

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр

(назва освітнього ступеня)

на тему: Розроблення та дослідження автоматизованої системи «Розумний будинок»
з біометричною ідентифікацією користувачів та управлінням мікрокліматом

Виконав: студент

VI курсу, групи КТм-61

спеціальності

174 Автоматизація, комп'ютерно-інтегровані технології та
робототехніка
(шифр і назва спеціальності)

Станкевич М.В.
(підпис) (прізвище та ініціали)

Керівник

Тотосько О.В.
(підпис) (прізвище та ініціали)

Нормоконтроль

Чихіра І.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри

Голотенко О.С.
(підпис) (прізвище та ініціали)

Рецензент

Коноваленко І.В.
(підпис) (прізвище та ініціали)

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Голотенко О.С.
(підпис) (прізвище та ініціали)
«___» _____ 2025 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(шифр і назва спеціальності)

Студенту Станкевич Михайло Володимирович
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення та дослідження автоматизованої системи «Розумний будинок» з біометричною ідентифікацією користувачів та управлінням мікрокліматом

Керівник роботи Тотосько Олег Васильович, к.т.н., доцент кафедри КТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 12 » 11 2025 року № 4/7-962

2. Термін подання студентом завершеної роботи 23 грудня 2025р.

3. Вихідні дані до роботи Наукові публікації про процес розпізнавання особи

4. Зміст роботи (перелік питань, які потрібно розробити)

1. АНАЛІТИЧНА ЧАСТИНА. 2. ТЕХНОЛОГІЧНА ЧАСТИНА. 3. КОНСТРУКТОРСЬКА ЧАСТИНА. 4. Науково-дослідна частина. 5. СПЕЦІАЛЬНА ЧАСТИНА. 6. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ОСНОВНІ ВИСНОВКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Тема. 2. Актуальність роботи. 3. Мета роботи та цілі. 4. Приклад системи домашньої автоматизації. 5. Arduino ATmega 2560, Arduino UNO R3. 6. Внутрішня схема оптичного детектора пилю. 7. Апаратне забезпечення GSM SIM900A. 8. Схема 4-канального релейного модуля. 9. Блок-схема системи домашньої ідентифікації. 10. Блок-схема джерела живлення системи домашньої автоматизації. 11. Блок-схема системи домашньої автоматизації. 12. Дослідження системи автоматизації. 13. Дослідження відсоткових змін. 14. Знімок екрана програми збору даних. 15. Знімок екрана програми збору необроблених даних. 16. Висновки. 17. Завершення.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Тотосько О.В.		
Безпека в надзвичайних ситуаціях	Теслюк В.М.		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.2025	Виконано
2.	Підбір наукових джерел по темі роботи	26.11.2025-28.11.2025	Виконано
3.	Опрацювання наукових публікацій та збір даних по темі роботи	29.11.2025-1.12.2025	Виконано
4.	Виконання дослідження згідно мети кваліфікаційної роботи	2.12.2025-4.12.2025	Виконано
5.	Оформлення першого та другого розділів	5.12.2025-7.12.2025	Виконано
6.	Оформлення третього розділу	8.12.2025-10.12.2025	Виконано
7.	Оформлення розділу четвертого розділу	11.12.2025-13.12.2025	Виконано
8.	Виконання завдання до підрозділу «Охорона праці»	14.12.2025-15.12.2025	Виконано
9.	Виконання завдання до підрозділу «Безпека в надзвичайних ситуаціях»	16.12.2025-17.12.2025	Виконано
10.	Оформлення кваліфікаційної роботи	18.12.2025-19.12.2025	Виконано
11.	Нормоконтроль	19.12.2025-20.12.2025	Виконано
12.	Перевірка на плагіат	21.12.2025	Виконано
13.	Попередній захист кваліфікаційної роботи	22.12.2025	Виконано
14.	Захист кваліфікаційної роботи		

Студент

(підпис)

Станкевич М.В.

(прізвище та ініціали)

Керівник роботи

(підпис)

Тотосько О.В.

(прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота магістра складається з пояснювальної записки та графічної частини (ілюстративний матеріал – слайди).

Об'єм графічної частини дипломної роботи становить 17 слайдів.

Об'єм пояснювальної записки складає 76 друкованих сторінок формату А4.

В роботі використано 37 літературних джерел.

У роботі було розроблено автоматизовану систему ідентифікації особи з використанням ПЛК.

Було розглянуто основні аспекти процесу ідентифікації особи, основні параметри, як необхідно контролювати. Встановлено, що процес має характерні особливості та вимагає активного процесу керування в режимі реального часу.

Для побудови системи було описано технічні характеристики обладнання, розроблено конфігурацію системи, описано основні функції керування.

В роботі було розроблено систему ідентифікації особи з використанням ПЛК. На основі аналізу основних залежностей та моделей ідентифікації було розроблено ефективну систему розпізнавання на базі контролера ARDUINO.

Ключові слова: КОНТРОЛЕР, ІДЕНТИФІКАЦІЯ, РОЗПІЗНАВАННЯ, АВТОМАТИЧНИЙ КОНТРОЛЬ.

Станкевич М.В., Розроблення та дослідження автоматизованої системи «Розумний будинок» з біометричною ідентифікацією користувачів та управлінням мікрокліматом: кваліфікаційна робота магістра за спеціальністю «174 — Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / М.В. Станкевич – Тернопіль: ТНТУ, 2025. – 76 с.

