

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки

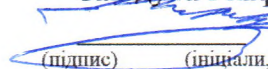
(повна назва інституту/факультету)

Акустичні та мультимедійні електронні системи

(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

 С.А. Найда
(підпис) (ініціали, прізвище)

“01” червня 2020 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності (спеціалізації) 171 Електроніка «Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки»

(код та назва спеціальності)

на тему: Система відеоспостереження з функцією розпізнавання з двома каналами передавання інформації

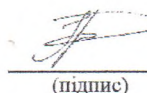
Виконала: студентка IV курсу, групи ДВ-61
(шифр групи)

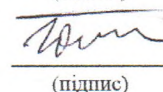
Чуян Ірина Олегівна

(прізвище, ім'я, по батькові)

Керівник доцент, к.т.н. Оникієнко Ю. О.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)


(підпис)


(підпис)

Консультант

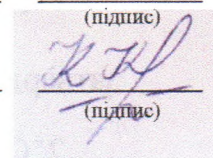
(назва розділу)

(посада, науковий ступінь, вчене звання, прізвище, ініціали)

(підпис)

Рецензент доцент, к.т.н. доцент Клен К.С.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)


(підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент


(підпис)

Київ – 2020 року

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

Факультет електроніки
(повна назва)

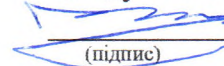
Акустичні та мультимедійні електронні системи
(повна назва)

Рівень вищої освіти – перший (бакалаврський)

Спеціальність (спеціалізація) 171 Електроніка “ Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки ”
(код і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

 С.А.Найда
(підпис) (ініціали, прізвище)

«25» _____ травня _____ 2020 р.

ЗАВДАННЯ

на дипломну роботу студенту

Чуян Ірині Олегівні _____
(прізвище, ім'я, по батькові)

1. Тема роботи: Система відеоспостереження з функцією розпізнавання з двома каналами передавання інформації

керівник роботи Оникієнко Юрій Олексійович, к.т.н. _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «25» _____ травня _____ 2020 р. №1196-с

2. Строк подання студентом роботи 1 червня 2020р.

3. Вихідні дані до роботи: Модулі GSM SIM800с, ESP32-CAM, USB-TTL конвертер FTDI.

4. Зміст (дипломної роботи) пояснювальної записки: 1) Провести теоретичний аналіз протоколів систем безпеки; 2) Проаналізувати засоби реалізації системи безпеки з відеоспостереженням та розпізнаванням обличчя; 3) Виконати реалізацію дослідного зразку системи безпеки.

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо) _____

1 презентація, 12 слайдів

6. Консультанти розділів проекту (роботи)*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____ 23.03.2020р. _____

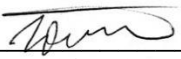
Календарний план

з/п	Назва етапів виконання дипломного проекту (роботи)	Строк виконання етапів роботи	Примітка
1	Огляд літератури по системам відеоспостереження та технологіям розпізнавання обличч.	13.04.2020-19.04.2020	виконано
2	Написання та аналіз перших трьох розділів.	20.04.2020-09.05.2020	виконано
3	Аналіз побудови систем відео-спостереження. Створення власної системи.	10.05.2020-19.05.2020	виконано
4	Оформлення розділів. Оформлення висновків та переліку посилань на літературу.	20.05.2020-31.05.2020	виконано
5	Підготовка та оформлення презентації для доповіді	01.06.2020-09.06.2020	виконано

Студент

Керівник роботи


(підпис)


(підпис)

І.О.Чуян

(ініціали, прізвище)

Ю.О. Онікієнко

(ініціали, прізвище)

УДК 778.534.6

РЕФЕРАТ

Дипломна робота: 87с., 2 табл., 37 рис., 2 дод., 23 джерел.

СИСТЕМА БЕЗПЕКИ, ВІДЕОПОСТЕРЕЖЕННЯ, РОЗПІЗНАВАННЯ ОБЛИЧ,
ПЕРЕДАВАННЯ ІНФОРМАЦІЇ, ESP-32, GSM800С

Актуальність дослідження технологій відеоспостереження та систем безпеки полягає у тому, що точність в таких системах дуже важлива та напряду залежить від якості її створення. Розвиток відеоспостереження відкриває нові можливості не тільки для фіксації правопорушень, а і для їх попередження.

Обґрунтування необхідності проведення дослідження. Існує багато стандартів та технічних рішень різних виробників. Зважаючи на це, виникає необхідність створення нових рішень для полегшення передачі даних на великих відстанях та удосконалення відеопотоку.

Мета даної роботи створення системи відеоспостереження з функцією ідентифікації особи та можливістю екстреного зв'язку на основі аналізу особливостей побудови і роботи систем відеоспостереження.

Об'єктом дослідження є системи безпеки та всі її компоненти.

Результатом дипломної роботи є створена система безпеки з функцією розпізнавання та з двома каналами передавання інформації.

Практичним значенням результату є можливість використання створеного приладу для охорони будь-яких об'єктів та здійснювати моніторинг процесу на кожному з його етапів; запобігати порушенням умов праці, техніки безпеки; запобігати розкраданню та псуванню майна.

ABSTRACT

Diploma work: 87p., 2 tables., 37 fig., 2 attachments, 23 sources.

SECURITY SYSTEM, VIDEO SURVEILLANCE, FACE RECOGNITION,
TRANSMISSION OF INFORMATION, ESP-32, GSM800C

The relevance of the study of video surveillance technologies and security systems is that the accuracy of such systems is very important and directly depends on the quality of its creation. The development of video surveillance opens up new opportunities not only for recording offenses, but also for their prevention.

Justification of the need for research. There are many standards and technical solutions from different manufacturers. Due to this, there is a need to create new solutions to facilitate long-distance data transmission and improve video flow.

The purpose of this work is to analyze the features of construction and operation of video surveillance systems, to offer a version of the video surveillance system with advanced functionality, namely the additional functions of personal identification and the possibility of emergency communication.

The object of research is security systems and all its components.

The result of the thesis is a security system with a recognition function and two channels of information transmission.

The practical significance of the result is the ability to use the created device to protect any objects and monitor the process at each of its stages; prevent violations of working conditions, safety; prevent theft and damage to property.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	9
ВСТУП	10
1 ОГЛЯД СИСТЕМ ВІДЕОПОСТЕРЕЖЕННЯ.....	12
1.1 Загальні відомості про системи відеоспостереження	12
1.2 Типові схеми побудови систем відеоспостереження	17
1.3 Обладнання для систем відеоспостереження	23
2 СИСТЕМА ВІДЕОПОСТЕРЕЖЕННЯ З ФУНКЦІЄЮ РОЗПІЗНАВАННЯ.....	26
2.1 Принципи розпізнавання об'єктів.....	26
2.2 Методи розпізнавання осіб	28
2.2.1 Розпізнавання райдужної оболонки	28
2.2.2 Розпізнавання відбитків пальців	30
2.2.3 Розпізнавання обличчя.....	33
2.3 Особливості розпізнавання в системах відеоспостереження	37
2.3.1 Відеоаналітика в системах відеоспостереження	37
2.3.2 Розпізнавання обличчя в системах відеоспостереження	39
3 СПОСОБИ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ ВІДЕОПОСТЕРЕЖЕННЯ ...	41
3.1 Особливості бездротового відеоспостереження на основі телекомунікаційних протоколів	41
3.2 Опис протоколів GSM, 3G, 4G	42
3.2.1 Побудова і робота мережі	42
3.2.2 Характеристики протоколу.....	44

3.2.3 Відмінності 3G, 4G відеоспостереження від GSM	45
3.2.4 GSM модуль для систем безпеки	46
3.3 Опис технології Wi-Fi.....	47
3.3.1 Конфігурації і робота мережі	47
3.3.2 Технічні характеристики.....	49
3.3.3 Wi-Fi для систем безпеки.....	51
3.4 Опис технології Bluetooth.....	52
3.4.1 Призначення, конфігурації і робота мережі	52
3.4.2 Технічні характеристики мережі	54
3.5 Порівняння способів передачі в системах відеоспостереження	54
4 СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ З ФУНКЦІЄЮ РОЗПІЗНАВАННЯ ТА З ДВОМА КАНАЛАМИ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ	57
4.1 Основні характеристики системи.....	57
4.2 Блок-схема системи відеоспостереження та схема підключення	59
4.3 Алгоритм роботи системи	59
4.4 Опис окремих складових системи відеоспостереження	61
4.4.1 Опис модуля ESP32.....	61
4.4.2 Опис камери OV2640	62
4.4.3 Опис GSM модуля SIM800с	63
4.4.4 Програмування і передача IP адреси користувачу	65
4.4.5 Опис програмного забезпечення	70
4.4.6 Опис інтерфейсу користувача	71

ВИСНОВКИ.....	74
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ	76
Додаток А. Лістинг програми для пристрою	78
Додаток Б. Summary	84

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AISS	–	Automated Information Systems Security
AIVSS	–	Advance Intelligent video surveillance system
GSM	–	The Global System for Mobile Communications
AHD	–	Analog High Definition
HDTV	–	High Definition Transport Video Interface
HDCVI	–	High Definition Composite Video Interface
IP	–	Internet Protocol
HDVR	–	Hybrid Digital Video Recorder
HD	–	Home Depot
ILSVRC	–	The ImageNet Large Scale Visual Recognition Challenge
PTZ	–	A pan–tilt–zoom
3G	–	Third generation
4G	–	Fourth generation
BS	–	Base station
LAC	–	Local Area Controller
MSC	–	Mobile services Switching Center
IMSI	–	International Subscriber Identification Number
HLR	–	Home Location Register
VLR	–	Visitor Location Register
ISDN	–	Integrated Services Digital Network
FDN	–	Fixed Dialing Number
DSL	–	A domain-specific language
ISM	–	Industrial, Scientific, Medical

ВСТУП

Системи відеоспостереження з можливістю передачі інформації є актуальними на сьогоднішній день та являються найбільш затребуваними системами для охоронних та моніторингових цілей. Розвиток систем відеоспостереження відкриває нові можливості не тільки для фіксації правопорушень, а, що є більш важливим, для їх попередження. Тому дані системи набули широкого застосування.

Бездротові відеокамери спостереження мають підвищену мобільністю, оскільки відсутність проводів дозволяє розміщувати їх в будь-якому зручному місці та злочинці не зможуть дезактивувати такі відеокамери спостереження, перерізавши їх кабелі.

Багато хто купує бездротові системи безпеки, бажаючи скористатися їх численними перевагами. Однак ці системи безпеки також мають недоліки, які можуть викликати у їх користувачів розчарування.

Бездротові системи безпеки є відносно новими рішеннями, в яких використовуються найсучасніші технології. З огляду на ці факти попит на них вище, ніж попит на традиційні системи безпеки. Тому ціна на них буде вище. Багато компонентів системи безпеки, наприклад, охоронні датчики, працюють від акумулятора. Батареї можуть з часом розрядитися і зробити вашу систему неефективною. Несправний датчик може залишити вас уразливими до тих пір, поки у вас не буде можливості замінити батареї. У міру того як батареї будуть розряджатися, деякі системи безпеки можуть гірше функціонувати і, отже, видавати помилкові сигнали тривоги або не реагувати на команди.

Перечисленні вище недоліки можуть бути виправленими новою запропонованою системою з розширеним функціоналом, низькою ціною за матеріали та можливістю підключення до будь-якого джерела живлення.

Метою роботи є створення системи відеоспостереження з розширеним функціоналом, а саме з додатковими функціями ідентифікації особи та можливістю екстреного зв'язку.

Для досягнення поставленої мети потрібно виконати такі завдання:

- проаналізувати різні протоколи керування відеоспостереження та систем безпеки;
- дослідити специфіку роботи систем безпеки;
- обрати спосіб передачі даних;
- створити алгоритм роботи власної системи безпеки та необхідне програмне забезпечення.

1 ОГЛЯД СИСТЕМ ВІДЕОПОСТЕРЕЖЕННЯ

1.1 Загальні відомості про системи відеоспостереження

Системи відеоспостереження з можливістю передачі інформації є актуальними на сьогоднішній день, це затребувана система для моніторингових та охоронних цілей. Розвиток систем безпеки та відеоспостереження відкриває нові можливості не тільки для фіксації правопорушень, а і для їх попередження. Тому дані системи набули надзвичайно широкого застосування та використовуються всюди, наприклад в аеропортах, офісах (Рисунок 1.1).



Рисунок 1.1 – Застосування систем відеоспостереження

Протягом останніх кількох десятиліть значні темпи зростання інфраструктури були досягнуті у питаннях, пов'язаних із безпекою у всьому світі.

Таким чином, із збільшенням попиту на безпеку відеоспостереження стало важливим напрямом досліджень. Інтелектуальна система відеоспостереження в основному цензурує продуктивність, події або зміну інформації, як правило, стосовно людей, транспортних засобів або будь-яких інших об'єктів здалеку за допомогою електронного обладнання (зазвичай цифрової камери).

У широкому розумінні відеоспостереження можна охарактеризувати як інтелектуальну техніку обробки відео, створену для надання допомоги персоналу безпеки шляхом надання надійних оповіщень у режимі реального часу та підтримки ефективного відео аналізу для судових розслідувань.

Розглядаються різні вимоги до розробки надійної та надійної системи відеоспостереження. Також розглядаються різні типи камер, необхідні в різних екологічних умовах, таких як внутрішні та зовнішні в системах спостереження (Рисунок 1.2).



Рисунок 1.2 – Приклад застосування камери відеоспостереження

Помічено, що спостереження з повною участю операторів людини має певні недоліки, як, наприклад, висока вартість робочої сили, відхилення тривалої

фіксації та обмежена можливість багатоекранного моніторингу. Традиційні системи спостереження доповнюються та навіть замінюються вдосконаленими інтелектуальними системами спостереження (AISS), оскільки останні використовуються для виявлення ненормальної поведінки та моделей у відеороликах шляхом розробки технологій штучного інтелекту, розпізнавання образів та комп'ютерного зору. Це дозволяє підвищити точність моніторингу кількох сценаріїв кількома спостерігачами.



Рисунок 1.3 – Застосування IP-камер для технології відеоспостереження

В останні кілька років ринок відеоспостереження зазнав значної трансформації в системи відеоспостереження третього покоління, переходячи до IP-відео з традиційного аналогового відео (Рисунок 1.3), спричиняючи кращу обробки та покращений алгоритм стиснення. З третім поколінням почалася ера

інтелектуального відеоспостереження не тільки в науково-дослідних лабораторіях, але і на ринку.

З початком 2010-х років багато дослідницьких лабораторій, наприклад, лабораторії Kiwi Security Labs, почали впроваджувати «Передові інтелектуальні системи відеоспостереження» (AIVSS). У цій технології представлена нова категорія функцій, які, як очікується, матимуть великий вплив на ринок систем безпеки.

Крім апаратних засобів та програмного забезпечення, які розглядаються як поліпшувачі продуктивності та архітектури міжопераційної обробки, продуктивність будь-якої системи залежить від конфіденційності системи. Більше того, у багатьох країнах питання конфіденційності набувають все більшого значення і розглядаються як сповільнювач ефективності.

З одного боку, продуктивність мережі залежить від продуктивності кожного з мережевих елементів, продуктивності доступу, продуктивності передачі тощо, які також розглядаються як сповільнювач продуктивності, а з іншого боку, продуктивність мережі багато в чому залежить від процес управління безпекою вдосконаленої системи. Захист знову бере на себе значну частину виконання безпеки та у формах адміністрування безпеки та відповідно щодо виконання системи як уповільнювача виконання [1].

