура на стороні сервера, що означає виконання більшої частини програмної логіки на серверах. Технологія AJAX використовується на стороні

браузера для забезпечення функціонально насиченого і інтерактивного інтерфейсу користувача. На стороні клієнта Vaadin будується на основі GWT і може бути розширена з її допомогою.

Основним елементом Vaadin є бібліотека Java, розрахована на спрощення створення і обслуговування високоякісних веб-інтерфейсів користувачів. Основна ідея сервероцентричной моделі програмування Vaadin полягає в тому, що вона дозволяє забути про мережі та програмувати інтерфейси користувачів точно так же, як ми програмуємо все настільні додатки Java, тобто за допомогою звичайних наборів засобів, таких як AWT, Swing або SWT - тільки ще простіше. Сервероцентрична модель програмування дозволяє Vaadin взяти на себе управління призначеним для користувача інтерфейсом в браузері і зв'язок AJAX між браузером і сервером. Підхід Vaadin дозволяє не витрачати сили на вивчення і налагодження технологій на стороні браузерів, таких як HTML або JavaScript.

Бібліотека Vaadin чітко відокремлює уявлення призначеного для користувача інтерфейсу від логіки і дозволяє розробляти їх окремо. Підхід Vaadin полягає у використанні тим, що визначають зовнішній вигляд додатків. Теми контролюють зовнішній вигляд інтерфейсів користувачів за допомогою шаблонів CSS і (при бажанні) HTML. Vaadin надає теми за замовчуванням, але при необхідності можна створювати свої власні. У серверної частини Vaadin використовується Google Web Toolkit (GWT) для візуалізації інтерфейсу користувача в браузері. Програми GWT пишуться на Java, але компілюються в JavaScript. GWT ідеально підходить для реалізації додаткових компонентів інтерфейсу користувача (або компонентів оформлення вікна, за термінологією GWT) і логіки взаємодії в браузері, тоді як Vaadin обробляє логіку самого додатка на сервері. Платформа Vaadin розроблена з розрахунком на розширюваність і дозволяє легко використовувати будь-які компоненти GWT від сторонніх виробників на додаток до компонентів, пропонованих в Vaadin.

Використання GWT також означає, хто весь необхідний код пишеться виключно на Java.

Можливості Vaadin:

Використання Java як єдиної мови програмування при створенні веб-додатків і веб-контенту - одна з найбільш значущих функцій в Vaadin. Фреймворкіс використовує модель і певні елементи призначеного для користувача інтерфейсу, віджети, що робить її дуже близькою до моделі розробки десктоп-додатків на Java з використанням HTML і Javascript

Організація моделі даних і віджетів дозволяє відображати в браузері великі обсяги даних без значної завантаження пам'яті і без додаткових дій з сторони розробника.

Використання Google Web Toolkit для відображення сторінок з результатами пошуку і обробки дій користувача (на зразок термінального клієнта). Так як Google Web Toolkit функціонує тільки на стороні клієнта, Vaadin додає додаткову затвердження даних на стороні сервера: це вирішує проблеми безпеки, пов'язані з можливістю підміни даних або коду Javascript. Відповідно, при зміні і пошкодженні даних, що надходять від браузера, сервер, визначивши це, не пропускає запити.

Можливість розширення стандартного набору віджетів Vaadin за рахунок інших віджетів, написаних для GWT, а також модифікації його за допомогою CSS. Однак стандартний додаток, що створюється на Vaadin, не вимагає програмування саме на GWT та подальшої компіляції GWT-компілятором, якщо тільки розробник не додає в проект нестандартні віджети.

Діаграма класів

Під час проектування системи були створені діаграми класів, для спрощення розуміння «логіки» системи. Розглянемо набір класів, за допомогою яких забезпечується обмін даними між системою і базою даних.