ЗМІСТ

ВСТУП	6
1. АНАЛІТИЧНА ЧАСТИНА	8
1.1. Постановка задачі для автоматизації та ідентифікації особи.	8
1.2. Огляд відомих технічних рішень	12
2 ТЕХНОЛОГІЧНА ЧАСТИНА.....	18
2.1. Огляд системи	18
2.2. Характеристики використаних мікроконтролерів	18
2.3 Характеристики датчиків	20
2.4 Характеристики модулів.....	24
3 КОНСТРУКТОРСЬКА ЧАСТИНА	32
3.1 Апаратна архітектура та реалізація	32
3.2 Реалізація програмного забезпечення.....	39
3.3. Принцип роботи системи	46
4. НАУКОВО-ДОСЛІДНА ЧАСТИНА	49
4.1 Дослідження розпізнавання особи.....	49
5. СПЕЦІАЛЬНА ЧАСТИНА.....	58
5.1 Програмне забезпечення для збору даних	58
5.2 Протоколи	60
6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ.....	63
6.1 Організація охорони праці при роботі з системою управління.....	63
6.2 Електробезпека.....	65
6.3 Розрахунок заземлення.....	68
ОСНОВНІ ВИСНОВКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ.....	72
ПЕРЕЛІК ПОСИЛАНЬ.....	73

ВСТУП

Система домашньої автоматизації з кожним днем стає популярною в усьому світі, оскільки робить життя більш гладким і мінімізує робоче навантаження. Враховуючи внесок системи в полегшення повсякденного життя та посилення безпеки та безпеки будинку, очевидна необхідність розвитку та модернізації системи. Домашня автоматизація стосується автоматичного та електронного керування побутовими приладами, функціями та діяльністю. Найважливішим пристроєм сучасності є мобільний телефон. Зараз мобільний Android є дуже поширеною та дуже важливою частиною нашого життя. Використання цього пристрою в контрольно-спостережній роботі робить наше життя легким і комфортним. Отже, цей проект створено таким чином, щоб ми могли контролювати наш дім за допомогою одного пристрою. Система складається з апаратних, комунікаційних та електронних інтерфейсів, які працюють для інтеграції електричних пристроїв один з одним. Проект стане в нагоді інвалідам та людям похилого віку. Ця дипломна робота спрямована на модернізацію та розробку системи домашньої автоматизації з голосовим керуванням, яка дозволяє керувати всіма електронними пристроями в квартирі за допомогою голосової команди, забезпечує безпеку шляхом виявлення пожежі, виявляє підозрілі рухи, а також допомагає власнику особистою допомогою. Крім того, він забезпечує безпеку завдяки автоматичним дверям, керованим датчиком відбитків пальців. Виконання всіх цих завдань за допомогою одного пристрою Android робить все швидше, оскільки Android підтримує SMS-спілкування. Це дозволяє людині керувати приладами з віддаленого місця через Інтернет. Користувач може легко перевірити та закрити машини, залишені під час його відсутності, що допоможе заощадити енергію. У цьому проекті ми об'єднали домашню допомогу та систему безпеки за допомогою мікроконтролера. Отже, цей проект служить базовою структурою системи

ІІІ (штучного інтелекту). Програмування виконується в операційній системі Windows. Датчики та пристрої послідовного зв'язку вбудовані та синхронізовані з персональним комп'ютером.

1. АНАЛІТИЧНА ЧАСТИНА

1.1. Постановка задачі для автоматизації та ідентифікації особи.

У теперішній час немає потреби впроваджувати прогрес технологій. Як ми знаємо, прогрес пройшов довгий шлях і майже досяг свого піку модернізації. Сьогодні інновації перетворилися на скоординовану частину життя людей. Він впливав і продовжує впливати на численні частини повсякденного життя та дозволив покращити соціальну асоціацію, простоту транспорту, здатність насолоджуватися хвилюванням і медіа, а також допоміг у розвитку фармацевтики. Одним з найважливіших пристроїв сучасності є смартфон. Іншим важливим елементом сучасності є Інтернет. Ключ до кроку у світ автоматичної системи керування – це поєднання смартфона та Інтернету. Тому за допомогою цих двох мікроконтролерів стала можливою домашня автоматизація. Якщо ми поглянемо на кілька років тому, люди використовували пральні машини, водонагрівачі, фени тощо для домашніх справ. Не в кожному будинку, але в західних країнах ці машини використовуються щодня для домашніх справ. Ми можемо розглядати ці машини як початок домашньої автоматизації. Тепер ми можемо керувати телевізором, світлом, вентилятором холодильника тощо за допомогою телефонів Android. Цей проект стосується легкої та дешевої системи домашньої автоматизації та системи безпеки.

Кількість клієнтів смартфонів зросла в 2024 році, як зазначено в поточному звіті, поширеному Counterpoint Technology Market Research. Дослідження показує, що сімдесят п'ять відсотків частки ринку займає Android, і загалом у другій половині 2024 року було відвантажено сто шість мільйонів смартфонів Android. Смартфон Android став найкращою операційною системою на ринку в даний час у всьому світі, і став найпопулярніша операційна система, відома людству. Це робить телефон

Android найнеобхіднішим елементом сучасного життя. За допомогою цього маленького пристрою стала можливою автоматизація дому. Швидкий розвиток дистанційного листування надихнув нас на використання мобільних телефонів для дистанційного керування побутовою технікою. Окрім будинків, у нас є ресторани, де їжу подають за допомогою робота.

Домашня система, керована Android, не є поширеною, але певною мірою доступна в деяких офісах. Швидкий розвиток дистанційного листування надихнув нас на використання мобільних телефонів для дистанційного керування побутовою технікою. Фактичного визначення вбудованої системи немає. Пристрої, керовані комп'ютером, можна назвати вбудованими системами.

З появою кращого обладнання та кращого програмування стільникові телефони виявилися потужними гаджетами та перетворилися на невід'ємну частину повсякденного життя людини. Відповідно існує три епохи домашньої комп'ютеризації

По-перше, бездротова технологія з проксі-сервером. Приклад: автоматизація Next Zigbee. Штучний інтелект керує електричними пристроями. Приклад: Amazon Echo. Новітня технологія — робот, який взаємодіє з людиною. Приклад: робот Rovio, Roomba.

У нас є хороші та дешеві засоби для бездротових мереж, які все ще розвиваються. Це не означає, що ми цього не хочемо. Уряд і деякі організації намагаються розвивати нашу країну у сфері високих технологій. Зараз високі технології не обмежені кількома функціями. Те, що виводить високі технології на наступний рівень, це автоматична система. Ось чому зростає попит на автоматичні електронні пристрої. Для цього необхідна домашня автоматизація.

У 2016 році генеральний директор Facebook Марк Цукерберг створив для свого дому керованого голосом помічника зі штучним інтелектом (AI). Його надихнув персонаж «Джарвіс» із фільму «Залізна людина». Він описав,

що це як цифровий дворецький, який може говорити, відтворювати музику, керувати світлом і тостерами. Він також може сказати, хто стоїть за дверима. Цей проект зробив персонажа фільму майже реальним. Ця чудова його робота надихнула нас на реалізацію проекту домашньої автоматизації. У кількох розкішних будинках західних країн використовується багато розумної побутової техніки, як-от підземний холодильник, розумна шафа тощо. Ми віримо, що настане день, коли майже всі будинки будуть розумними. Цей проект – маленький крок до досягнення цієї мети.