Основна мета такої системи – забезпечення надійної система виявлення рухомих об'єктів, яка постійно шукає рух і кожного разу, коли знаходить рух об'єкта, він одночасно починає записувати відео, після чого він дає сповіщення про тривогу та надсилання повідомлення на адресу зацікавленої особи.

Встановивши систему відеоспостереження можливо: здійснювати моніторинг виробничого процесу на кожному з його етапів, мати повну та

задокументовану інформацію про нещасні випадки на виробництві; запобігати порушенням якості виробництва, умов праці, техніки безпеки; запобігати розкраданню та псуванню вироблених товарів та продуктів, виробничого майна. Використання систем безпеки зі всіма можливостями для виробництва представлено на Рисунку 1.4.



Рисунок 1.4 – Відеоспостереження на виробництві

Система відеоспостереження - затребувана система з метою безпеки та моніторингу для офісу і для дому. Розвиток систем відеоспостереження пропонує нові можливості не лише для реєстрації правопорушень, але, що ще важливіше, для їх запобігання.

Система відеоспостереження дозволяє вести віддалений контроль з камер відеоспостереження через Інтернет на будь-якому персональному пристрою, таких як планшет, смартфон, стаціонарний комп'ютер (Рисунок 1.5).



Рисунок 1.5 – Гаджети для технології відеоспостереження

Все частіше системи відеоспостереження використовуються і для дому, де виникає необхідність передавати певну інформацію до власника. Передача може здійснюватися за допомогою технологій GSM, Bluetooth, Wi-Fi та ін. Тип модуля визначається відстанню на яку потрібно передавати певну інформацію.

1.2 Типові схеми побудови систем відеоспостереження

Побудова системи відеоспостереження для об'єкта, там де планується вестися охоронна діяльність, на сьогодні є досить важливим етапом, від якого залежить подальша робота і здатність обладнання справлятися з поставленими обов'язками та завданнями. У побудові відео-системи необхідно враховувати такі фактори: вид та призначення системи відеоспостереження, тип та вартість необхідного обладнання, розрахунок кількості необхідних складових для

конкретного об'єкта, територіальні особливості, вимоги до системи і фінансові можливості власника.

Важливий момент при побудові системи відеоспостереження – точно визначити цілі її установки і завдання, які має вирішувати система відеоспостереження.

Якщо, наприклад, вибір було зроблено на користь аналогової системи, то і обладнання потрібно вибирати відповідне. Для системи відеоспостереження такого типу будуть потрібні аналогові камери відеоспостереження, матричні відеокомутатори, мультиплексори, відеомагнітофони та інше. Для створення цифрової системи відеоспостереження потрібні вже зовсім інші пристрої: ПК, комутатори, мережеві камери відеоспостереження та ін.

Не існує універсального варіанту побудови будь-якої системи відеоспостереження для всіх об'єктів. Також не представляється можливим розглянути всі способи побудови, так як варіантів може бути багато із-за різноманітності умов та обладнання. Існують деякі стандартні підходи до вибору відеопристроїв та їх розташування на об'єкті. Наприклад, якась система відеоспостереження для охорони офісу може складатися з аналогових камер відеоспостереження та плат відеозахоплення. Такий варіант давно використовується. Але можна вибрати і більш сучасний на сьогодні підхід — цифрове відеоспостереження. Якщо думати про місця установки відеопристроїв, то, в першу чергу, камери для відеоспостереження потрібно встановлювати таким чином, щоб під їх об'єктив потрапляли такі місця, де відбуваються найважливіші операції в організації. Якщо це, наприклад, фінансові установи, то до них слід віднести касові зони, відділи бухгалтерії та ін.



Рисунок 1.6 – Приклад відеоспостереження в магазині

Система безпеки та відеоспостереження, яка використовується для охорони торгового підприємства в свій склад включає спеціальне програмне забезпечення, яке може контролювати роботу касових апаратів, персональний комп'ютер із платою відеозахоплення, це все запобігає різним шахрайським діям. Під об'єктиви камер відеоспостереження, на сам перед, повинні потрапляти вітрини з товаром, особливу увагу потрібно приділити місцям реалізації та продажу дорогої продукції. Крім того, відеокамери слід встановити по периметру магазину, задля підвищення рівня безпеки об'єкта, як показано на Рисунку 1.6.

Останнім часом широко поширилась установка відеоспостереження в домах. Все більша кількість сімей задається питанням безпеки свого майна та їх самих. Систему відеоспостереження в квартирі слід почати будувати з моніторингу входних дверей. Відео дозволить зрозуміти, чи варто впускати гостя [2].

Будь-яка система відеоспостереження може бути побудована на підставі наступних принципів:

- зі значним ступенем сегментування, використанням локальних сегментів, пов'язаних з центральним сховищем або точкою доступу до даних;
- з максимально простим механізмом доступу до будь-якого відеопотоку, з можливістю підключення кожного комп'ютера до будь-якої камери.

Залежно від прийнятого принципу організації доступу, при реалізації конкретного проекту вибираються моделі камер, додаткового обладнання, ліній передачі даних.

- *Пряма.* Система відеоспостереження прямого типу використовує принцип поділу сегментів (Рисунок 1.7).

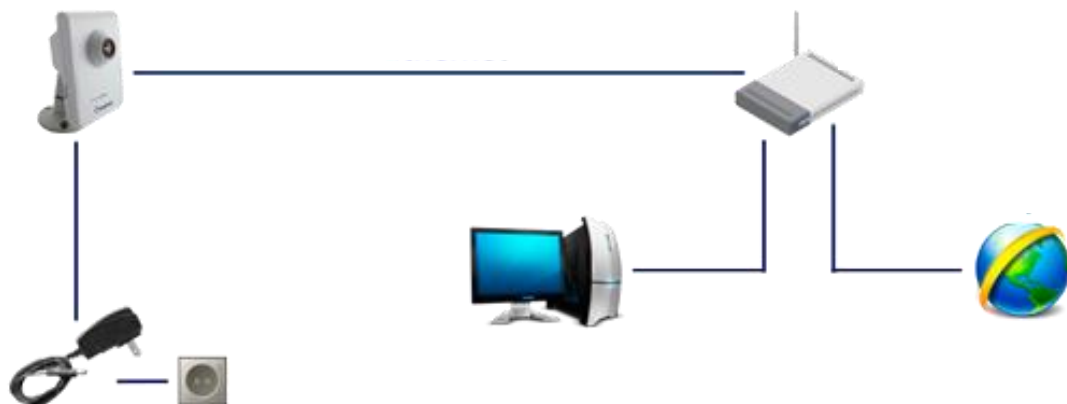


Рисунок 1.7 – Пряма структура побудови системи безпеки

Описуючи простими словами, таку структуру можна охарактеризувати так:

- камера (або декілька) підключається до комутатора;
- комп'ютери, підключені до цього ж вузловому інших мережних пристроїв - можуть отримати доступ до відеопотоку камер;
- для користувачів іншого сегмента мережі - дані відеоспостереження сусідній мережевій зоні безпосередньо недоступні.

Прямий принцип побудови відеоспостереження - це структура типу зірка. В її центрі знаходиться головний вузол зберігання або обробки даних. Саме він є загальною точкою доступу.

Всі користувачі отримують дані тільки після підключення до сервера, що дозволяє прозоро і зручно регулювати права доступу і інші політики поводження з результатами відеоспостереження.

- *Перехресна.* Перехресна схема відеоспостереження - максимально відкрита для всіх учасників мережі (Рисунок 1.8).

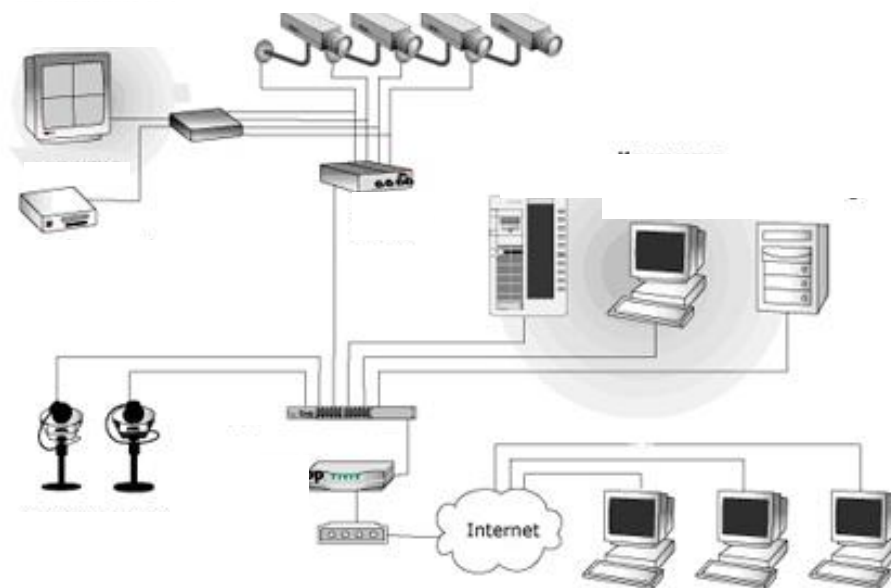


Рисунок 1.8 – Перехресна структура побудови системи безпеки

Якщо аналізувати, як побудувати систему відеоспостереження з IP камерами даного типу - можна легко зрозуміти, що для реалізації проекту знадобляться вельми сучасні пристрої.

Рекомендується в перехресній моделі використовувати камери з внутрішньою системою авторизації, здатні працювати як учасник локальної або глобальної комп'ютерної мережі.

Дана схема відеоспостереження передбачає простий доступ кожного комп'ютера до будь-якої камери.

Така структура легко будується. Однак управління правами і обмеженнями - являє собою досить складну задачу, не відрізняється гнучкістю і швидкістю проведення перебудовань.

Потенційно, через людський фактор або внаслідок зловмисного пристрою - зловмисник отримує можливість доступу до всіх даних перехресної структури [3].

Як відомо, IP відеокамера є повністю самодостатнім пристроєм, який здатний самостійно стиснути відео і передати його вже в стислому вигляді, має вбудований Web сервер, що знімає будь-які обмеження в дистанціях між камерою відеоспостереження та користувачем. Дані пристрої можуть працювати як в зв'язці комп'ютером, відеореєстратором - так і автономно.

Така універсальність, дає досить багато варіацій для побудови системи відеоспостереження на IP відеокамері:

- Класичне побудова. З використанням відеореєстратора і зовнішніх; джерел живлення для камер відеоспостереження;
- Варіант з використанням комп'ютера як сховища інформації та керуючого пристрою;
- Використання IP відеокамер автономно;
- Побудова системи з використанням технології Wi-Fi [4].

1.3 Обладнання для систем відеоспостереження

Система відеоспостереження використовує компоненти, безпосередньо підключені для створення, передачі, показу та зберігання відеодані. Система відеоспостереження може бути такою ж простою, як камера, придбана в магазині електроніки, підключена до відеомонітора.

IP камера ще недавно була занадто дорогою для середньостатистичного користувача. Однак ціна на цифрове обладнання постійно падає. Сьогодні навіть середньостатистична невелика компанія може побудувати систему відеоспостереження на IP камерах. При цьому загальна ціна рішення може бути нижче, ніж реалізація проекту на аналогових пристроях через меншої кількості необхідного обладнання.



Рисунок 1.9 – Приклад обладнання для систем відеоспостереження

Для того, щоб побачити, що система моніторингу роботи працює як окремий пристрій, необхідно подбати про наявність наступного обладнання: камер, монітора, обладнання для запису та додаткового обладнання, такі як комутатори, розширювачі та ін. (Рисунок 1.9).

Основні категорії системного відеоспостереження:

- Відеокамери - аналогові, AHD, HDTVI, HDCVI, IP камери (вуличні, внутрішні, купольні, чорно-білі та кольорові, міні, корпусні, циліндричні та безкорпусні), з датчиком руху, муляж;
- Відеореєстратори - звичайні аналогові, гібридні - AHD, HDVR, HDCVI, HDTVI, HD, IP;
- ІК-підсвітка;
- Монітори - різняться за розмірами, якісними зображеннями, кількістю відео та аудіо виходами, також мають спеціальні технічні характеристики у відмінних від комп'ютерних;
- Плати відеозахоплення. У залежності від моделей, таке обладнання відрізняється кількістю аудіо-, відеовходів (4, 8, 16);
- Додаткове обладнання - комутатори та розширювачі.

Відеоспостереження для будинку:

Залежно від місця установки, системи відеоспостереження діляться на:

- Внутрішні - аналогові, IP, поворотні, кольорові, бездротові і т.д.;
- Вуличні - оснащені високим класом захисту від зовнішніх впливів (кліматичних і механічних), мають нічну інфрачервону підсвітку, завдяки якій забезпечують якісне зображення навіть при повній темряві, і розраховані на безперебійну роботу [5].

Висновки до розділу 1

Останнім часом системи спостереження набувають великої популярності. Уряд, організації, житлові товариства тощо використовують ці системи для перевірки різних видів діяльності з метою безпеки та безпеки.

Раніше системи спостереження мали велику залежність від операторів, останнім часом перевагу надають автоматизованим системам через кращу ефективність та надійність.

Система відеоспостереження необхідна для забезпечення безпеки об'єкта. Наявність камер відеоспостереження або навіть знаків, що попереджають про моніторинг відеоспостереження в видимих місцях, запобігає крадіжкам зі зломом.

Система відеоспостереження також може підвищити безпеку людей, що працюють в приміщеннях, задля своєчасного виявлення загрози життю. Регулярне технічне обслуговування забезпечить безперебійну роботу клієнтського обладнання на протязі всього строку експлуатації.

2 СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ З ФУНКЦІЮ РОЗПІЗНАВАННЯ

2.1 Принципи розпізнавання об'єктів

Розпізнавання об'єктів - технологія в області комп'ютерного зору для пошуку та ідентифікації об'єктів у послідовності зображення чи відео. Зображення предметів можуть дещо відрізнятися в різних точках огляду, в різних розмірах і масштабах, або навіть при їх перекладі або обертанні. Об'єкти можливо розпізнати навіть коли вони частково перешкоджають зору. Це завдання як і раніше є викликом для систем комп'ютерного зору. Багато підходів до цього завдання впроваджено протягом декількох десятиліть.

Класифікація зображень передбачає прогнозування класу одного об'єкта в зображенні. Локалізація об'єкта означає визначення місця розташування одного або декількох об'єктів у зображенні та нанесення рясного ряду навколо їх розміру. Виявлення об'єктів поєднує ці дві задачі та локалізує та класифікує один або кілька об'єктів у зображенні.

Таким чином, можливо виділити три завдання:

1. Класифікація зображень: передбачити тип або клас об'єкта на зображенні.
 - Введення: зображення з одним об'єктом, наприклад фотографії.
 - Вихід: мітка класу (наприклад, одне або більше цілих чисел, які відображаються на мітках класів).
2. Локалізація об'єктів: Знайти присутність об'єктів на зображенні та вказати їх розташування за допомогою обмежувального поля.

- Введення: зображення з одним або декількома об'єктами, наприклад фотографією.

- Вихід: одна або кілька обмежувальних коробок (наприклад, визначених точкою, шириною та висотою).

3. Виявлення об'єктів: Знайти присутність об'єктів із обмежувальним вікном та типами або класами розташованих об'єктів на зображенні.

- Введення: зображення з одним або декількома об'єктами, наприклад фотографією.

- Вихід: одна або кілька обмежувальних коробок (наприклад, визначених точкою, шириною та висотою) та мітка класу для кожного обмежувального поля.