У верху перебувати інтерфейс IID, який розширюють все класи суті. Він створений для спрощення сприйняття коду програми. Для того що б не

представляти всі класи у вигляді AbstractClass <ClassName, ID>, за допомогою даного інтерфейсу, ми представляємо класи як AbstractClass <ClassName>. Розглянемо кожну сутність окремо. Клас «AccessLevel» існує для зберігання рівня доступу до того чи іншого об'єкту для кожної групи персоналу. Клас «GroupWorker» необхідний для об'єднання персоналу в якесь безліч, за різними принципами, для забезпечення прав доступу. «WorkBench» зберігає дані про те, в яких приміщеннях працювати той чи інший співробітник, на підприємстві. Це необхідно для того що б коректно підрахувати час проведений на робочому місці. На приклад, співробітник IT відділу має право відвідувати приміщення свого відділу, серверну, їдальню і кабінет відділу маркетингу, але в їдальні і в відділі маркетингу- він не проводить ніяких корисних робіт для підприємства, відповідно проведений час на цих місцях -не вважається за час проведений на роботі. У разі відсутності будь-якого з приміщень в даному списку- вказує на те що відповідна група користувачів не має права доступу до приміщення. Клас «RealSalary», зберігає інформацію про заробітну плату за місяць, з урахуванням лікарняних, штрафних або ж преміальних. Клас «MissByIll» для ведення обліку про лікарняних кожного співробітника, ця інформація необхідна, для коректного підрахунку заробітної плати, за місяць.

Клас «User» служити для зберігання и верифікації персональної інформації про співробітників підприємства. Використовуючи ці дані система приймає рішення щодо дозволу доступу в приміщення. Якщо співробітника з даними ID не існує в базі даних, то система заборонить доступ до будь-якому приміщенню. «Transition» необхідний для обліку інформації про переходах скоєних робочим персоналом. На основі цієї інформації будується список переходів певного співробітника, вираховується час проведений на робочому місці і розрахунок заробітної плати, а так само ґрунтуючись даною інформацією можна дізнатися де знаходитися працівник в даний момент.

Нижче подано діаграму класів бізнес логіки системи контролю та управління доступом. Клас «Index» виступає в ролі головної сторінки системи,

він створює об'єкт класу в якому започатковано всі необхідні компоненти розміщені на головній сторінці та проводиться розмітка сторінки. Так само клас «Index» відповідає за виклик всіх форм, усередині яких розміщена вся необхідна інформація для управління системою, на приклад форма «User» відображає список всіх користувачів з можливість фільтрувати список за різними критеріями. На формі «Stage» відображений план поверху, натиснувши на потрібну кімнату на плані приміщення відкривається список всіх співробітників знаходяться в цій кімнаті в даний момент. Так само можна знайти певного користувача на плані приміщення задавши його id або ж Прізвище та ініціали.

Клас «AbstractForm» містить всі узагальнені методи всіх класів форм, такі як додавання, видалення, заміна, які відкривають користувачеві компоненти полів для введення даних. Кожна з форм займається відображенням даних на екран, а так само їх додаванням, видаленням і заміною.

Так само на схемі присутній допоміжний клас. «SpringContextHelper»-цей клас забезпечує отримання даних з репозиторіїв до контролерів. Замість DAO класів використовується PagingAndSortingRepository - це інтерфейс бібліотеки spring-data, який входить до складу фреймворка «Spring». Використовуючи дану бібліотеку, не потрібно створювати абстрактну фабрику DAO і успадковувати усіма DAO класами узагальнені методи. Але для нормальної передачі інформації з бази даних, через репозиторії, до контролера, необхідно створити SpringContextHelper. Усередині цього класу необхідно створити конструктор всередині якого передати змінну яка визначає набір методів, які сервлет використовує для зв'язку з його контейнером сервлетів. В іншому випадку дані не виводитися не будуть.

У класі «Components» описана розмітка, яка буде використана для головної сторінки. Крім того в цьому класі будуть ініціалізуватись всі компоненти інтерфейсу головної сторінки.

Для підключення нейронної моделі GGV-Face 2 використаємо Python. Використання саме цієї мови програмування для роботи з нейронною мережею

обґрунтовано в статті «Understanding the math and how it works» [26]. Використовуючи веб фреймворк Flask ми отримуємо REST API з двома методами.

- Метод ідентифікація

  Вхідними параметрами цього методу буде зображення. Після завантаження відбудеться пошук обличь на зображення, в випадку знаходження декількох – кожен з них буде перевірено по базі наявних обличь.