Майже в кожному домі є смартфони, смарт-телевізор, розумний годинник, розумний холодильник, розумна пральна машина, розумний гараж, що зрештою веде до розумного дому. Звідси можна передбачити, що одного дня майже кожен будинок стане розумним будинком з автоматичною системою керування.

Ця бездротова система на базі Arduino включає в себе керування такими побутовими приладами, як освітлення, вентилятор, кондиціонер, телевізор, дата шоу, час, датчик пилу, кімнатна температура, датчики диму та руху та система безпеки з датчиком відбитків пальців.

Цей проект пропонує дистанційне керування побутовою технікою з безпекою будинку як всередині, так і зовні. Проект складається з:

1. Управління такими приладами, як світло, настільний вентилятор, телевізор, кондиціонер, штори тощо, здійснюватиметься за допомогою телефону Android через зв'язок Bluetooth за допомогою модуля Bluetooth. Використовується лише всередині будинку.

2. Щільність рівня пилу визначатиметься датчиком пилу та очищатиметься.

3. Система покаже дату, день, час і температуру. Для цього ми обрали модуль DS1307 RTC. LM35 покаже температуру. Усі вони також відображатимуться на рідкокристалічних дисплеях 16 x 2.

4. Датчик газу MQ-2 виявляє небезпечний газ і дим.

5. Рух штор залежатиме від потреби у світлі, яка вимірюється за допомогою світлозалежного резистора (LDR).
6. PIR-датчик (HC – SR501) використовується для виявлення руху.
7. Через модуль GSM ми будемо керувати вищевказаними приладами на відстані за допомогою текстових повідомлень. Це забезпечить безпеку всередині будинку за допомогою датчика PIR.
8. Модуль розпізнавання відбитків пальців призначений для системи автоматичного замикання та відмикання дверей.
9. Arduino Mega 2560 — мікроконтролер в операційній системі Windows.
10. Нарешті, усіма приладами керують голосові додатки та додатки для Android через мобільний телефон Android.

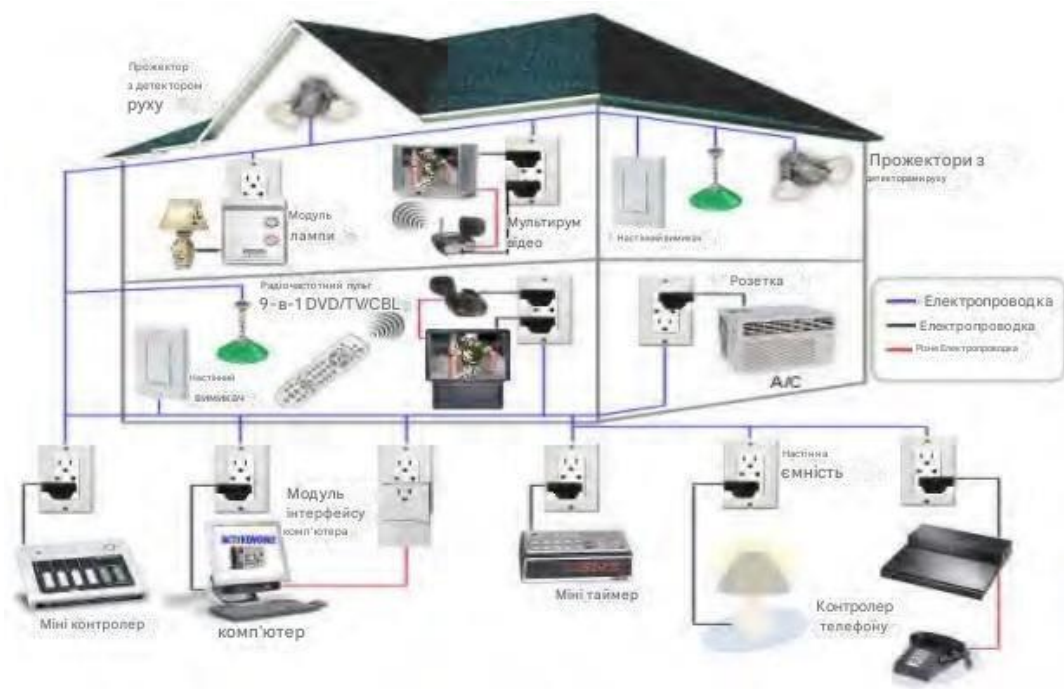


Рисунок 1.1: Приклад системи домашньої автоматизації.

1.4 Переваги

У наш час домашня автоматизація стає важливою для покращення способу життя.

Домашня автоматизація пропонує футуристичний спосіб життя, в якому людина може контролювати весь будинок за допомогою смартфона, від увімкнення телевізора до замикання чи відмикання дверей. Він також забезпечує ефективне використання енергії. Система автоматизації також дозволяє нам контролювати побутову техніку та стежити за будинком на відстані.

Це вигідно бабусям і дідусям, які зазвичай залишаються вдома самі. Інваліду також дуже корисно доглядати за будинком і легко повідомляти, якщо в будинку є якісь проблеми.

За даними Всесвітньої організації охорони здоров'я, серцеві захворювання, такі як астма чи інсульт, викликані забрудненням повітря, вбивають багато людей. Деякі респіраторні захворювання, викликані надлишком пилу, поступово призводять до інфекції.

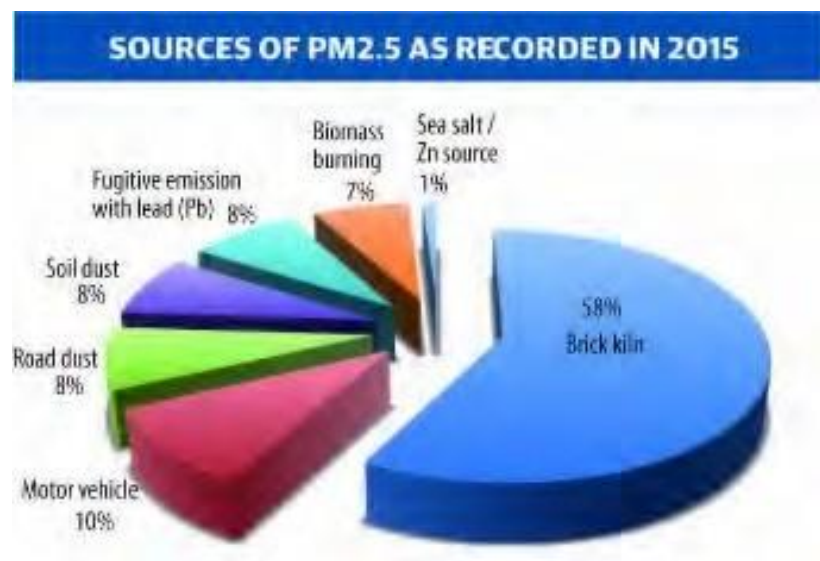


Рисунок 1.2: Джерело пилу в повітрі

Тому дуже важливо знизити рівень пилу в можливих місцях.