Ще одним розширенням цієї розбивки завдань комп'ютерного зору є сегментація об'єктів, яка також називається "сегментація екземпляра об'єкта" або "семантична сегментація", де екземпляри розпізнаних об'єктів позначаються виділенням конкретних пікселів об'єкта замість грубої рамки обмеження.

Більшість останніх нововведень у проблемі розпізнавання зображень стали частиною участі у завданнях ILSVRC.

Це щорічна академічна конкуренція з окремим викликом для кожного з цих трьох типів проблем із метою сприяння незалежним та окремим вдосконаленням на кожному рівні, які можна використовувати в більш широкому плані. Наприклад, нижче наведено перелік трьох відповідних типів завдань нижче, взятих із оглядового документа ILSVRC за 2015 рік:

- Класифікація зображень: Алгоритм, що створює перелік категорій об'єктів, наявних на зображенні.

- Локалізація одного об'єкта: Алгоритм, що створює список категорій об'єктів, присутніх на зображенні, разом із вікном, що обмежує вісь із зазначенням положення та масштабу одного екземпляра кожної категорії об'єктів.
- Виявлення об'єкта: Алгоритм, що створює перелік категорій об'єктів, наявних на зображенні, разом із вікном, що обмежує вісь із зазначенням положення та масштабу кожного примірника кожної категорії об'єктів [6].

2.2 Методи розпізнавання осіб

2.2.1 Розпізнавання райдужної оболонки

Розпізнавання райдужної оболонки або сканування райдужної оболонки - це процес використання видимого та ближнього інфрачервоного світла для фотографування ока. Це форма біометричної технології в тій же категорії, що і розпізнавання обличчя та відбитки пальців.

Прихильники технології сканування райдужної оболонки стверджують, що вона дозволяє правоохоронцям порівнювати зображення райдужки підозрюваних із наявною базою зображень, щоб визначити або підтвердити особу суб'єкта. Вони також заявляють, що сканування райдужної оболонки швидше і надійніше, ніж сканування відбитків пальців, оскільки людині легше затемнити або змінити пальці, ніж змінити очі.

Але не потрібно забувати, що сканування райдужної оболонки значно обмежує конфіденційність. Можливо сканувати райдужки з відстані або навіть у русі, а це означає, що дані можна збирати приховано, без відома людей, не кажучи вже про згоду. Також є проблеми з безпекою: якщо база даних біометричної інформації буде викрадена або порушена, неможливо отримати новий набір очей,

як один отримав би переоформлений номер кредитної картки. А біометрику райдужної оболонки часто збирають та зберігають сторонні виробники, що значно посилює проблеми безпеки.



Рисунок 2.1 – Сканування райдужної оболонки

Сканування райдужної оболонки вимірює унікальні візерунки райдужки, кольорові кола в очах людей (Рисунок 2.1). Біометричні сканери розпізнавання райдужної оболонки працюють шляхом освітлення райдужної оболонки невидимим інфрачервоним світлом, щоб підібрати унікальні візерунки, які не видно неозброєним оком. Сканери райдужної оболонки виявляють і виключають вії, повіки та окулярні відблиски, які, як правило, блокують частини райдужної оболонки. Кінцевий результат - набір пікселів, що містять лише райдужку. Далі, малюнок ліній і кольорів очей аналізується для отримання бітового малюнка, що кодує інформацію в райдужній оболонці. Цей бітовий зразок оцифровується та

порівнюється із збереженими шаблонами в базі даних для перевірки (відповідність шаблону один на один) або ідентифікації (узгодження шаблону один на багато).



Рисунок 2.2 – Приклад застосування сканування ока

Камери для сканування райдужної оболонки можуть бути встановлені на стіні чи іншому фіксованому місці, або вони можуть бути ручними та портативними (Рисунок 2.2). Дослідники з університету Карнегі Меллон розробляють сканери дальнього радіусу дії, які навіть можуть бути використані для захоплення знімків на відстані до 40 футів [7].

2.2.2 Розпізнавання відбитків пальців

Через свою унікальність відбитки пальців використовувались для ідентифікації протягом століття, останнім часом ставали автоматизованими (тобто біометричними) завдяки прогресу в обчислювальних можливостях. Ідентифікація відбитків пальців популярна через притаманну їй простоту, численні джерела (10

пальців), доступні для збору, та встановлене ними використання правоохоронними органами та міграційною службою, як база даних (Рисунок 2.3).



Рисунок 2.3 – База даних відбитків пальців

Практика використання відбитків пальців як методу ідентифікації осіб застосовується з кінця XIX століття, коли сер Френсіс Галтон визначив деякі моменти або характеристики, з яких можна було б визначити відбитки пальців. Ці "точки Галтона" є фундаментом для науки про ідентифікацію відбитків пальців, яка розширилась і перейшла за минуле століття. Ідентифікація відбитків пальців розпочала свій перехід до автоматизації наприкінці 1960-х років разом з появою обчислювальних технологій. З появою комп'ютерів, і підмножина Galton Points була використана для розробки автоматизованої технології відбитків пальців.

Відбиток пальців, як правило, представляє собою серію темних ліній, що представляють високу, найвищу частину шкіри хребта тертя, тоді як долина між цими хребтами виглядає як пробіл і є низькою, неглибокою частиною шкіри хребта тертя. Ідентифікація відбитків пальців ґрунтується насамперед на деталях, або на розташуванні та напрямку кінців хребта та роздвоєння (розколи) вздовж конькового шляху.

Для збору цифрового зображення поверхні відбитків пальців використовуються різні типи датчиків - оптичний, ємнісний, ультразвуковий та тепловий. Оптичні датчики знімають відбиток пальця, який є найпоширенішим датчиком сьогодні та використовується при ідентифікації людей (Рисунок 2.4).



Рисунок 2.4 – Приклад застосування використання відбитків пальців як методу ідентифікації осіб

Дві основні категорії методів зіставлення відбитків пальців - це відповідність на основі дрібниць і відповідність шаблону. Збірка шаблонів просто порівнює два

зображення, щоб побачити, наскільки вони схожі. Зіставлення шаблонів зазвичай використовується в системах відбитків пальців для виявлення дублікатів. Найпоширеніша методика розпізнавання - хвилинна відповідність, покладається на хвилинні бали, зокрема на розташування та напрямок кожної точки [8].

2.2.3 Розпізнавання обличчя

Розпізнавання обличчя - це метод виявлення або перевірки особи, використовуючи їх обличчя. Системи розпізнавання обличчя можна використовувати для ідентифікації людей на фотографіях, відео або в режимі реального часу. Правоохоронні органи також можуть використовувати мобільні пристрої для ідентифікації людей під час зупинок поліцією.

Але технологія розпізнавання обличчя може помилятися, що може потягнути покарання людей за злочини, які вони не вчиняли. Програмне забезпечення для розпізнавання обличчя особливо погано розпізнає афроамериканців та етнічних меншин, жінок та молодих людей, часто неправильно ідентифікуючи або не виконуючи їх ідентифікації.

Системи розпізнавання обличчя використовують комп'ютерні алгоритми для вибору конкретних, відмінних деталей обличчя людини. Ці деталі, такі як відстань між очима або форма підборіддя, потім перетворюються на математичне зображення та порівнюються з даними про інші обличчя, зібраними в базі даних розпізнавання обличчя. Дані про певне обличчя часто називають шаблоном обличчя і відрізняються від фотографії, оскільки вони розроблені так, щоб включати лише певні деталі, які можна використовувати для відрізнення одного обличчя від іншого.

Найближчим часом технологія розпізнавання обличчя, швидше за все, стане більш розповсюдженою. Вона може бути використана для відстеження руху людей

у світі, як автоматичні зчитувачі номерних знаків для відстеження транспортних засобів за номерами табличок. Розпізнавання обличчя в реальному часі вже використовується в інших країнах і навіть на спортивних змаганнях у Сполучених Штатах та інших країнах (Рисунок 2.5).



Рисунок 2.5 – Застосовування технології сканування обличчя

Деякі системи розпізнавання обличчя, замість того, щоб позитивно ідентифікувати невідому особу, розроблені для обчислення шкали ймовірності відповідності між невідомою особою та певними шаблонами обличчя, що зберігаються в базі даних. Ці системи пропонують кілька потенційних співпадінь, класифікованих за ймовірністю правильної ідентифікації, замість того, щоб просто повернути один результат.

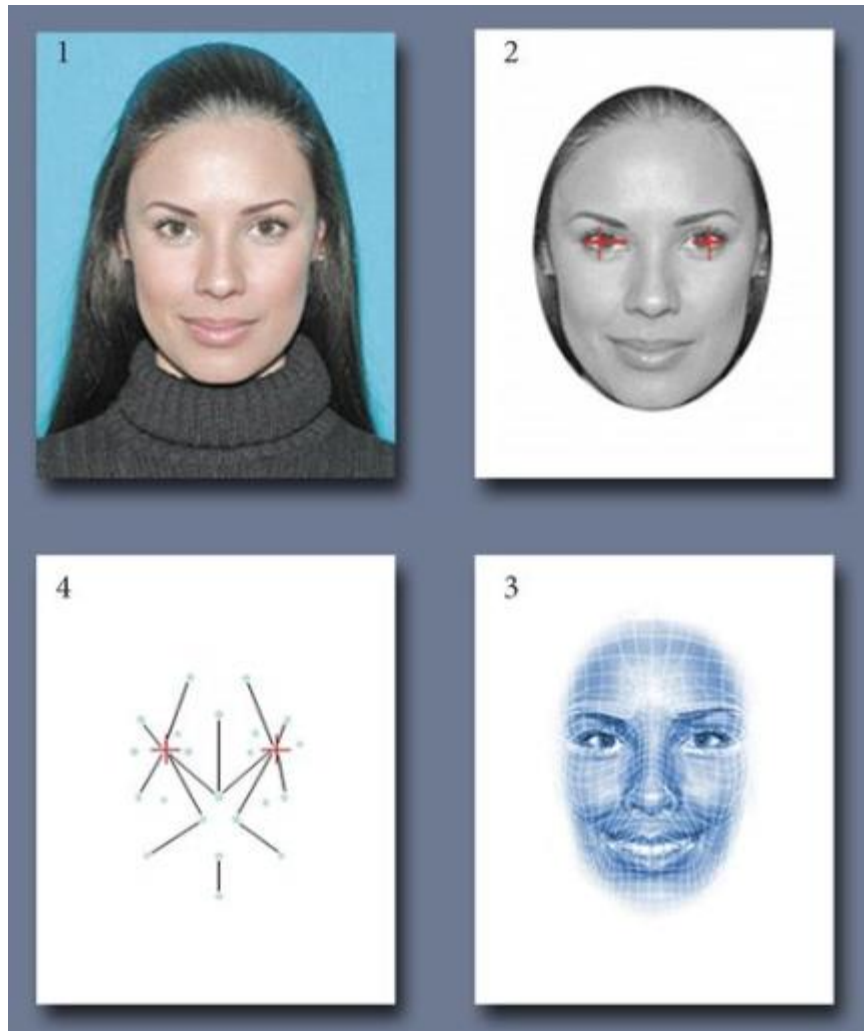


Рисунок 2.6 – Алгоритм ідентифікації людини

Як працює ідентифікація обличчя (Рисунок 2.6):

1. Зображення знімається
2. Визначаються місця розташування очей
3. Зображення перетворюється в чорно-біле і обрізається
4. Зображення перетворюється в шаблон, використовуваний пошуковою системою для результатів порівняння обличчя. Зображення розшукується за

допомогою складного алгоритму порівняння шаблону з іншими шаблонами у файлі.

Системи розпізнавання обличчя відрізняються своєю здатністю ідентифікувати людей у складних умовах, таких як погане освітлення, низька якість дозволу зображення та неоптимальний кут зору, наприклад: на фотографії, зробленій згори, дивлячись на невідому людину або в натовпі (Рисунок 2.7).



Рисунок 2.7 – Приклад застосування технології в публічному місті

Що стосується помилок, то слід розуміти два ключові поняття:

"Неправдивий мінус" - це коли система розпізнавання обличчя не відповідає особі людини зображенню, яке фактично міститься в базі даних. Іншими словами, система помилково поверне нульові результати у відповідь на запит.

"Неправдивим позитивом" є те, коли система розпізнавання обличчя відповідає зображенню особи в зображенні в базі даних, але ця відповідність насправді неправильна. Це коли поліцейський подає зображення "Джо", але система помилково повідомляє офіцеру, що на фотографії є "Джек".

Досліджуючи систему розпізнавання обличчя, важливо уважно ознайомитися зі вірогідністю "помилково позитивної" та "помилкової негативної" вірогідності, оскільки це майже завжди є компромісом. Наприклад, якщо використовується розпізнавання обличчя для розблокування телефону, краще, якщо система кілька разів не зможе ідентифікувати (помилковий негатив), ніж система неправильно ідентифікує інших людей, і дозволяє цим людям розблокувати телефон (хибно позитивний). Якщо результатом неправильної ідентифікації є те, що невинна людина потрапляє до в'язниці (як неправильна ідентифікація в базі даних помилок), тоді система повинна бути спроектована таким чином, щоб було якомога менше помилкових позитивів [9].

2.3 Особливості розпізнавання в системах відеоспостереження

2.3.1 Відеоаналітика в системах відеоспостереження

Відеоаналітика може перетворити стандартні системи відеоспостереження в інтелектуальні та ефективні системи виявлення та оповіщення. Тепер технологія відеоспостереження здатна автоматично розпізнавати обличчя людей, транспортних засобів, тварин та сумки.

Інтегровані з відеоаналітикою відеоспостереження, як програмне забезпечення для обличчя, так і системи загального розпізнавання здатні рахувати, вимірювати швидкість і моніторинг напрямку. Наприклад, системи розпізнавання

можуть відстежувати тривалість часу перебування людей у певній зоні або те, як довго залишається сумка без нагляду. Деякі рішення для відео аналітики навіть здатні зрозуміти колір.

Інтелектуальне програмне забезпечення для відео аналітики може розпізнавати різні способи поведінки та підняти тривогу за визначеним користувачем правилом, наприклад, "людина, що рухається від транспортного засобу до транспортного засобу на автостоянці" або "великий білий автомобіль, припаркований у контрольованій зоні" (Рисунок 2.8).