  Вихідними параметрами є масив ід користувачів що були виявлені на фотографії та масив зображень обличь персон які не були ідентифіковані.

- Метод реєстрації в системі

  Цей метод дозволяє додати одне чи декілька зображень в систему для нового чи існуючого користувача. Аргументами цієї функції це ідентифікатор людини та масив фотографій, з яких в подальшому буде отримано зображення обличчя.

  Вихідними даними є відношення – ідентифікатор користувача до кількості зображень цього користувача в базі нейронної мережі.

3.5 Тестування нейронної мережі та верифікація результатів

Після реалізації програмного модулю можна почати тестування. Для цього ми будемо підміняти вхідних потік з камери зображеннями з наборів даних, призначених для тестування нейронних мереж з розпізнавання обличь. Попередньо проведемо навчання нейронної мережі чистиною цих зображень.

Для тестування використаємо три великих за обсягом наборів даних, або так званих датасетів.

База кольорових зображень FERET, США

Програма FERET мала на меті створити велику базу зображень обличь, зібрану незалежно від розробників алгоритму. Доктор Гаррі Векслер з

університету Джорджа Мейсона був обраний для керівництва колекцією цієї бази даних. Збір бази даних був виконаний спільними зусиллями доктора Векслером та доктора Філліпсом. Зображення збирали в напів-контрольованому середовищі. Для підтримки певної послідовності у всій базі даних використовували однакові фізичні настройки у кожному сеансі фотозйомки. Оскільки обладнання потрібно було збирати заново для кожного сеансу, деякі зображення були зібрані в різні дати. База даних FERET була зібрана за 15 сеансів у період з серпня 1993 р. До липня 1996 р. База даних містить 1564 набори зображень на загальну суму 14 126 зображень, що включає 1199 осіб та 365 дублікатів наборів зображень. Набір дублікатів - це другий набір зображень людини, які вже знаходяться в базі даних і зазвичай були зроблені в інший день. Для деяких осіб пройшло понад два роки між їх першим і останнім засіданнями, деякі теми були сфотографовані кілька разів. Цей проміжок часу був важливим, оскільки він дозволив дослідникам вперше вивчити зміни у зовнішньому вигляді суб'єкта, які відбуваються протягом року.

База даних індійських обличь

База даних містить набір зображень обличчя, зроблених у лютому 2002 року в кампусі IIT Kanpur. Є одинадцять різних зображень кожного з 40 різних предметів. Для деяких предметів включені додаткові фотографії. Усі зображення були зроблені на яскравому однорідному тлі з предметами у вертикальному положенні. Файли у форматі JPEG. Розмір кожного зображення - 640x480 пікселів, з 256 рівнями сірого на піксель. Зображення організовані у двох основних каталогах - чоловіки та жінки. У кожному з цих каталогів є під-каталоги з назвою у вигляді порядкових номерів, кожен відповідає одній особі. У кожному з цих каталогів є одинадцять різних зображень однієї особи, які мають назви форми abc.jpg, де abc - номер зображення для цього предмета. Обличчя мають різні орієнтації: погляд вперед, погляд вліво, погляд вправо, погляд вгору, поворот обличчя вліво, поворот обличчя вправо, поворот обличчя вниз. Також доступні різні емоції: нейтральна, посмішка, сміх, сум / огида.

База даних обличчя Гонконзького політехнічного університету в науково-дослідних розробках

Біометричний науково-дослідний центр Гонконзького політехнічного університету розробив пристрій запису обличчя NIR в реальному часі і використовував його для створення масштабної бази даних облич. Система захоплення обличчя NIR складається з камери, світлодіодного джерела світла, фільтра, картки захоплення кадру та комп'ютера. Використовувана камера - це камера чутлива до діапазону NIR. Активне джерело світла знаходиться в спектрі NIR між 780 нм - 1100 нм. Пікова довжина хвилі - 850 нм. Потужність загального світлодіодного підсвічування регулюється для забезпечення хорошої якості зображення NIR обличчя, коли обличчя камери становить 80 см до 120 см, що зручно для користувачів. Використовуючи описаний вище пристрій збору даних, ми зібрали зображення NIR обличчя 335 осіб. Під час запису предмету спочатку запропонували сісти перед камерою, і були зібрані нормальні зображення лобових облич. Потім суб'єкта було запропоновано висловити та поставити зміни, і відповідні зображення були зібрані. Для зйомки зображень на обличчі з варіаціями масштабування ми попросили випробовуваних рухатись поблизу або від камери в межах певного діапазону. Нарешті, для збору зображень осіб, що змінюються за часом, зразки з 15 суб'єктів були зібрані у два різні періоди з інтервалом більше двох місяців.