1.2. Огляд відомих технічних рішень

Домашню автоматизацію або розумні будинки можна описати як впровадження технології в домашнє середовище для забезпечення зручності, комфорту, безпеки та енергоефективності для його мешканців.

У різних країнах існує багато інших проектів домашньої автоматизації. Всі вони відрізняються один від одного дизайном; особливості, пристрої, елементи та алгоритм. Вони були розроблені відповідно до конкретних потреб і наявності компонентів у відповідних областях. Деякі з них дешеві; деякі з них дуже дорогі. Для роботи необхідна наявність як апаратного, так і програмного забезпечення. Після довгих пошуків ми знайшли багато статей. Шукаючи статті про безпеку, ми також знайшли кілька проектів, виконаних для безпеки гаражів. В основному це робиться в західних країнах. Багато проектів виконуються лише з метою безпеки за допомогою Arduino або Raspberry Pi. Знову ж таки, проекти створені лише для керування побутовою технікою за допомогою Arduino або Raspberry Pi.

Існує кілька проектів, присвячених модулю розпізнавання відбитків пальців для серйозних проблем домашньої безпеки. В одному з проектів використовувався біометричний метод для електронного паспорта нового покоління. Електронний паспорт, як його іноді називають, представляє сміливу ініціативу щодо впровадження двох нових технологій: радіочастотної ідентифікації (RFID) і біометрії.

Крім того, існують проекти, виконані на модулі розпізнавання відбитків пальців, які описують методи ідентифікації відбитків пальців. Велика різноманітність систем потребує надійних схем розпізнавання особи для підтвердження або визначення особи особи, яка запитує їхні послуги. Мета таких схем полягає в тому, щоб забезпечити доступ до наданих послуг лише законним користувачам і нікому іншому. У цих документах не згадувалося про те, як використовувати його для домашньої безпеки за допомогою будь-яких мікроконтролерів.

Розпізнавання обличчя є ще одним чудовим і розумним способом, який служить цілям безпеки. Ми знайшли проекти безпеки дверей за допомогою розпізнавання обличчя за допомогою Raspberry Pi. Ми уникали цієї частини з міркувань безпеки, оскільки помилки частіше трапляються під час розпізнавання обличчя, ніж під час розпізнавання відбитків пальців. Відбиток пальця має високу точність. Вони прямо не згадували про мету безпеки чи Raspberry Pi. Вони лише згадали про техніку розпізнавання. Різні люди по-різному описували процедуру розпізнавання.

В основному всі вони намагалися мінімізувати помилки комп'ютера для розпізнавання обличчя.

Троє дослідників з Малайзії запропонували веб-систему якості повітря в приміщенні з GSM і Arduino. Система складається з датчика газу, датчика температури та вологості, датчика частинок пилу та вузла бездротової сенсорної мережі (WSN) як бездротового передавача. Настільний комп'ютер виконує роль базової станції.

За словами Чена Ші-Чунга, запропоновані ним системи розроблені так, що їх можна легко адаптувати для різних застосувань, таких як керування машинами в машинобудівній промисловості, автомобільній промисловості, навігація мобільних бездротових вузлів, автоматизація офісів тощо.

Є кілька систем домашньої автоматизації, які використовують ZigBee або Bluetooth для бездротового з'єднання. За допомогою Wi-Fi і завдяки впровадженню IPv6 можливе підключення майже необмеженої кількості вбудованих пристроїв.

Іза Еліна та Склавос Ніколас запропонували систему на основі входів камер і датчиків, яка працює на різних рівнях контролю доступу користувача на основі політики паролів. Система працює через SMS-зв'язок через доступну мережу GSM.

Також представили проект та реалізовану систему автоматизації на основі Java через World Wide Web. Він має автономну вбудовану системну плату, інтегровану в домашній сервер на базі ПК.

Ендрю, автор книги «Домашня автоматизація Raspberry Pi за допомогою Arduino», представив Raspberry Pi і мотику, щоб використовувати її для домашньої автоматизації. Він описав використання Raspberry Pi з Arduino для операційної системи Linux. У книзі описано автоматичне керування деякими побутовими приладами. Спочатку він описав, як встановити все необхідне обладнання та всі необхідні умови. По-перше, він розповів історію Arduino та Raspberry Pi з усіма розетками, необхідними специфікаціями екрану та всіма необхідними портами з джерелом живлення. Ми змогли знайти необхідні дані Arduino, оскільки використовували його. Наведено гарні приклади термометра, відкривання та закривання завіси на основі даних про світло та температуру. З іншого боку, він не показав жодного прикладу, пов'язаного з безпекою житла.

Annan Zhu, Peijie Lin і Shuying Cheng з Фучжоуського університету Китаю описали систему дистанційного керування побутовою технікою за допомогою телефону Android через мережу GSM (2012 Міжнародна конференція з техніки керування та комунікаційних технологій). Вони зосередилися на дизайні терміналу Android, зв'язку між ARM і модулем GSM. Зведення до мінімуму труднощів у постачанні відповідного низьковольтного постійного струму для MCU та бездротового модуля за допомогою одного проводу під напругою також було одним із завдань. Тут ми знайшли лише керування пристроями за допомогою android, не більше того.

Стаття авторів про Сінгапур Томас Гоннот, Вон-Дже І, Ехсан Монсефі Джафар Саніє показали стандарт протоколу для системи домашньої автоматизації під назвою Home Automation Device Protocol (HADP). Їх компонентами стали Wi-Fi, Bluetooth 4.2, ZigBee IP, 6LoWPAN, стандарти

IEEE 802.15.4 і мережевий рівень Ethernet з підтримкою протоколу IPv6. В основному вони пропонували протокол якщо-це-то-то. Таким чином, він з'єднав багато пристроїв за допомогою з'єднання WIFI.