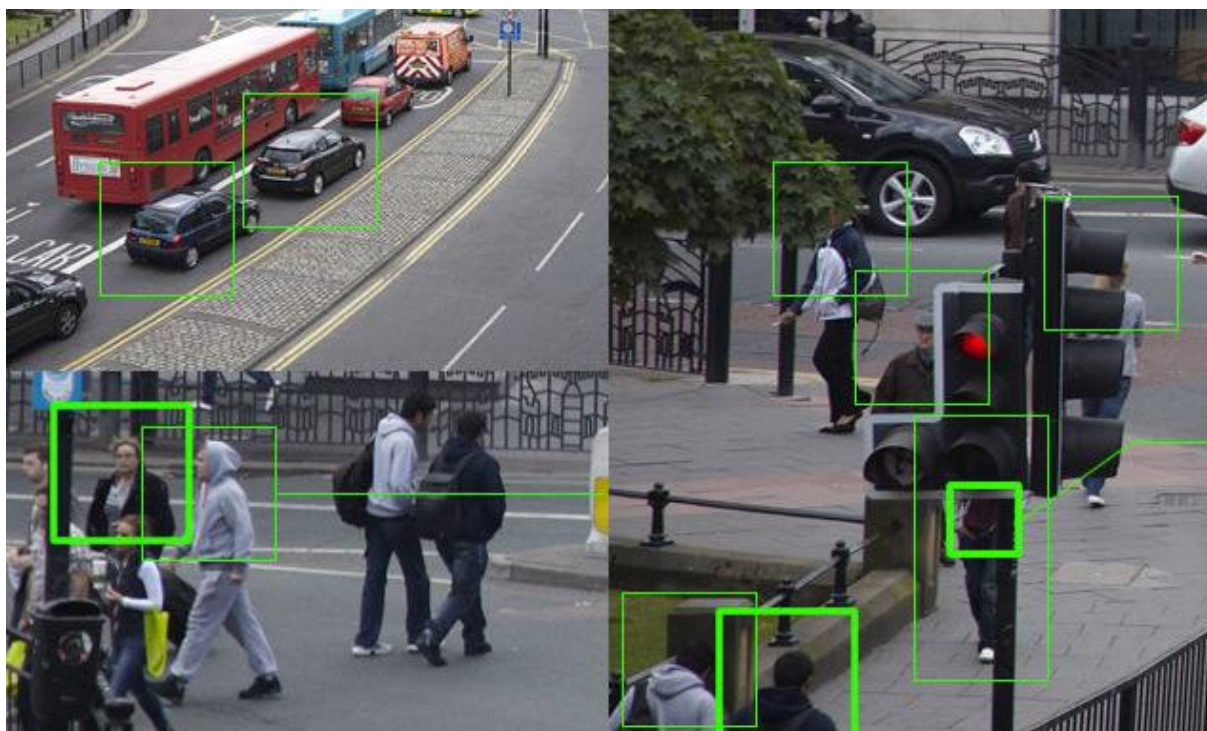


Рисунок 2.8 – Приклад застосування відеоаналітики

Інтелектуальне відео також може підвищити ефективність операторів кабінетів управління, автоматизувати тривогу для систем без моніторингу, маневрувати PTZ-камерами для збільшення об'єктів, створюючи сигнали тривоги та економити час під час пошуку записів відеоспостереження.

2.3.2 Розпізнавання обличчя в системах відеоспостереження

Розпізнавання обличчя - це так же спосіб ідентифікації особи задля безпеки. Система розпізнавання обличчя використовує біометрику для відображення рис обличчя з фотографії чи відео. Потім порівнює інформацію з базою даних відомих обличч для пошуку відповідності. Розпізнавання обличчя може допомогти перевірити особистість, але воно також викликає проблеми конфіденційності.

Біометричні системи розпізнавання обличчя порівнюють зображення людей, що надходять із системи відеоспостереження в базу даних та надсилають сповіщення, коли відбувається позитивна відповідність. Такі технології успішно використовують в житлових будинках, офісах тощо (Рисунок 2.9).



Рисунок 2.9 – Приклад застосування технології розпізнавання обличчя

Основними кроками в розпізнаванні обличчя є:

- Виявлення обличчя.
- Запис виявлених обличч.
- Порівнювати записані обличчя з тими, що зберігаються в базі даних.

- Автоматичний процес пошуку найближчої відповідності [10].

Висновки до розділу 2

Ідентифікація людини вже давно набула широкого використання по всьому світу. З її використанням стало можливим покращення систем безпеки та правоохоронних напрямлень.

Існує три основних способи розпізнавання особи.

- Сканування райдужки ока з відстані або навіть в русі, а це означає, що ці дані можливо збирати приховано, без відома людей.
- Ідентифікація відбитків пальців людини популярна через притаманну їй простоту придбання.
- Розпізнавання обличчя - лише початок реалізації методу розпізнавання. Обличчя людини - це лише один із об'єктів, який слід виявити. Інші об'єкти можна ідентифікувати таким же чином. Наприклад, це можуть бути очі людей та їх пальці.

Відеоспостереження є важливою частиною системи безпеки, де найголовнішим доповненням є ІР-камери та функція розпізнавання. Камери для відеоспостереження та ідентифікація людини важлива тим, що за її допомоги можливо збирати дані про обличчя конкретних осіб та зберігати їх.

3 СПОСОБИ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

3.1 Особливості бездротового відеоспостереження на основі телекомунікаційних протоколів

Під бездротовим відеоспостереженням мається на увазі система, в якій між телекамерою і користувачем, або кінцевим пристроєм запису/видачі відеокартинки, лінією передачі інформації є радіочастотний канал. Приклади пристроїв наведені на Рисунку 3.1. За способом передачі даних такі системи підрозділяються на:

- WiFi;
- GSM, 3G, 4G;
- Bluetooth;



Рисунок 3.1 – Види бездротових пристроїв

Безпроводне відеоспостереження необхідно там, де прокласти кабель практично неможливо, або витрати на прокладку настільки високі, що перебивають необхідність будь-якої охорони, ще при використанні мобільних систем охорони (ті які постійно переміщаються), або коли потрібно віддалено стежити за об'єктом, що охороняється без присутності на об'єкті охорони, або сторожа, в цьому випадку до системи пред'являють вимоги повної автономності, без обслуговування. Останній варіант особливо корисний там, де крім стільникового зв'язку немає більше ніяких каналів передачі інформації, а до користувача і обладнання для запису можуть бути багато сотень кілометрів, в цьому випадку архів відеозапису буде знаходитися не на об'єкті, а у користувача в захищеному і надійному місці, то зловмисники не зможуть знищити архів, який буде доказом злочину [11].

Часто системи відеоспостереження використовуються і для дому, де виникає необхідність передавати певну інформацію до власника. Передача здійснюється за допомогою GSM модулю, Bluetooth, Wi-Fi та ін. Тип модуля визначається відстанню на яку потрібно передавати певну інформацію.

3.2 Опис протоколів GSM, 3G, 4G

3.2.1 Побудова і робота мережі

При здійсненні дзвінка або отримання дзвінка, телефон абонента встановлює з'єднання по радіоканалу з однією з антен прилеглої базової станції (BS - Base Station). У систему стільникового зв'язку GSM входить набір базових станцій, кожна з яких може включати в себе 1-12 приймально-передавальних антен. Для забезпечення якісного зв'язку в радіусі своєї дії антени мають різнобічну спрямованість. Антени представляють собою прямокутні конструкції, які можна

побачити на спеціальних щоглах або на даху висотних будівель. Такі антени приймають сигнали і передають їх по спеціальному кабелю в керуючий блок BS. Базова станція являє собою сукупність антен і керуючого блоку. Існують території, які можуть обслуговуватися відразу декількома базовими станціями, підключеними до контролера локальної зони (LAC). Один контролер може об'єднувати до 15 базових станцій на певній території. Контролери локальної зони комутуються з Центром управління мобільними послугами (MSC, «комутатор»), який, в свою чергу, має вхідні і вихідні з'єднання з будь-якими чинними видами стільникового і дротового зв'язку. Регіональні стільникові мережі стандарту GSM можуть використовувати всього один центр управління послугами мобільного зв'язку. У той же час, великі оператори мобільного зв'язку, які мають кілька мільйонів абонентів, використовують кілька об'єднаних між собою центрів MSC. Архітектура мережі GSM наведена на Рисунку 3.2.

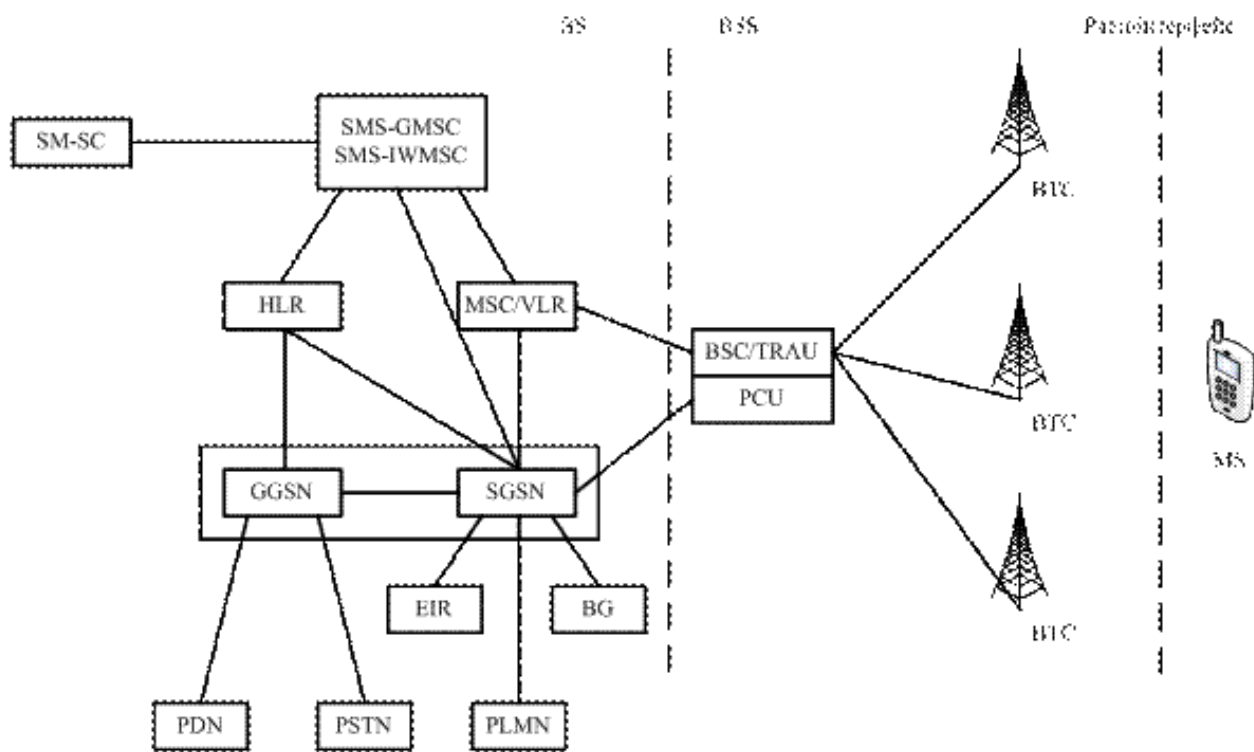


Рисунок 3.2 – Архітектура мережі GSM

3.2.2 Характеристики протоколу

Щоб зрозуміти ієрархію настільки складної системи, необхідно використовувати значення технічного терміну handover (хендовер), який позначає функцію передачі обслуговування абонента в стільникових мережах з естафетного принципом. Це означає, що якщо клієнт переміщається по вулиці і одночасно розмовляє по телефону, то для збереження безперервності розмови необхідно здійснювати своєчасне перемикання телефону абонента з одного сектора (стільника) базової станції в інший, а також зі сфери контролю однієї BS або LAC в іншу і т.д. Тому, якби використовувалося пряме підключення секторів базових станцій до комутатора, то, незважаючи на велику кількість інших завдань, останньому довелося б самотійно здійснювати процедуру хендовера для всіх існуючих абонентів. Для забезпечення рівномірного завантаження устаткування і зниження ймовірності його відмов від перевантажень, схема організації мобільних мереж GSM побудована за багаторівневим принципом. Іншими словами, при переміщенні абонента із зони дії одного сектора базової станції в зону дії іншого, перемикання здійснює блок управління даної BS, при цьому «вищі» по ієрархії пристрої LAC або MSC не задіяні. Аналогічно, при хендовері між різними базовими станціями, працює вже LAC і т. Д.

Комутатор виконують ті ж функції, що і АТС в провідних мережах, і є головним керуючим пристроєм мереж GSM. Центр послуг мобільного зв'язку визначає адресатів дзвінка, регулює функціонування додаткових послуг і безпосередньо вирішує, чи має абонент право на здійснення дзвінка в даний момент часу.

На SIM-карті, яка розташовується в телефоні абонента, знаходиться спеціальний номер IMSI (International Subscriber Identification Number), що означає

«Міжнародний розпізнавальний номер абонента». IMSI є унікальним номером для всіх існуючих мобільних мереж у всьому світі, за яким мобільні оператори однозначно ідентифікують абонентів. У момент натискання кнопки живлення телефону він відправляє код IMSI на базову станцію, яка, в свою чергу, передає його спочатку на LAC, а той ще далі по ієрархії на комутатор. При цьому в процесі беруть участь ще два додаткових пристрої - HLR і VLR, які пов'язані безпосередньо з комутатором. HLR позначає «Регістр домашніх абонентів» і зберігає коди IMSI всіх абонентів власної мережі, а VLR («Регістр гостей абонентів») містить інформацію про всіх абонентів, які використовують мережу цього мобільного оператора в конкретний момент часу.

При передачі коду IMSI в HLR використовується система шифрування, яку забезпечує Центр аутентифікації. Спочатку HLR перевіряє наявність у своїй базі абонента з даним номером, а в разі наявності - чи має абонент право на користування послугами мережі в даний момент, або ж, наприклад, в даний момент має фінансову блокування. Якщо перевірка закінчилася позитивно для абонента, його номер перенаправляється в VLR, після чого клієнт може здійснювати дзвінки або користуватися іншими послугами стільникового зв'язку [12].

3.2.3 Відмінності 3G, 4G відеоспостереження від GSM

3G і 4G відеоспостереження керується тими ж принципами, що і GSM: відеоспостереження, яке не залежить від прокладки кабелю, щоб в разі тривоги інформацію про пригоду можна було передати миттєво. Істотних відмінностей не багато.

На відміну від GSM-відеоспостереження, де пристрій виходить на зв'язок тільки в разі тривоги, 3G і 4G відеоспостереження знаходиться на зв'язку завжди, в будь-який момент можливо подивитися на об'єкт спостереження.

Якщо говорити про логіку роботи всієї системи, то користування мобільним інтернетом ближче до використання стандартного інтернет-підключення, ніж до використання GSM-мереж.

Якщо GSM-відеоспостереження часто вимагає використання охоронної сигналізації з підтримкою GSM (асортимент камер з GSM невеликий), то для використання мобільного інтернету можна брати будь-який роутер, що працює з USB-модемами, або зв'язку з 3G / 4G роутерами будь-якого мобільного провайдера з підтримкою WiFi і WiFi-камери [13].

3.2.4 GSM модуль для систем безпеки

У GSM модуль вставляється SIM карта оператора стільникового зв'язку з підключеним «інтернет» тарифом, основною умовою є щоб цей тариф включав в себе надання абоненту фіксованого IP адреси. Вся інформація транслюється GSM пристроєм на інтернет сервіс підтримує це обладнання, а користувач, в свою чергу через інтернет за допомогою цього сервісу керує всією системою і отримує на свій комп'ютер картинки, і відео з об'єкта. Приклад GSM модуля показано на Рисунку 3.3 [14].



Рисунок 3.3 – Приклад GSM-модуля. SIM900

Особливості GSM-модуля:

- Підвищена ефективність спектру.
- Міжнародний роумінг.
- Сумісність із цифровою мережею інтегрованих служб (ISDN).
- Підтримка нових послуг.
- Керування SIM-книгою.
- Номер фіксованого набору (FDN).
- Годинник у режимі реального часу з керуванням сигналом тривоги.
- Для телефонних дзвінків використовується шифрування.
- Служба короткого повідомлення (SMS) [15].

3.3 Опис технології Wi-Fi

3.3.1 Конфігурації і робота мережі

WiFi - це універсальна технологія бездротових мереж, яка використовує радіочастоти для передачі даних. WiFi дозволяє високошвидкісне підключення до Інтернету без використання кабелів.

Wi-Fi - це стандартний спосіб підключення комп'ютерів до бездротових мереж. Майже всі сучасні комп'ютери підтримують технологію Wi-Fi, що дозволяє користувачам знаходити та підключатися до бездротових маршрутизаторів. Більшість мобільних пристроїв, систем відеоігор та інших автономних пристроїв також підтримують Wi-Fi, що дозволяє їм також підключатися до бездротових мереж. Коли пристрій встановлює з'єднання Wi-Fi з маршрутизатором, він може спілкуватися з маршрутизатором та іншими пристроями в мережі. Однак маршрутизатор повинен бути підключений до Інтернету (через DSL або кабельний

модем), щоб забезпечити доступ до Інтернету до підключених пристроїв. Тому можливе підключення до Wi-Fi, але немає доступу до Інтернету.