Таблиця 3.4 Результати тестування наборів даних

Набір даних	Відсоток вдалих розпізнавань
FERET, США	96%
IIT Kanpur	100%
База даних обличчя Гонконзького політехнічного університету в науково-дослідних розробках	91%

Найменший відсоток розпізнавання був отриманий з зображень з великим поворотом обличчя. В випадку відмови базу даних можна навчити фотографією яку він не розпізнав. Таким чином відсоток розпізнавання може бути піднятий до 100%. Окрім цього варто зазначити що у тестових наборах даних нейронну мережу навчали за допомогою зображень, в той же час, на підприємствах можна буде використовувати камери. Завдяки навчанню по відео нейронна мережа буде мати на вхід безліч кадрів гарної якості де кожен кут повороту буде представлений.

Висновки до розділу

В цьому розділі було розроблено архітектуру майбутнього рішення по контролю доступом на підприємстві, визначено технологія для розробки бекенд та фронтенд частини. Визначено фреймворк для роботи з базою даних та окреслено домену структуру.

Для зручної розробки системи було створено UML діаграми що описують певні бізнес процеси в системі.

Крім того в цьому розділі було проведено тестування за допомогою 3 наборів даних, кожен з яких мав свої специфічні особливості, і отримано результати які дозволяють підтвердити високу якість розпізнавання облич.

ВИСНОВКИ

В межах цією роботи було реалізовано базову версію системи контролю доступу на основі нейронної мережі. Основною задачею було вивчити підходи до оптимізації роботи нейронної мережі, провести підготовчі тести та вибрати найшвидшу з існуючих тренованих моделей.

В ході дослідження в якості програмної бази для розробки була обрана нейронна модель VGG-Face. Транзитивне навчання цієї моделі займе набагато менше часу, а точність розпізнавання з самого початку буде високою. Ще однією перевагою цієї моделі є тонко налаштовані шари нейронної мережі.

Під час проведення експериментів було виявлено, що на точність розпізнавання сильно впливають такі фактори: якість освітлення в приміщенні, роздільна здатність камери, чи була нейронна мережа навчена використовуючи окремі риси облич.

Також було з'ясовано, що серед алгоритмів для класифікації рис обличь найякіснішим є алгоритм на основі нейронної мережі. Саме тому було використано метод віоли Віоли-Джонса як найефективніший серед існуючих, він дозволяє розпізнати риси обличчя при великих кутах нахилу. У підсумку, після всіх маніпуляцій, пов'язаних з попередньою обробкою фотографій і підбором параметрів, точність розпізнавання на розширеній тестової вибірці матиме вищий результат ніж у комерційних аналогів.

В рамках дослідження було проведено ряд тестів для оптимізації кроків розпізнавання обличчя. Було визначено що навчання нейромережі використовуючи окремі ділянки обличчя значно підвищить якість роботи класифікаторів. Окрім того було визначено які зони обличчя класифікатор опрацьовує найгірше. Це дозволило також розглянути питання місцеположення камер перед фізичними бар’єрами.

Для подальшого покращення продукту та підвищення конкурентоспроможності можна виділити декілька кроків: розробка зручного інтерфейсу для інтеграції даного програмного рішення з іншими комерційними

програмами, покращення інтерфейсу з використанням останніх досягнень в розробці користувацьких інтерфейсів комерційного призначення, збільшення навчальної вибірки використовуючи набори зображень що знаходяться у вільному доступі, налаштування сервера під потреби програмного засобу.