К. М. Абубекер,Хосе Дж Едатала,Синто Себастьянз Індії представила датчики PIR та інтелектуальний режим енергозбереження в лічильнику банкоматів. Він використовує піроелектричні інфрачервоні датчики для виявлення пішоходів і користувачів банкоматів. Система контролюється годинником реального часу RTC DS 1307, щоб розрізняти денний і нічний час за допомогою відеоспостереження. Це забезпечує відмінний захист лічильника банкомату.

За статтею Суреш, Дж. Бхавя, С. Сакші,використання PIR-датчика з Arduino Mega – це дешева та ефективна система безпеки, яка може повідомити про зловмисника за допомогою текстового повідомлення. Люди здебільшого покладаються на особисту охорону для безпеки будинку. Вони зробили це простіше та дешевше, ніж дорогі відеокамери спостереження.

Знову ж таки, є ще одна стаття, як запобігти крадіжкам у будинку П. Сатья Раві Теджа, В. Кушаль, А. Сай Срікарпід назвою «Світлочутлива охоронна система для виявлення та контролю крадіжок за технологією GSM». Вони зробили це за допомогою датчика на основі LDR (Light Dependent Resistor), який діє як електронне око для виявлення крадіжки або спроби, і процедури сигналізації на основі SMS за допомогою технології GSM (Global Systems for Mobile Communications). Це також дуже дешево.

Це кілька попередніх досліджень, проведених на подібну тему. Раніше зазначалося, що в більшості з них відсутні або система безпеки, або система контролю. Ми уникали системи розпізнавання обличчя для домашньої безпеки, оскільки люди намагаються мінімізувати багато помилок у розпізнаванні обличчя. Обличчя має бути під певним кутом, щоб комп'ютер міг його розпізнати. Тому модуль розпізнавання відбитків пальців більш надійний для безпеки дверей. Деякі з цих проектів виконані за допомогою

Arduino, деякі з них зроблені за допомогою Raspberry Pi. Такі компоненти, як датчики та екрани, також мають різні моделі. Наша мета полягає в тому, щоб об'єднати ці системи разом, тобто керувати побутовою технікою та системою безпеки за допомогою Arduino, зберігаючи це якомога дешевше.

2 ТЕХНОЛОГІЧНА ЧАСТИНА

2.1. Огляд системи

Дуже важливо знати всю інформацію про апаратні та програмні характеристики, які ми використовували для проекту. Ми використовуємо такі компоненти:

1. Arduino Mega 2560
2. Arduino Uno R3
3. Датчики:
 - a. Датчик газу MQ-2 (SEN 00091)
 - b. PIR детектор руху (HC – SR501)
 - c. Датчик пилу
 - d. Датчик температури LM 35
 - e. Датчик світлозалежного резистора (LDR).
4. Модуль Bluetooth HC-05
5. GSM Shield SIM900A
6. Релейний модуль (4 канали)
7. РК-дисплей із заголовком (16x2)
8. Модуль розпізнавання відбитків пальців (FPM10A)
9. Макетна дошка
10. Перехідник
11. Серводвигун
12. DS1307 RTC
13. П'єзозумер

2.2. Характеристики використаних мікроконтролерів

Arduino Mega 2560 — плата мікроконтролера на основі ATmega2560. Він має 54 контакти цифрового входу/виходу (з яких 14 можна використовувати як виходи ШІМ), 16 аналогових входів, 4 UART (апаратні послідовні порти), кварцевий генератор 16 МГц, USB-з'єднання, роз'єм

живлення, роз'єм ICSP тощо Він містить все необхідне для підтримки мікроконтролера; просто підключіть його до комп'ютера за допомогою USB-кабелю або живіть за допомогою адаптера змінного струму в постійний струм або акумулятора, щоб розпочати роботу.

У нашому проекті ми використали адаптер із Arduino Mega 2560, який забезпечить живлення всіх компонентів.

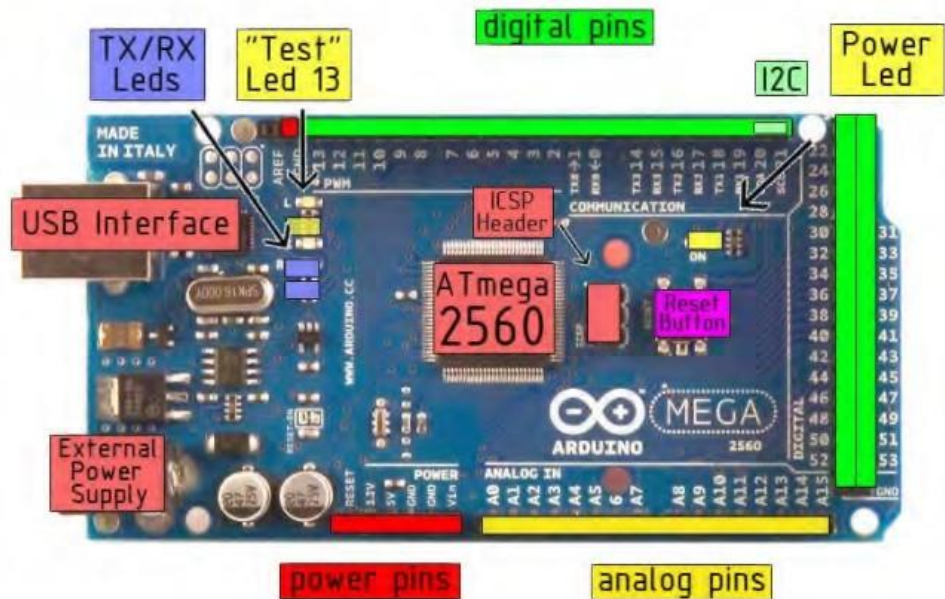


Рисунок 3.1: Arduino ATmega 2560.

Arduino Mega 2560:

Ця плата працює в 5 В 40-50 мА. Він має 54 контакти, з яких 16 є аналоговими входами. Аналоговий вхід, цифровий вхід, контакти PWM розділені.

Кожен із 54 цифрових контактів Mega можна використовувати як вхід або вихід за допомогою функцій `pinMode()`, `digitalWrite()` і `digitalRead()`.