Рисунок 3.4 – Приклад побудови Wi-Fi мережі

Більшість точок бездротового доступу та бездротових маршрутизаторів теоретично можуть мати 255 підключених пристроїв одночасно (Рисунок 3.4). Це багато комп'ютерів, смартфонів, планшетів, камер та інших пристроїв і, ймовірно, значно перевищує потреби типового будинку.

Потрібно зауважити, що кожен комп'ютер або пристрій, який додано до мережі, зменшить пропускну здатність, доступну для інших пристроїв, використовуючи те саме підключення до Інтернету. Це тому, що всі ці пристрої діляться не лише однією і тією ж бездротовою мережею, але вони також

обмінюються тим самим підключенням до Інтернету від постачальника послуг широкосмугового зв'язку. У цьому випадку вузьке місце не обов'язково пов'язане з бездротовими з'єднаннями, а саме з кількістю трафіку або пропускної здатності, яка може пройти через Інтернет-маршрутизатор до постачальника послуг широкосмугового зв'язку [16].

Оскільки Wi-Fi є стандартом бездротових мереж, будь-який пристрій із бездротовою картою "Сертифікований Wi-Fi" повинен бути розпізнаний будь-якою точкою доступу "Сертифіковано Wi-Fi", і навпаки. Однак бездротові маршрутизатори можуть бути налаштовані так, щоб вони працювали лише з певним стандартом 802.11, що може перешкоджати спілкуванню старшого обладнання з маршрутизатором. Наприклад, маршрутизатор 802.11n може бути налаштований на роботу лише з пристроями 802.11n. Якщо вибрати цей параметр, пристрої з мікросхемами 802.11g Wi-Fi не зможуть підключитися до маршрутизатора, навіть якщо вони мають сертифікат Wi-Fi. Мережі WiFi працюють у неліцензованих 2,4 радіодіапазонах із швидкістю передачі даних 11 Мбіт / с (802.11b) або 54 Мбіт / с (802.11a) відповідно [17].

3.3.2 Технічні характеристики

Wi-Fi - це технологія бездротової мережі, яка дозволяє комп'ютерам та іншим пристроям спілкуватися по бездротовому сигналу. Він описує мережеві компоненти, що базуються на одному із стандартів 802.11, розроблених IEEE та прийнятих Wi-Fi Alliance. Приклади стандартів Wi-Fi в хронологічному порядку включають:

IEEE 802.11a

Створена в 1999 році, ця версія Wi-Fi працює в діапазоні 5 ГГц. Це було зроблено з надією зустрітися з меншими перешкодами, оскільки багато пристроїв

(як і більшість бездротових телефонів) також використовують діапазон 2,4 ГГц. 802.11a також досить швидкий, максимальна швидкість передачі даних перевищує 54 Мбіт / с. Однак частота 5 ГГц має більше труднощів з об'єктами, які перебувають на шляху сигналу, тому діапазон часто поганий.

IEEE 802.11b

Також у 1999 р. Цей стандарт використовує більш типовий діапазон 2,4 ГГц і може досягти максимальної швидкості 11 Мбіт / с. 802.11b був стандартом, який розпочав популярність Wi-Fi.

IEEE 802.11g

Розроблений в 2003 році, стандарт 802.11g збільшив максимальну швидкість передачі даних до 54 Мбіт / с, зберігаючи при цьому використання надійного діапазону 2,4 ГГц. Це призвело до широкого прийняття стандарту.

IEEE 802.11n

Введена в 2009 році, ця версія мала повільне початкове прийняття. 802.11n працює як на 2,4 ГГц, так і на 5 ГГц, а також підтримує багатоканальне використання. Кожен канал пропонує максимальну швидкість передачі даних 150 Мбіт / с, що означає, що максимальна швидкість передачі даних стандарту - 600 Мбіт / с.

IEEE 802.11ac

Стандарт змінного струму - це те, що ви знайдете більшість бездротових пристроїв, якими користуєтесь під час написання. Спочатку випущений у 2014 році, AC різко збільшує пропускну здатність даних для пристроїв Wi-Fi до максимальної кількості 1300 мегабіт в секунду. Крім того, ac додає підтримку MU-

MIMO, додаткові канали Wi-Fi широкомовної передачі для діапазону 5 ГГц та підтримку більшої кількості антен на одному маршрутизаторі.

IEEE 802.11ax

Наступним кроком для маршрутизатора та бездротових пристроїв є стандарт «ax». Коли ax завершить свою розробку, ви отримаєте доступ до теоретичної пропускної здатності мережі 10 Гбіт / с - приблизно на 30-40 відсотків в порівнянні зі стандартом змінного струму. Крім того, бездротова «ax» збільшить пропускну спроможність мережі за рахунок додавання трансляцій підканалів, модернізації MU-MIMO та дозволу більше одночасних потоків даних [18].

Порівняльна характеристики наведено в Таблиці 3.1.

Таблиця 3.1 - Приклади стандартів Wi-Fi

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

3.3.3 Wi-Fi для систем безпеки

WiFi - найпоширеніша і затребувана технологія для організації бездротових мереж. За допомогою WiFi обладнання можна легко зробити бездротове відеоспостереження.

WiFi безпроводне відеоспостереження використовує 2,4 ГГц діапазон. Щоб організувати систему знадобляться:

- роутер;

- ір телекамери з вбудованим WiFi приймально / передавачем, або провідні телекамери, які підключаються до точки доступу для подальшої бездротової передачі даних;
- ноутбук, стаціонарний комп'ютер, або мобільний телефон.

3.4 Опис технології Bluetooth

3.4.1 Призначення, конфігурації і робота мережі

Bluetooth - специфікація для бездротових персональних мереж. Спочатку цей стандарт забезпечував обмін даними між мобільними телефонами, комп'ютерами, принтерами, цифровими фотоапаратами, на його основі роблять також бездротове відеоспостереження (Рисунок 3.6).



Рисунок 3.6 – Керування домашніми пристроями за допомогою Bluetooth

Спочатку все Bluetooth-пристрої знаходяться в режимі Standby, в якому вони кожні 1,28 секунди прослуховують 32 фіксовані частоти. Пристрій, опинившись в незнайомому оточенні, починає посилати запити на цих частотах.

При прийомі запиту Bluetooth-пристрій реагує на нього відповідно до режиму, в якому воно знаходиться. У режимі відгуку (discoverable mode) пристрій завжди відповідає на всі отримані запити. Режим обмеженого відгуку (limited discoverable mode) має на увазі, що пристрій може відповідати на запити лише обмежений час або при інших певних умовах. Третій режим, відмови у відгуку (non-discoverable mode), забороняє пристрою відповідати на запит.

Крім того, при підключенні пристрій може бути тим, що підключається (connectable mode) або недоступним (non-connectable mode). У другому випадку пристрій не зможе налаштувати ряд параметрів з'єднання і обмінюватися даними.

Після взаємного виявлення пристрою визначають використовуваний діапазон частот, розмір сторінок, кількість і порядок зміни частот і інші фізичні параметри з'єднання.

Кожне Bluetooth-пристрій має глобальний унікальний адресу (аналог MAC-адрес у мережевих плат), але на рівні користувача зазвичай використовується ім'я пристрою, який може бути будь-яким і не бути унікальним. Ім'я може бути завдовжки до 248 байт і використовувати кодову сторінку відповідно до Unicode UTF-8.

Bluetooth-пристрої можуть встановлювати з'єднання не тільки типу точка-точка, але, що і є важливо, багатоточкові з'єднання. При цьому вони об'єднуються в пікомережі. Процедура з'єднання ініціюється одним, причому будь-яким, з пристроїв, який і стає головним (master) в пікомережі. При цьому в одній пікомережі може бути не більше семи ведених (slave) пристроїв.

3.4.2 Технічні характеристики мережі

Для роботи радіоінтерфейсу Bluetooth використовується так званий нижній (2,45 ГГц) діапазон ISM (Industrial, Scientific, Medical), призначений для роботи промислових, наукових і медичних приладів. Особливістю даного діапазону є те, що майже у всіх країнах світу, він вільний від ліцензування, тобто для використання сертифікованого передавального обладнання, що працює на цих частотах, не потрібне додаткове дозвіл.

Швидкість каналу для Bluetooth-пристроїв становить 723,2 Кбіт/с в асинхронному режимі або 433,9 Кбіт/с в повністю синхронному режимі. Через Bluetooth-з'єднання можна передавати аудіоінформацію - через 3 канали по 64 Кбіт/с кожен, в разі, якщо не передаються інші дані. Можлива і комбінована передача даних і голосу [19].

3.5 Порівняння способів передачі в системах відеоспостереження

WI-FI системи більш надійні, ніж аналогові і можуть застосовуватися в сучасних охоронних системах відеоспостереження. Переваги такої системи є відсутність сигнальних проводів, можливість передачі відео на дуже великі відстані. Недоліками являється дороге обладнання, можливість зникнення, завмирання відеосигналу, обмежена швидкість передачі (обумовлена обмеженою шириною каналу), і найголовніше - необхідність прямої видимості між передавальною і приймальною стороною.

Використовувати мережі стільникових операторів, в т.ч. і мережі третього покоління 3G, для передачі відеосигналу на сьогодні найвигідніше. Вставляємо в камеру SIM карту, подаємо на неї харчування - і вона готова до використання і

перегляду відео з будь-якої точки нашої планети. І це дуже перспективна тема, тому що ширина каналів постійно збільшується, а вартість обладнання знижується. Немає необхідності прокладати сигнальні дроти, доступ до відеоінформації з будь-якої точки світу, повсюдне використання, навіть там, де немає Інтернету [20].

Перевага Bluetooth тільки в тому, що він має найменше енергоспоживання, але підходить тільки в тому випадку, якщо сигнал потрібно передавати в межах об'єкту. Тому використовувати Bluetooth в системах безпеки не завжди оправдано.

Таблиця 3.2 – Порівняльна характеристика способів передачі в системах відеоспостереження

Параметр модуля	GSM	Wi-Fi	Bluetooth
Приклад модуля	GSM SIM800c	Wi-Fi ESP8266	BK8000L
Призначення	Стільниковий зв'язок	Місцеві мережі	Bluetooth-з'єднання
Відстань дії	Сотні км	100м	10м
Швидкість передачі даних	2 Мбіт/с в системі 3G	до 150 Мбіт/с	723,2 Кбіт / с

В Таблиця 3.2 наведено порівняльні характеристики бездротових мереж. Проаналізувавши параметри модулів передачі інформації, врахувавши всі переваги та недоліки, впливає те що найбільш кращий варіант є GSM, його переваги в тому що радіус дії майже безмежний, все залежить тільки від покриття стільникового зв'язку, користувачу не потрібно мати спеціальний додаток. Wi-Fi має найбільшу

швидкість, але інформацію можливо передавати тільки в тому випадку якщо користувач має покриття та спеціальний додаток.

Висновки до розділу 3

Висока швидкість передачі даних, стабільність і захищеність каналу зв'язку для організації бездротового відеоспостереження забезпечує Wi-Fi.

GSM. При своїх численних недоліках це єдина з перелічених систем, яка дозволяє віддалено стежити за об'єктом, що охороняється за допомогою мобільних GSM пристроїв, оперативно видає «в перші руки» сигнали тривоги через електронну пошту, MMS та SMS повідомлення. Це єдина з бездротових систем, яка буде постійно на контролі у користувача, де б він не знаходився в межах мережі GSM.

Bluetooth не набув широко застосування в системах безпеки через неспроможність дії на велику відстань та малу швидкість.

Враховуючи все вище наведене, найкраще всього вибрати GSM-модуль та Wi-Fi з'єднання.

4 СИСТЕМА ВІДЕОПОСТЕРЕЖЕННЯ З ФУНКЦІЄЮ РОЗПІЗНАВАННЯ ТА З ДВОМА КАНАЛАМИ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

4.1 Основні характеристики системи

Враховуючи переваги функції розпізнавання обличчя і переваги технології GSM та Wi-Fi, запропоновано систему відеоспостереження, яка має функції розпізнавання «свій-чужий» та канал передачі даних, що додає можливості ідентифікації та розширює можливості передачі інформації. Така система відеоспостереження дозволить забезпечити кращий захисту того чи іншого об'єкту. Застосування запропонованої системи безпеки можливе в об'єктах, де потрібна система допуску.

Система забезпечує:

- контроль доступу за допомогою розпізнавання осіб.
- відправку смс-повідомлень через GSM-модуль, коли система не ідентифікує особу та у режимі налаштувань.
- підключення безконтактних датчиків за допомогою Bluetooth (опціонально).
- відеоспостереження через камеру та передачі прямої трансляції через Wi-Fi.
- можливість зберігання даних на SD-карті.

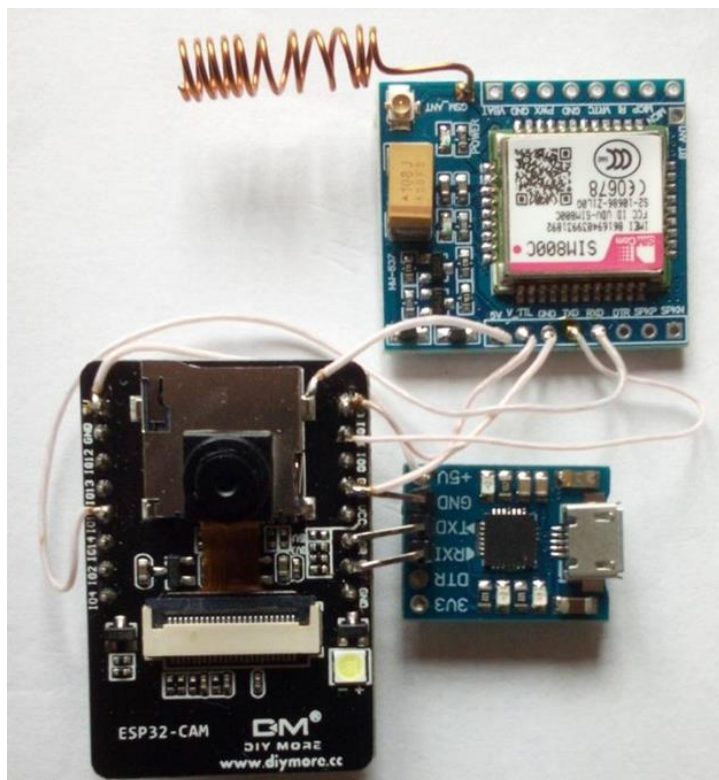


Рисунок 4.1 – Зовнішній вигляд системи

Система, яка представлена на Рисунку 4.1, працює наступним чином. Наприклад, у приміщенні встановлена така система відеоспостереження та доступ є тільки в трьох людей. В пам'яті уже записані їх обличчя. Коли до камери наближається людина, система ідентифікує її та зрівнює з уже збереженими даними про осіб, яким доступ є. Якщо співпадіння немає, то через GSM-модуль передається повідомлення про проникнення на об'єкт та посиленням на IP-адресу вбудованого сервера, з якого виконується відеотрансляція з даного приміщення.

Переваги системи:

- можлива на будь-якому об'єкті або будинку,
- не потребує великих матеріальних затрат на установку або підтримання системи,
- захистить будинок або будь-яку інформацію.

4.2 Блок-схема системи відеоспостереження та схема підключення

Система складається з мікропроцесорної плати ESP32-CAM, з вбудованими технологіями Wi-Fi та Bluetooth, модулю GSM, відеокамери та блоку живлення. Блок-схема системи наведена на Рисунок. 4.2.

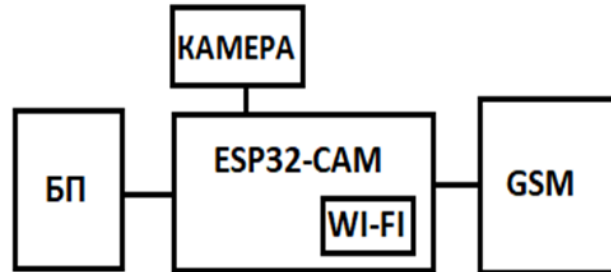


Рисунок 4.2 - Блок-схема запропонованої системи відеоспостереження

4.3 Алгоритм роботи системи

Алгоритм роботи запропонованої системи представлений на Рис. 4.3:

1. Запуск програми.
2. Перевірка підключення до Wi-Fi.
3. Модуль ESP32-CAM зчитує інформацію з камери, потім передає картинку до інтернету на вказану IP-адресу.
4. Камера зчитує дані, і якщо знаходить обличчя, то сканує його на відповідність до створеної бази даних.
5. Якщо співпадіння є, то система переходить до начального стану пошуку обличчя.
6. Якщо співпадіння нема, то система передає екстрене повідомлення власнику на телефон з посилання на вказану IP-адресу.

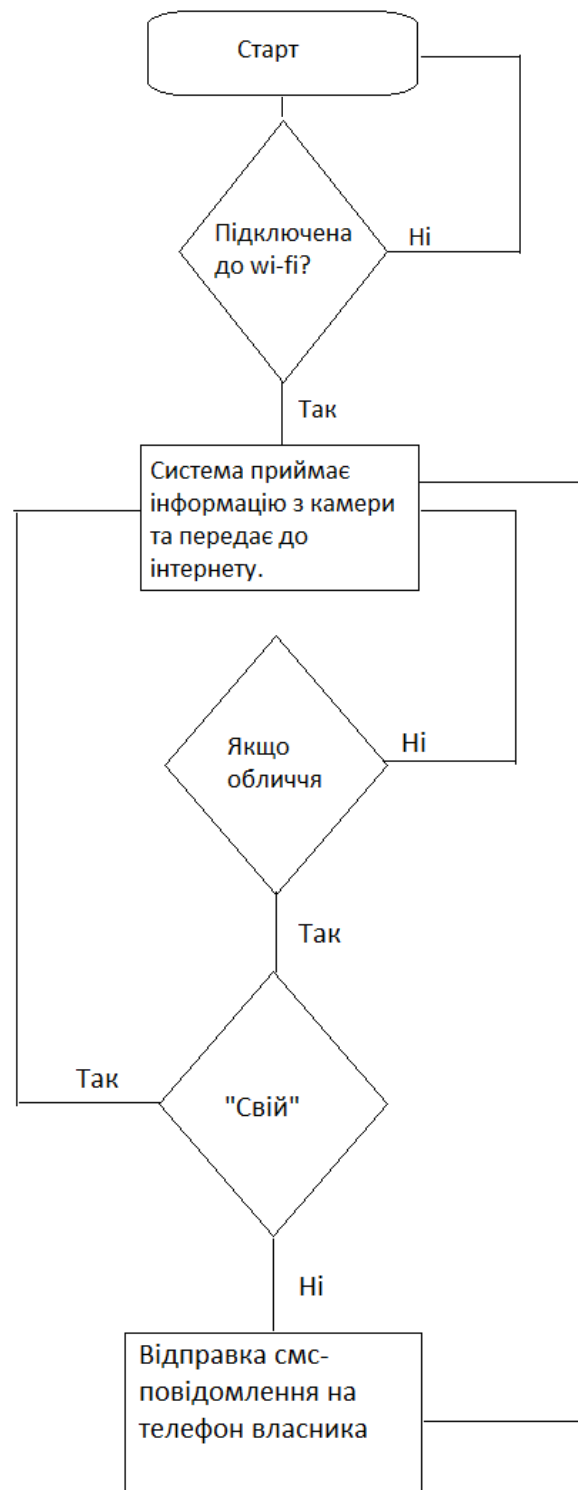


Рисунок 4.3 Алгоритм роботи запропонованої системи

4.4 Опис окремих складових системи відеоспостереження

4.4.1 Опис модуля ESP32

ESP32-CAM - це модуль для підключення камери з чіпом ESP32-S, який коштує приблизно 10 доларів. Окрім камери OV2640 та декількох GPIO для підключення периферійних пристроїв, вона також має роз'єм для карт microSD, який може бути корисним для зберігання зображень, зроблених за допомогою камери, або для зберігання файлів.

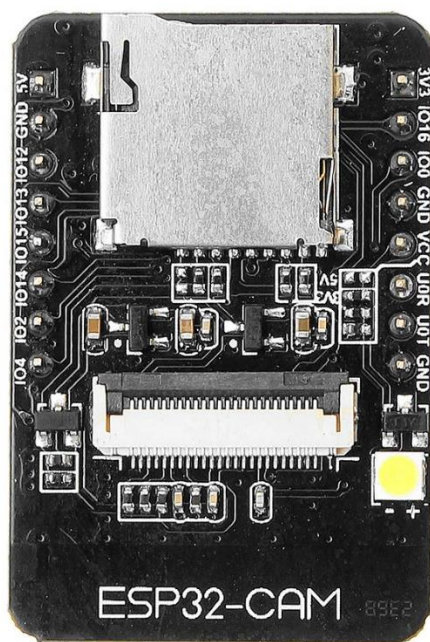


Рисунок 4.4 Зовнішній вигляд ESP32-CAM

Технічні характеристики плати ESP32-CAM зображеної на Рисунку 4.4:

- Модуль бездротового зв'язку - модуль ESP32-S WiFi 802.11 b/g/n + Bluetooth 4.2 LE з PCB антеною, роз'єм u.FL, 32 Мбіт SPI флеш-пам'ять, 4 Мбіт PSRAM.
- Вбудоване сховище – слот для мікро SD-карти до 4 Гб.

- Формат зображення – JPEG (підтримує тільки OV2640), BMP, відтінки сірого.
- Світлодіодний спалах.
- Споживана потужність:
- Deep-sleep – 6 мА @ 5 В мінімум.
- Modem-sleep – 20 мА @ 5 В мінімум.
- Розмір – 40.5x27x4.5 мм.
- Діапазон температур – робочий: від -20°C до ~85°C; зберігання: від -40°C до ~90°C @ відносна вологість <90%.

4.4.2 Опис камери OV2640



Рисунок 4.5 – Камера OV2640

Технічні характеристики камери OV2640 (Рисунок 4.5) плати ESP32-CAM:

- Фоточутливий масив: 640x480.
- ІО напруга: 1,7-3,0 В.

- Енергоспоживання: 60 мВт/5 fpsVGA.
- Робоча температура: -30°C ~ 70°C.
- Оптичний Розмір: 1/6".
- Поле зору: 25°.
- Максимальна частота кадрів: 30 fpsVGA.
- Чутливість: 1,3 В/(люкс-сек).
- Відношення сигнал-шум: 46 дБ.
- Динамічний діапазон: 52 дБ.
- Область пікселів: 3,6 мкмх3,6 мкм.

4.4.3 Опис GSM модуля SIM800с

GSM SIM800C - це повнофункціональний модуль з чотирьохдіапазонним (Quad-Band) GSM / GPRS режимом і підтримкою інтерфейсу Bluetooth 3.0. Стандартний інтерфейс управління модуля SIM800C надає доступ до сервісів мереж GSM / GPRS 850/900/1800 / 1900МГц для здійснення голосових викликів, відправлення / прийому SMS повідомлень, обміну цифровими та факсимільними даними. Низький рівень споживання енергії, малий розмір, наявність Bluetooth і великий перелік додаткових нестандартних функцій дозволяють реалізувати цікаві прикладні M2M рішення.

GSM модуль, наведений на Рисунку 4.6, дозволяє передавати дані через звичайний стільниковий зв'язок іншим пристроям, зазвичай це мобільний телефон, який на сьогоднішній день є у кожної людини. Перевага в тому що можлива швидка телефонізація стаціонарних об'єктів, до яких важко або економічно

недоцільно підводити дріт'яні комунікації або з метою заміни провідних телефонних комунікацій для економії фінансових витрат на послуги зв'язку.



Рисунок 4.6 - Модуль GSM SIM800c

Характеристики:

- робота в мережах: 850/900/1800/1900 МГц,
- клас GPRS B multi-slot 12/10,
- відповідність GSM phase 2/2 +,
- клас потужності 4 (2 Вт @ 850/900 МГц),
- клас потужності 1 (1 Вт @ 1800/1900 МГц),
- стандарт Bluetooth: 3.0,
- інтерфейси 2xUART, USB, Bluetooth, GPIO, ADC,
- управління АТ командами,
- діапазон напруги живлення: 3,4 ~ 4,4 В,
- розміри: 15,7 x 17,6 x 2,3 мм,
- робочий діапазон температур: -40 °C ~ 85 °C [21].

4.4.4 Програмування і передача IP адреси користувачу

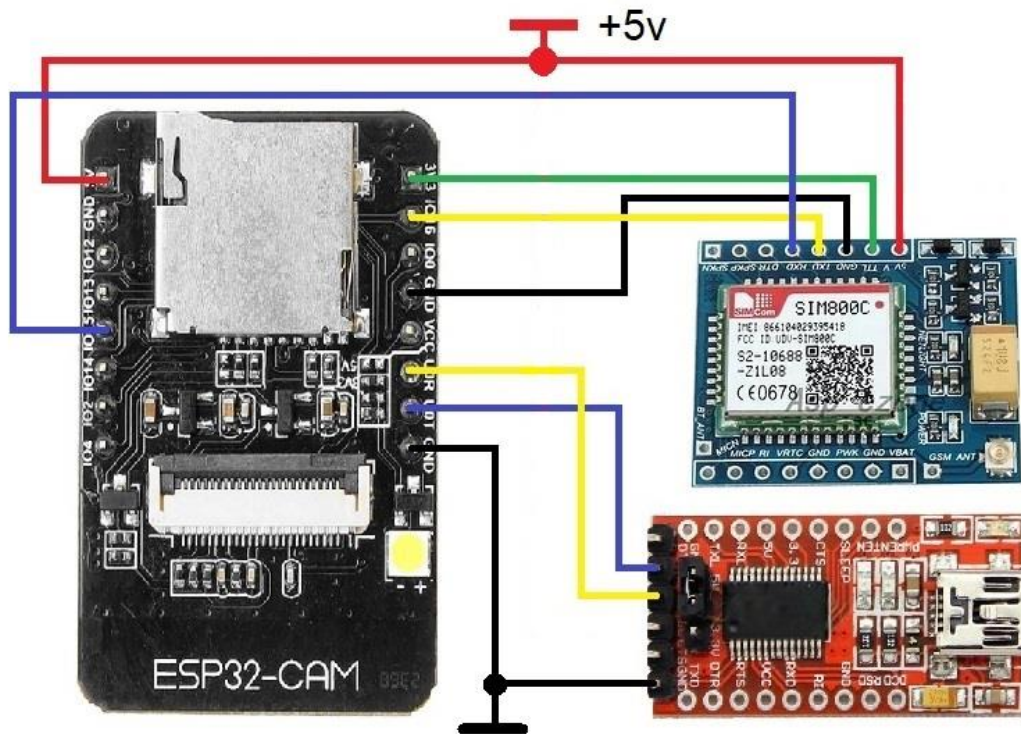


Рисунок 4.7 – Схема підключення модулів

Підключення модулів до ESP32-CAM зображено на Рисунок 4.7. Червоний і чорний провід - це живлення. Модуль дуже вимогливий до якості напруги живлення. Для модуля треба + 5V і мінімум 2 А. Синім і жовтим позначені два проводи передачі даних і підключення до Ардуіно.

Взаємодія модуля SIM800с з контроллером ESP32-CAM здійснюється за допомогою AT команд. AT команди складаються з серій коротких текстових рядків, які об'єднують разом, щоб сформувати повні команди операцій, таких як набір номера, початок з'єднання або зміна налаштувань, необхідних для передачі СМС. Основні AT команди, які використовуються в системі є:

✓ AT+CMGF=1. Відповідь: ОК. (Переводимо в текстовий режим відправки повідомлень).

✓ AT+CSCS=»GSM». Відповідь: ОК. (Встановити набір: 7-бітний алфавіт GSM «GSM» (3GPP TS 23.038); 16-розрядний універсальний багатоконтатний набір символів «UCS2» (ISO / IEC10646); Рядки символів UCS2 перетворюються в шістнадцяткові числа від 0000 до FFFF; напр. «004100620063» дорівнює трьом 16-бітовим символам з десятковими значеннями 65, 98 і 99 Міжнародний довідковий алфавіт «IRA» (ITU-T T.50) Символьні рядки «HEX» складаються лише з шістнадцяткових знаків від 00 до FF; Комплект символів «PCCP» Код «PCDN» Комплект символів датського / норвезького ПК «8859-1» ISO 8859 Латинський 1 набір символів).

✓ AT+CSCS? Відповідь:+CSCS: «GSM» (Провіряємо, що потрібна кодова таблиця представлена коректно).

✓ AT+CMGS=»+380xxxxxxxx» Відповідь:> (Номер телефону вводить обов'язково з +, після чого відправляється смс «ALARM» і власник розуміє, що біля об'єкту помічено рух, і може перейти на вказану ір-адресу та подивитися хто там) [22].

Розглянуті вище АТ команди реалізовано у вигляді наступного коду:

```
✓ sim800c.print("AT+CMGF=1\r"); // Вибір режиму SMS
✓ delay(100); // Пауза 100 мс
✓ sim800c.print("AT+CMGS=\"+38098*****\"\r"); // Набір номеру
✓ delay(100); // Пауза 100 мс
✓ sim800c.print("ALARM!"); // Передача SMS тривоги
✓ delay(100); // Пауза 100 мс
✓ sim800c.print((char)26); // (передача символу закінчення
    повідомлення
✓ delay(100); // Пауза 100 мс
```

Для програмування системи та передачі IP адреси користувачу плату ESP32-CAM підключають до комп'ютера за допомогою USB-TTL конвертера FTDI (Рисунок 4.8). Підключення виконується згідно схеми, наведеної нижче.