Arduino Mega має захисний компонент із полізапобіжником, який захищає порти USB від переповнення струмом. Понад 500 мА автоматично розриває з'єднання, доки коротке замикання або перевантаження не буде усунуто.

Arduino UNO R3:

Arduino UNO називають «стоковим» Arduino. Він легко адаптується до всіх пристроїв програмування. Усі інші плати Arduino є різними версіями плати UNO. Майже всі функції схожі на Arduino MEGA з меншою кількістю контактів.

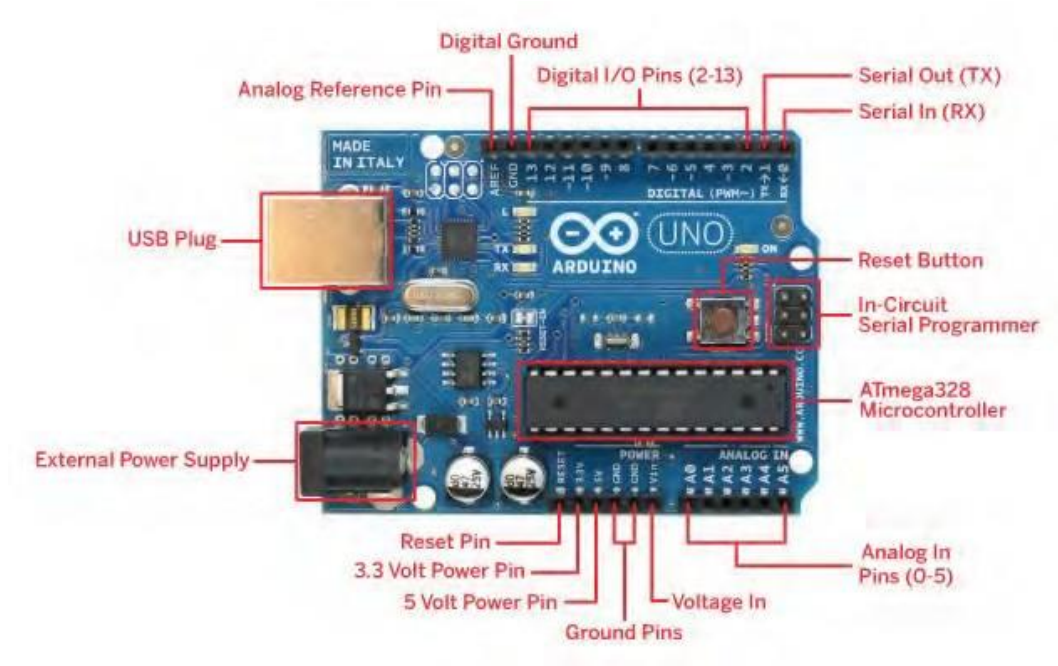


Рисунок 2.2: Arduino UNO R3 з розпіновками.

2.3 Характеристики датчиків

Нижче наведено введення та огляд датчиків, які ми використовували:

- Датчик газу MQ 2:
 - a) Висока чутливість до чадного газу та CH₄, LPG.
 - b) Стабільний і довгий термін служби

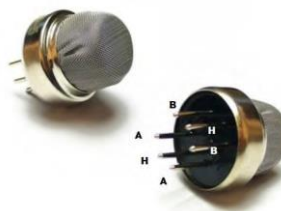


Рисунок 2.3: Датчик газу MQ 2.

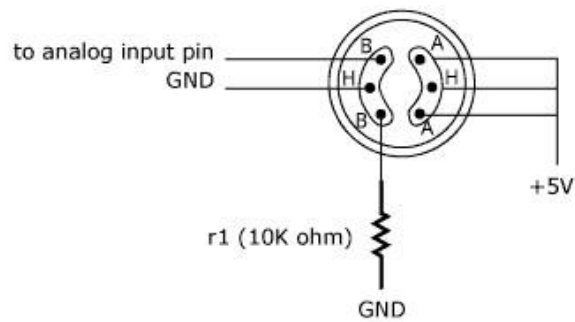


Рисунок 2.4: Схема контактів датчика газу.

Цей пристрій працює від джерела живлення 5 В як у змінному, так і в постійному струмі. Добре працює при кімнатній температурі. Це також має регульований резистор навантаження.

Дальність виявлення: Діапазони визначення газу: (а) 20 ppm-2000 ppm монооксид вуглецю, (b) 500 ppm-10000 ppm CH₄, (c) 500 ppm-10000 ppm LPG.

- *PIR Детектор руху (HC – SR501):*

HC-SR501 базується на інфрачервоній технології, модулі автоматичного керування, використовує конструкцію зонда LHI778, імпортовану з Німеччини, високу чутливість, високу надійність, режим роботи з ультранизькою напругою, широко використовується в різноманітному електричному обладнанні з автоматичним визначенням, особливо для продуктів з автоматичним керуванням, що живляться від батарейок.



Рисунок 2.5: (а) PIR детектор руху (вид зверху). (b) PIR детектор руху (вид знизу).

Специфікація:PIR-датчик має можливість працювати в мережі 5-20 В. При 3,3 В датчик буде високим, а при 0 В – низьким.

Він широко використовується в цілях безпеки, індукційних іграшках для тіла та іграшках для промислової автоматизації.

Піроелектричний інфрачервоний перемикач — це пасивний інфрачервоний перемикач, який складається з BISS0001, піроелектричних інфрачервоних датчиків і кількох зовнішніх компонентів. Він може автоматично відкривати всі види обладнання, включаючи лампи розжарювання, люмінесцентні лампи, домофон, автоматику, електричний вентилятор, сушарку та автоматичну пральну машину тощо.

Він широко використовується на підприємствах, готелях, магазинах, коридорах та інших чутливих зонах для автоматичного освітлення, освітлення та сигналізації.

- *Оптичний детектор пилю:*

GP2Y1010AU0F, пристрій із дуже низьким споживанням струму, який використовується для визначення рівня пилю, здатний виявляти в повітрі дуже дрібні частинки пилю, наприклад сигаретний дим. Інфрачервоний випромінювач і фототранзистор розміщені для виявлення відбитого від повітря світла. Щоб відрізнити частинки диму від домашнього пилю, він використовує імпульсну схему вихідної напруги. Він використовує фотометрію для виявлення частинок пилю.