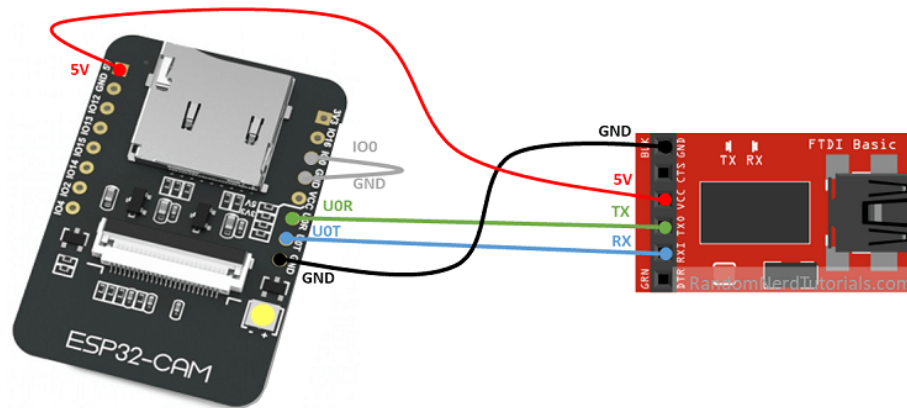


Рисунок 4.8 Схема підключення USB-TTL конвертера FTDI

Для задання імені Wi-Fi мережі, паролю доступу до неї та програмування системи в середовищі Arduino IDE потрібно зробити наступні дії:

- 1) Потрібно ввести свій логін та пароль для ідентифікації на веб-сервері (Рисунок 4.9).

```

CameraWebServer  app_httpd.cpp  camera_index.h  camera_pins.h
#include "esp_camera.h"
#include <WiFi.h>

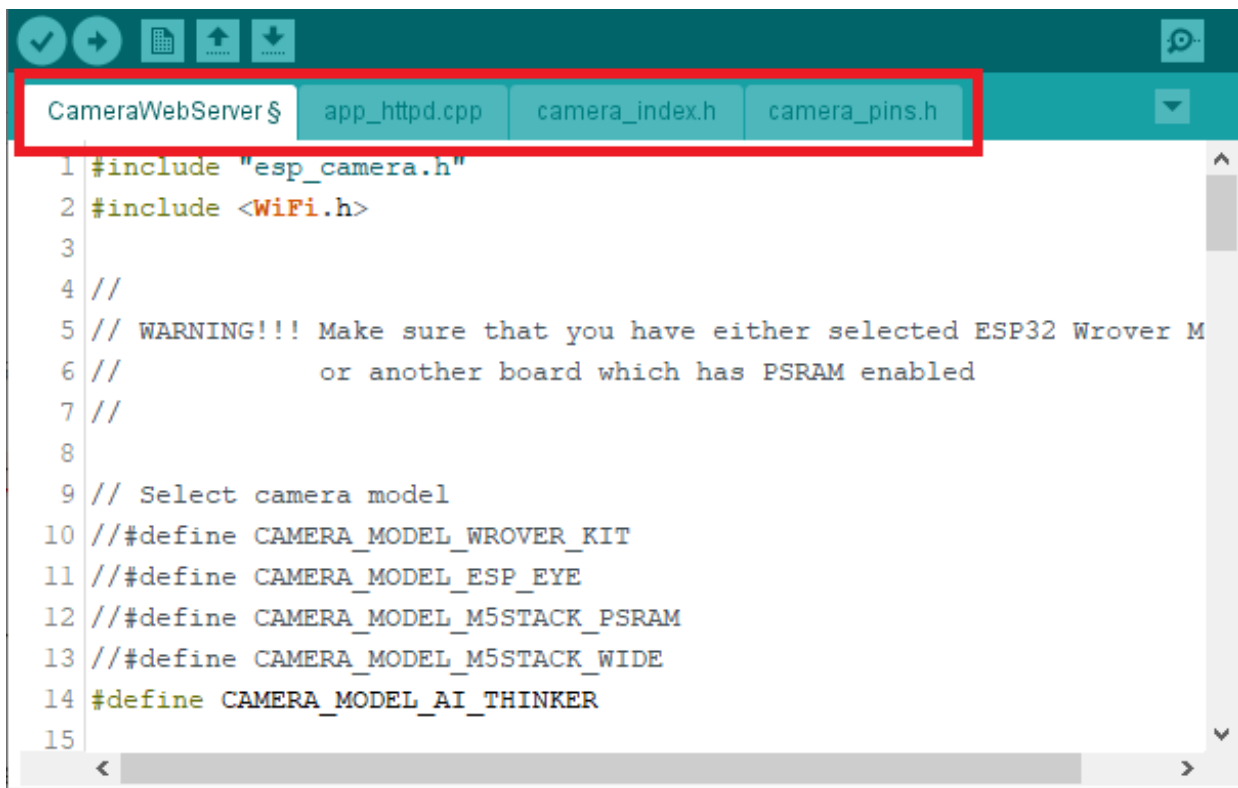
// Select camera model
#define CAMERA_MODEL_WROVER_KIT
// #define CAMERA_MODEL_ESP_EYE
// #define CAMERA_MODEL_M5STACK_PSRAM
// #define CAMERA_MODEL_M5STACK_WIDE
// #define CAMERA_MODEL_AI_THINKER

#include "camera_pins.h"
#include "AT_com.h"

const char* ssid = "*****";
const char* password = "*****";
  
```

Рисунок 4.9 – Поля для вводу логіну та паролю

- 2) Перейшовши до Інструменти> Плати потрібно вибрати AI-Thinker ESP32-CAM. Потрібно переконатися, що вибрано правильний модуль камери. У цьому випадку використовуємо модель AI-THINKER.
- 3) Перейшовши до Інструменти> Порт слід вибрати COM-порт, до якого підключений ESP32.
- 4) Потім потрібно натиснути кнопку завантаження, щоб завантажити код.
- 5) Коли видно точки у вікні налагодження, потрібно натиснути на борту кнопку RST ESP32-CAM.



The screenshot shows the Arduino IDE interface. At the top, there is a toolbar with icons for checking, running, uploading, and downloading. Below the toolbar, a red box highlights the project files: 'CameraWebServer \$', 'app_httpd.cpp', 'camera_index.h', and 'camera_pins.h'. The main code editor displays the following code:

```

1 #include "esp_camera.h"
2 #include <WiFi.h>
3
4 //
5 // WARNING!!! Make sure that you have either selected ESP32 Wrover M
6 //             or another board which has PSRAM enabled
7 //
8
9 // Select camera model
10 // #define CAMERA_MODEL_WROVER_KIT
11 // #define CAMERA_MODEL_ESP_EYE
12 // #define CAMERA_MODEL_M5STACK_PSRAM
13 // #define CAMERA_MODEL_M5STACK_WIDE
14 #define CAMERA_MODEL_AI_THINKER
15

```

Рисунок 4.10 – Основні файли програми у середовищі Arduino IDE

Щоб знайти IP-адресу системи (Рисунок 4.10), потрібно виконати наступні дії:

- Після завантаження коду потрібно відключити GPIO 0 від GND.

- Потім відкривши послідовний монітор зі швидкістю передачі даних у швидкості 115200, потрібно натиснути на кнопку RESET.
- Відкриється вікно с IP-адресою (Рисунок 4.11).

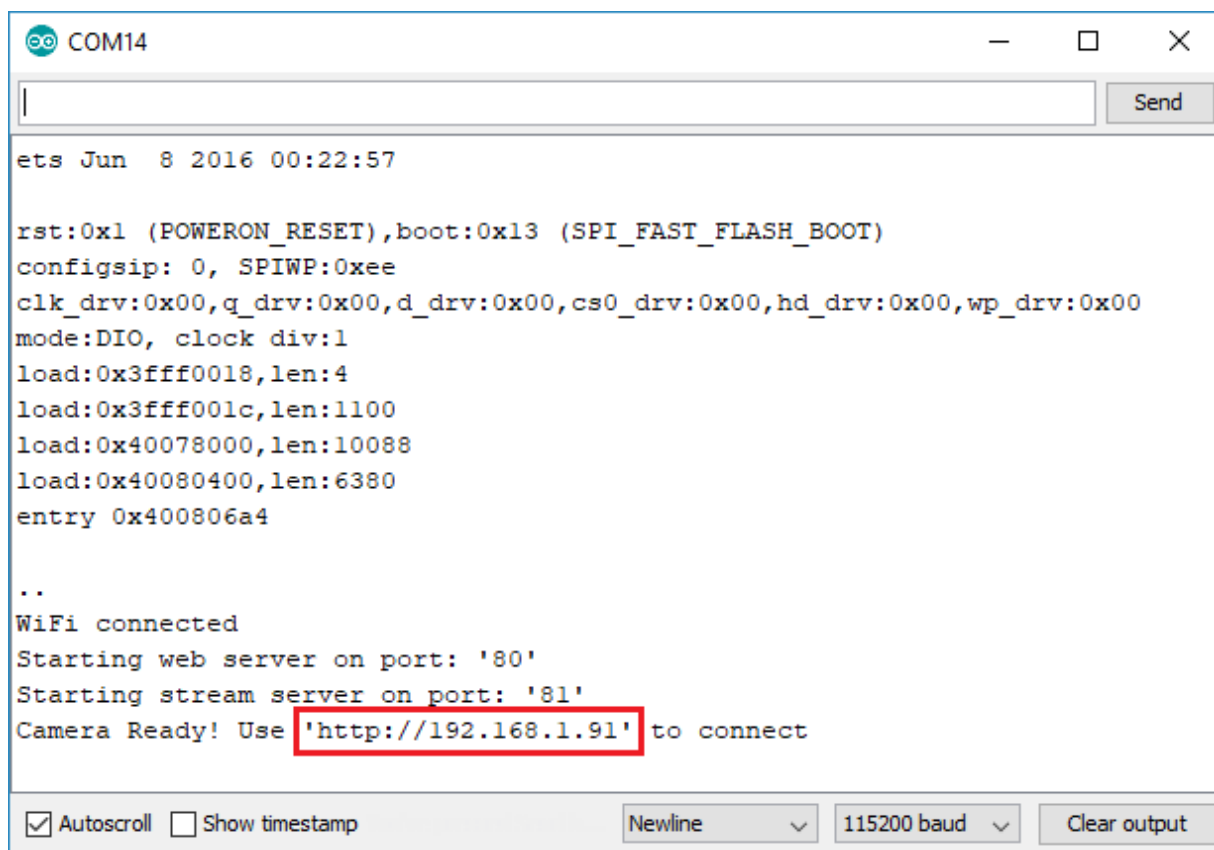


Рисунок 4.11 – Пошук IP-адреси

4.4.5 Опис програмного забезпечення

Програмне забезпечення системи написано для редагування у середовищі Arduino IDE і, відповідно, завантаження з нього в мікроконтролер ESP32-CAM. Код програми написано мовами «Processing» та C++ і зберігається у 4-х файлах: CameraWebServer.ino, app_httpd.cpp, camera_index.h, camera_pins.h. Файли запозичено в [xx], але модифіковано для забезпечення функціонування GSM модуля SIM800с. Нижче наведено короткий опис файлів з програмним забезпеченням.

- Основна програма знаходиться у файлі CameraWebServer.ino. У програмі виконується ініціалізація послідовних портів для взаємодії з комп'ютером та GSM модулем, ініціалізація Wi-Fi та завантаження Web-сервера, задіяних у роботі. Також програма виконує основний робочий цикл та взаємодіє з GSM модулем у випадку наявності неспівпадіння обличь.
- У файлі app_httpd.cpp зберігаються функції обробки відеоінформації, функції розпізнавання та порівняння обличь та функції забезпечення роботи Web-сервера.
- Файл camera_index.h зберігає Web-сторінку системи у бінарному вигляді.
- Файл зберігає налаштування для різних типів відеокамери.

Модифіковані файли CameraWebServer.ino та app_httpd.cpp наведено у додатку Б(?).

4.4.6 Опис інтерфейсу користувача

Інтерфейс пілотної версії програми використано з статті [23].

Програмна частина системи реалізована у вигляді Web-серверу, який зберігається у пам'яті контролера. Відкривши браузер і вписавши IP-адресу ESP32-CAM, після натиску кнопки Start, розпочинається трансляція передачі потокового відео. Також можливо зробити фотографії, натиснувши кнопку Get Still.

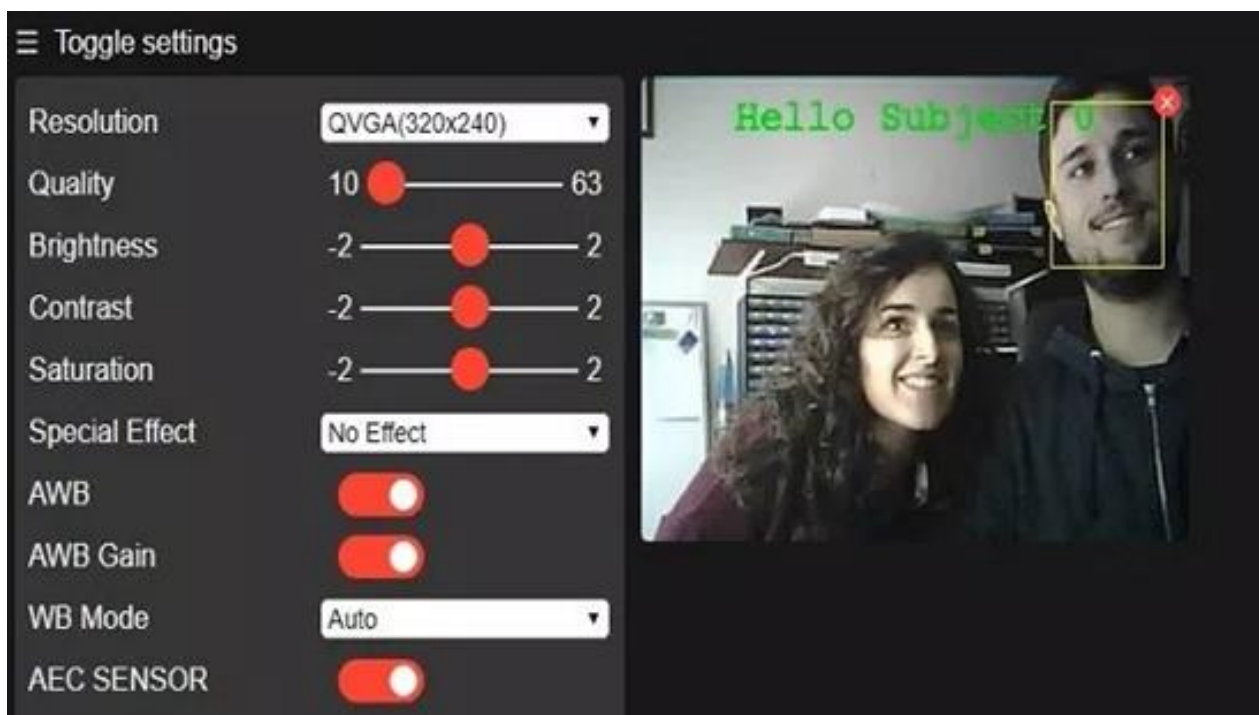


Рисунок 4.12 Ідентифікація программою «Свій»

Існує також кілька налаштувань камери, якими можна скористатися, щоб налаштувати параметри зображення: роздільна здатність, якість зображення, яскравість, контрастність та насичення. Вікно програми має екран для перегляду потокового відео коли веб-сервер запущений.

Функція розпізнавання та виявлення також обличчя може бути налаштована. Спочатку необхідно запам'ятати обличчя «своїх» користувачів, натиснувши відповідну кнопку. Зображення зберігаються на карті microSD.

Далі у процесі роботи коли у поле зору камери попадає обличчя, то воно ідентифікується. Якщо образ такого обличчя є у пам'яті, то на екрані з'являється напис привітання зеленим кольором, як на Рисунок 4.1. Якщо образу обличчя в пам'яті немає, то з'являється тривожний напис червоним кольором (Рисунок 4..13) і одночасно відправляється SMS на заданий номер.



Рисунок 4.13 Ідентифікація програмою «Чужий»

Висновки до розділу 4

Запропоновано систему відеоспостереження, яка має функції розпізнавання та канал передачі даних, що додає можливості ідентифікації та розширює можливості передачі інформації. Така система відеоспостереження дозволить забезпечити кращий захисту будь-якого об'єкту.

З використанням переваги функції розпізнавання обличчя і можливості технології GSM та Wi-Fi, введено додатковий канал для передачі повідомлень користувачу про виявлення сторонніх осіб та ідентифікація особи через сканування обличчя.

Програма реалізована у вигляді Web-серверу для зручного користування з будь-якого пристрою.

Переваги системи:

- контроль доступу за допомогою розпізнавання осіб.
- відправка смс-повідомлень через GSM-модуль, коли система не ідентифікує особу та у режимі налаштувань.
- відеоспостереження через камеру та передачі прямої трансляції через Wi-Fi.
- можливість зберігання даних на SD-карті.

ВИСНОВКИ

Системи відеоспостереження з функцією розпізнавання широко використовуються на сьогоднішній день. Вони призначені для отримання інформації про поточний стан об'єкту, що охороняється (технологічного процесу) шляхом збору, обробки, архівування, зберігання, відображення та аналізу цієї інформації.

В результаті аналізу сучасних автономних систем відеоспостереження запропоновано варіант системи в якому є додаткові функції. Система має два канали зв'язку задля кращого передавання інформації та можливість ідентифікації особи.

Для запропонованої системи вибрано саме ідентифікацію людини через сканування обличчя. Наразі такий спосіб ідентифікації використовується для контролю доступу в системах безпеки нарівні з іншими біометричними системами, такими як розпізнавання райдужної оболонки, відбитки пальців. Хоча точність системи розпізнавання обличчя як біометричної технології є нижчою, ніж розпізнавання райдужної оболонки ока та розпізнавання відбитків пальців, вона широко застосовується завдяки безконтактному та неінвазивному процесу. Існує багато методів, які використовуються в системах розпізнавання осіб, але в цілому вони ґрунтуються на порівнянні рис обличчя заданого зображення з обличчями, які зберігаються в базі даних.

Wi-Fi: серед переваг висока швидкість передачі даних, стабільність і захищеність каналу зв'язку; серед недоліків прив'язаність до IP-адреси.

GSM: серед переваг можливість віддалено стежити за об'єктом, що охороняється за допомогою мобільних GSM пристроїв, оперативно видає сигнали

тривоги через електронну пошту; серед недоліків те, що не всюди є покриття, але це спокійно можливо замінити на 3G та 4G.

Враховавши всі переваги та недоліки різних видів модулів передачі інформації, впливає те що для передачі сповіщень найбільш кращий варіант є GSM, так як його радіус дії майже безмежний. А відеопотік можна передавати як через GSM, так і по Wi-Fi.

Запропонована система може застосовуватися в офісах, закладах та в житлових будинках. ESP32-CAM пропонує недорогий спосіб побудови більш досконалих проектів домашньої автоматизації, які містять відео, фотографування та розпізнавання обличчя.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Advance Intelligent Video Surveillance System (AIVSS): A Future Aspect: веб-сайт. URL: <https://www.intechopen.com/books/intelligent-video-surveillance/advance-intelligent-video-surveillance-system-aivss-a-future-aspect> (дата звернення: 12.05.2020).
2. A. Ezzahout and R. O. Haj Thami, “Conception and development of a video surveillance system for detecting, tracking and profile analysis of a person,” in 2013 3rd International Symposium ISKO-Maghreb, 2013, pp. 1–5, DOI: 10.1109/ISKO-Maghreb.2013.6728128.
3. S. A. Atone, A. S. Bhalchandra, and P. H. Bhagat, “Moving Object Detection with an IP camera,” in 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), 2018, pp. 1–4, DOI: 10.1109/ICCONS.2018.8662963.
4. We are the Experts in IP Camera Systems: веб-сайт. URL: <https://kintronics.com/solutions/ip-camera-systems/> (дата звернення: 12.05.2020).
5. Remote Video Monitoring: веб-сайт. URL: <https://acadianmonitoringservices.com/video-monitoring/> (дата звернення: 12.05.2020).
6. A Gentle Introduction to Object Recognition With Deep Learning: веб-сайт. URL: <https://machinelearningmastery.com/object-recognition-with-deep-learning/> (дата звернення: 12.05.2020).
7. STREET-LEVEL SURVEILLANCE. Iris Recognition: веб-сайт. URL: <https://www.eff.org/pages/iris-recognition> (дата звернення: 17.05.2020).

8. What is Fingerprint Identification? : веб-сайт. URL: <https://www.biometricupdate.com/201205/what-is-fingerprint-identification> (дата звернення: 17.05.2020).

9. STREET-LEVEL SURVEILLANCE. Face Recognition: веб-сайт. URL: <https://www.eff.org/pages/face-recognition> (дата звернення: 17.05.2020).

10. Facial recognition video analytics: веб-сайт. URL: <https://clearview-communications.com/facial-recognition-video-analytics> (дата звернення: 17.05.2020).

11. The safe and reliable choice: веб-сайт. URL: https://www.milestonesys.com/solutions/platform/video-management-software/?gclid=CjwKCAjw5cL2BRASEiwAENqAPmHVY0g9lBXMUjmKCspACPKr8mwxjmJpHC2Ym7GTx5rpW6dV53b04BoCIw0QAvD_BwE (дата звернення: 17.05.2020).

12. Как работает сотовая сеть GSM: веб-сайт. URL: http://www.mobi-city.ru/articlereview/kak_rabotaet_gsm (дата звернення: 19.05.2020).

13. Что такое 3G, 4G видеонаблюдение? Чем оно отличается от GSM? : веб-сайт. URL: <https://hikvision.org.ua/ru/articles/что-такое-3g-4g-videonablyudenie-chem-ono-otlichaetsya-ot-gsm> (дата звернення: 19.05.2020).

14. Беспроводное видеонаблюдение на основе WiFi, WiMax, GSM, Bluetooth, FM модуляции: веб-сайт. URL: <http://podohranu.ru/besprovodnoe-videonablyudenie-na-osnove-WiFi-WiMax-GSM-Bluetooth-FM-moduljicii.html> (дата звернення: 19.05.2020).

15. GSM – Architecture, Features & Working: веб-сайт. URL: <https://www.elprocus.com/gsm-architecture-features-working/> (дата звернення: 19.05.2020).

16. How Many Devices Can Connect to my WiFi Network? : веб-сайт. URL: <https://www.engeniusnetworks.eu/faq-question/how-many-devices-can-connect-to-my-wifi-network/> (дата звернення: 21.05.2020).

17. Wi-Fi Definition: веб-сайт. URL: <https://techterms.com/definition/wi-fi> (дата звернення: 21.05.2020).

18. The Most Common Wi-Fi Standards and Types Explained: веб-сайт. URL: <https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/> (дата звернення: 21.05.2020).

19. Protocol specifications define the protocols that govern communication among devices on Bluetooth wireless networks: веб-сайт. URL: <https://www.bluetooth.com/specifications/protocol-specifications/> (дата звернення: 24.05.2020).

20. Video Transmission Methods: веб-сайт. URL: <https://www.videolinktv.com/technology/video-transmission-methods/> (дата звернення: 24.05.2020).

21. GSM SIM800C Module User Manual UDV-SIM800C _Rev 3 Shanghai Simcom: веб-сайт. URL: <https://arduinka.pro/commodule/gsm-sim800c/> (дата звернення: 25.05.2020).

22. Connection of GSM module SIM800C to ESP8266/ESP32/Arduino: веб-сайт. URL: <http://www.bizkit.ru/en/2019/02/05/13553/> (дата звернення: 25.05.2020).

23. ESP32-CAM Video Streaming and Face Recognition with Arduino IDE: веб-сайт. URL: <https://randomnerdtutorials.com/esp32-cam-video-streaming-face-recognition-arduino-ide/> (дата звернення: 27.05.2020).

ДОДАТОК А

Лістинг програми для пристрою

```

include "esp_camera.h"
#include <WiFi.h>

// Select camera model
#define CAMERA_MODEL_WROVER_KIT
// #define CAMERA_MODEL_ESP_EYE
// #define CAMERA_MODEL_M5STACK_PSRAM
// #define CAMERA_MODEL_M5STACK_WIDE
// #define CAMERA_MODEL_AI_THINKER
#include "camera_pins.h"

#define RX2 16      // RX for sim800c
#define TX2 15      // TX for sim800c

const char* ssid = "*****";
const char* password = "*****";
int matched_id;

HardwareSerial  sim800c(1); // Serial for sim800c

void startCameraServer();

void SendSMS()
{
    sim800c.print("AT+CMGF=1\r");      //Set the module to SMS mode

```

```

delay(100);
sim800c.print("AT+CMGS=\"+38098*****\"\\r"); // Phone number
delay(500);
sim800c.print("ALARM!"); //This is the text to send
delay(500);
sim800c.print((char)26); // End of the message
delay(500);
sim800c.println();
delay(500);
}

void setup() {
  Serial.begin(115200);
  Serial.setDebugOutput(true);
  Serial.println();
  sim800c.begin(115200, SERIAL_8N1, RX2, TX2); // sim800c begin

  camera_config_t config;
  config.ledc_channel = LEDC_CHANNEL_0;
  config.ledc_timer = LEDC_TIMER_0;
  config.pin_d0 = Y2_GPIO_NUM;
  config.pin_d1 = Y3_GPIO_NUM;
  config.pin_d2 = Y4_GPIO_NUM;
  config.pin_d3 = Y5_GPIO_NUM;
  config.pin_d4 = Y6_GPIO_NUM;
  config.pin_d5 = Y7_GPIO_NUM;
  config.pin_d6 = Y8_GPIO_NUM;
  config.pin_d7 = Y9_GPIO_NUM;

```

```

config.pin_xclk = XCLK_GPIO_NUM;
config.pin_pclk = PCLK_GPIO_NUM;
config.pin_vsync = VSYNC_GPIO_NUM;
config.pin_href = HREF_GPIO_NUM;
config.pin_sscb_sda = SIOD_GPIO_NUM;
config.pin_sscb_scl = SIOC_GPIO_NUM;
config.pin_pwdn = PWDN_GPIO_NUM;
config.pin_reset = RESET_GPIO_NUM;
config.xclk_freq_hz = 20000000;
config.pixel_format = PIXFORMAT_JPEG;
//init with high specs to pre-allocate larger buffers
if(psramFound()){
    config.frame_size = FRAMESIZE_UXGA;
    config.jpeg_quality = 10;
    config.fb_count = 2;
} else {
    config.frame_size = FRAMESIZE_SVGA;
    config.jpeg_quality = 12;
    config.fb_count = 1;
}

#ifdef CAMERA_MODEL_ESP_EYE
    pinMode(13, INPUT_PULLUP);
    pinMode(14, INPUT_PULLUP);
#endif

// camera init
esp_err_t err = esp_camera_init(&config);

```

```

if (err != ESP_OK) {
    Serial.printf("Camera init failed with error 0x%x", err);
    return;
}

sensor_t * s = esp_camera_sensor_get();
//initial sensors are flipped vertically and colors are a bit
saturated
if (s->id.PID == OV3660_PID) {
    s->set_vflip(s, 1); //flip it back
    s->set_brightness(s, 1); //up the blightness just a bit
    s->set_saturation(s, -2); //lower the saturation
}
//drop down frame size for higher initial frame rate
s->set_framesize(s, FRAMESIZE_QVGA);

#ifdef CAMERA_MODEL_M5STACK_WIDE
    s->set_vflip(s, 1);
    s->set_hmirror(s, 1);
#endif

WiFi.begin(ssid, password);

while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
}
Serial.println("");
Serial.println("WiFi connected");

```

```
startCameraServer();

Serial.print("Camera Ready! Use 'http://");
Serial.print(WiFi.localIP());
Serial.println("' to connect");
}

void loop() {
    delay(100);

    if(matched_id == -1)
    {
        matched_id = 0;
        SendSMS(); // send SMS using sim800c
    }
}
```

ДОДАТОК Б

SUMMARY

Video surveillance systems with the ability to transmit information are relevant today and are the most popular systems for security and monitoring purposes. The development of video surveillance systems opens up new opportunities not only for recording offenses, but, more importantly, for their prevention.

Therefore, these systems have become widely used. Recently, surveillance systems are becoming very popular. The government, organizations, housing associations, etc. use these systems to inspect various activities for security and safety.

Previously, surveillance systems were highly dependent on operators, but recently automated systems have been preferred due to better efficiency and reliability.

A video surveillance system is necessary to ensure the security of the facility. The presence of CCTV cameras or even signs warning of video surveillance in visible places prevents burglary.

A video surveillance system can also increase the safety of people working indoors. Regular maintenance will ensure the smooth operation of customer equipment throughout its life.

Human identification has long been widely used around the world, which has made it possible to improve security systems and law enforcement.

There are three main ways to recognize a person.

- It is possible to scan the iris from a distance or even in motion, which means that this data can be collected covertly, without the knowledge of people.

- Human fingerprint identification is popular because of its inherent ease of acquisition.
- Face recognition - just the beginning of the implementation of the recognition method. The human face is just one of the objects to be detected. Other objects can be identified in the same way. For example, it can be people's eyes and their fingers.

Video surveillance is an important part of the security system, where the most important additions are IP cameras and the recognition function. Surveillance cameras and human identification are important because they can be used to collect and store the faces of specific individuals.

Wi-Fi is used to quickly organize wireless video surveillance. High data rate, stability and security of the communication channel.

GSM. With its many shortcomings, it is the only one of these systems that allows you to remotely monitor the object, protected by mobile GSM devices, quickly gives "first hand" alarms via e-mail, MMS and SMS messages. This is the only wireless system that will be constantly monitored by the user, wherever he is within the GSM network.

Bluetooth has not been widely used in security systems due to the inability to operate at long distances and low speeds.

Given all the above, it is best to choose a GSM-module and Wi-Fi connection.

A video surveillance system with recognition functions and a data transmission channel is proposed, which adds identification capabilities and expands information transmission capabilities. This video surveillance system will provide better protection for any object.

Taking advantage of the face recognition feature and the capabilities of GSM and Wi-Fi technology, an additional channel has been introduced to send messages to the user about the detection of strangers and face identification through face scanning.

The program is implemented in the form of a Web-server for easy use from any device.

Advantages of the system:

- access control through face recognition.
- sending SMS messages via the GSM module when the system does not identify the person and in the settings mode.
- video surveillance via camera and live streaming via Wi-Fi.
- the ability to store data on the SD card.

Summing up everything

Video surveillance systems with recognition function are widely used today. They are designed to obtain information about the current state of the protected object (process) by collecting, processing, archiving, storing, displaying and analyzing this information.

As a result of the analysis of modern autonomous video surveillance systems the variant of system in which there are additional functions is offered. The system has two communication channels for better transmission of information and the ability to identify a person.

Although face recognition systems were originally used as applications, they have recently become increasingly used on mobile platforms and other technologies. Typically, the system is used to control access in security systems along with other biometric systems, such as iris recognition, fingerprints. Although the accuracy of facial recognition as a biometric technology is lower than that of iris recognition and fingerprint

recognition, it is widely used due to the non-contact and non-invasive process. There are many methods used in face recognition systems, but in general they are based on comparing the facial features of a given image with the faces stored in the database.

Therefore, for the proposed system, it was chosen to identify a person through a face scan.

Wi-Fi: among the advantages are high data rates, stability and security of the communication channel; Disadvantages include attachment to the IP address.

GSM: among the advantages is the ability to remotely monitor the object, which is protected by mobile GSM devices, promptly issues alarms via e-mail; among the disadvantages is that not everywhere there is coverage, but it is easily possible to replace it with 3G and 4G.

Given all the advantages and disadvantages of different types of information transmission modules, it follows that the best option for transmitting notifications is GSM, as its range is almost limitless. And the video stream can be transmitted both via GSM and Wi-Fi.

The proposed system can be used in offices, institutions and in residential buildings. ESP32-CAM offers an inexpensive way to build more advanced home automation projects that include video, photography and face recognition.