Рисунок 2.6: Оптичний детектор пилю.

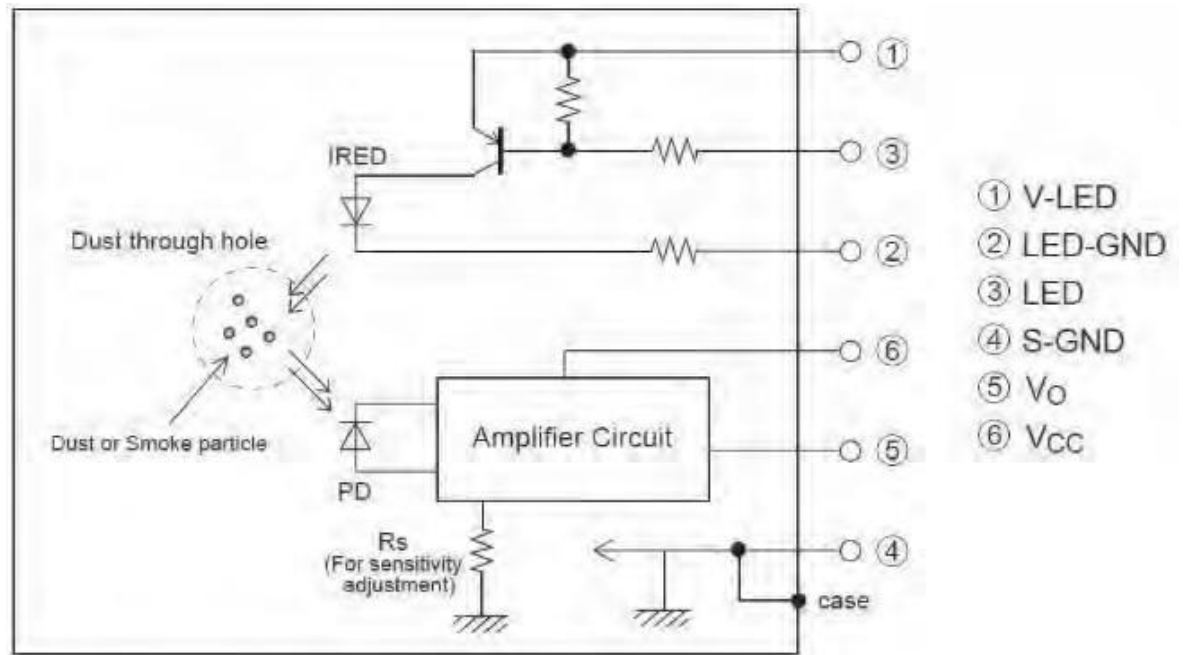
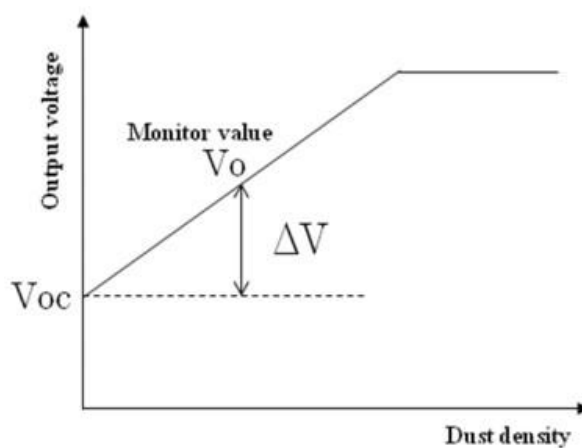
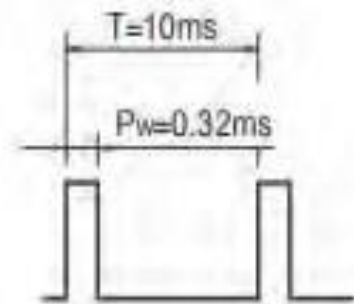


Рисунок 2.7: Внутрішня схема оптичного детектора пилу.



(a)

Pulse-driven wave form



(б)

Рисунок 2.8: (a) Вихідна напруга від щільності пилу. (б) Імпульсна хвиля.

Розмір компактний і дуже низьке споживання. Його RoHS не містить свинцю. Цей прилад може виявити пил за одним імпульсом. Як і інші пристрої, він працює від 5 В і максимум 20 мА.

Датчик пилу використовується для виявлення та контролю рівня запиленості повітря.

даних) 3 Мбіт/с із радіоприймачем 2,4 ГГц і основною смугою. Він використовує технологію CMOS із зовнішньою системою Bluetooth CSR Blue core 04 і AFH (функції адаптивного стрибкоподібного зміни частоти). Цей модуль забезпечує режим перемикання між головним і підлеглим режимами, що означає, що він не може приймати або передавати дані.

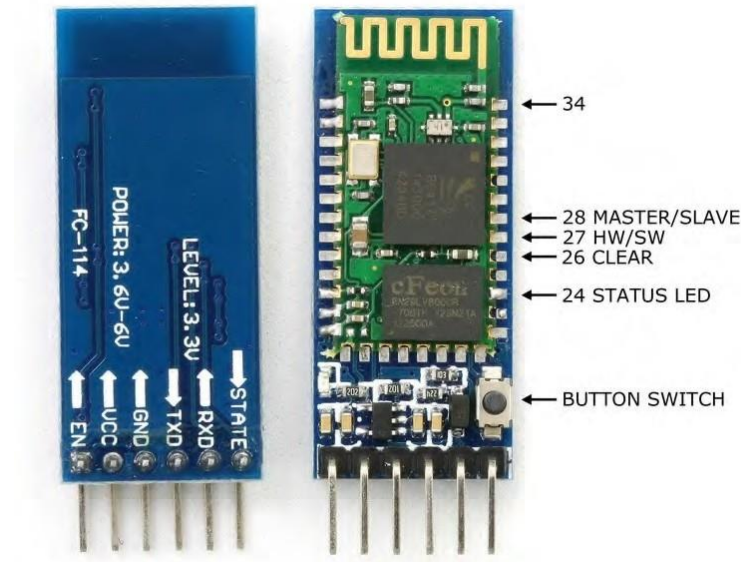


Рисунок 2.10: Модуль Bluetooth HC-05 із конфігурацією контактів.

Апаратні особливості: Bluetooth потребує 1,8 В для роботи, від 3,3 до 5 ВІ/О. Чутливість зазвичай становить -80 дБм, а інтерфейс UART із програмованою швидкістю передачі даних. Крайовий роз'єм також присутній.

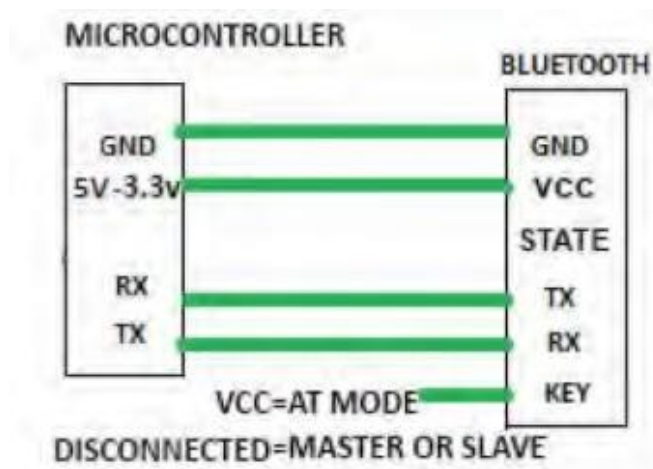


Рисунок 2.10: Типова схема підключення модуля Bluetooth.

Особливості програмного забезпечення:

а. Підлегла швидкість передачі даних за замовчуванням: 9600 Біт даних:
8.

Стоп-біт: 1.

Немає паритету.

б. P109 і P108 можна підключити до червоного та синього світлодіодів окремо. Коли провідний і підлеглий сполучені, червоний і синій світлодіод блимає з інтервалом 1 раз/2 с, у той час як від'єднані лише синій світлодіод блимає 2 рази/с. Автоматичне підключення до останнього включеного пристрою за замовчуванням.

с. Дозволити підключення пристрою для створення пари за умовчанням.

д. PIN-код автоматичного сполучення: «1234» за замовчуванням.

е. Автоматичне повторне підключення через 30 хвилин у разі відключення через межі діапазону з'єднання.

- *Модуль GSM SIM900A:*

Це вихідна плата з мінімальною системою дводіапазонного модуля GSM/GPRS SIM900A. Він може спілкуватися з контролерами через AT-команди.

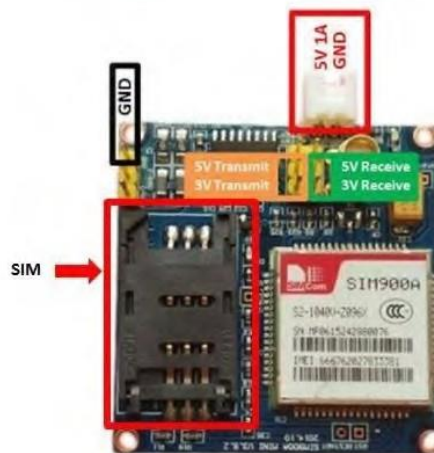


Рисунок 2.11: GSM SIM900A.

особливості:

а) Чотири діапазони 850/ 900/ 1800/ 1900 МГц

- b) Дводіапазонний 900/1900 МГц
- c) Мультислотова GPRS класу 10/8GPRS мобільна станція класу В
- d) Сумісність із GSM фаза 2/2+Клас 4 (2 Вт при 850/900 МГц)
- e) Клас 1 (1 Вт при 1800/1900 МГц)
- f) Управління через АТ-команди (GSM 07.07 ,07.05 і SIMCOM удосконалений АТ команди)
- g) Низьке енергоспоживання: 1,5 мА (режим сну)
- h) Робоча температура: від -40°C до +85°C

Максимальна напруга живлення може бути 5,5 В. Його споживання становить 2000 мА для імпульсного і 500 мА для постійного струму. Найвища швидкість передачі даних становить 115200 біт/с.

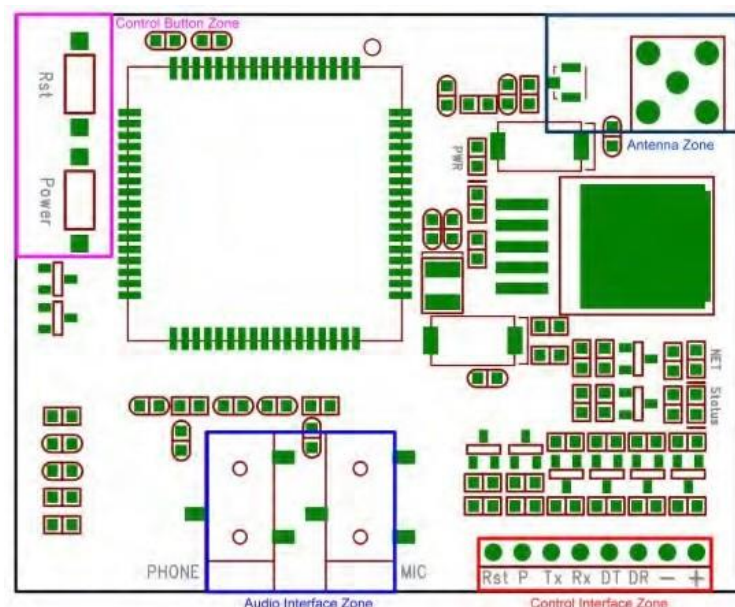


Рисунок 2.13: Апаратне забезпечення GSM SIM900A (вид зверху).

GSM відіграє дуже важливу роль у бездротовому зв'язку. Він повинен дотримуватися різних протоколів для безпечного бездротового зв'язку. Це:

- а. Специфікації даних: Максимум 85,6 Кбіт/с з GPRS клас 10. USSD
- Вказано стек PPP. Схема кодування CS 1,2,3,4

б. Специфікації для SMS:Двохточкові МО і МТ, SMS-мовлення, текстовий режим і режим PDU.

с. Особливості програмного забезпечення:0710 Протокол MUX із вбудованим протоколом TCP/UDP і FTP/HTTP

- Релейний модуль 5В 4-канальний:

Це 4-канальна релейна плата 5 В, яка використовується для керування різними приладами. Його можна використовувати як з мікроконтролерами, так і без них. Кожне реле 5 В потребує 20 мА керуючого струму. Має світлодіоди для індикації стану виходу.



Рисунок 2.14: 4-канальний релейний модуль 5 В.

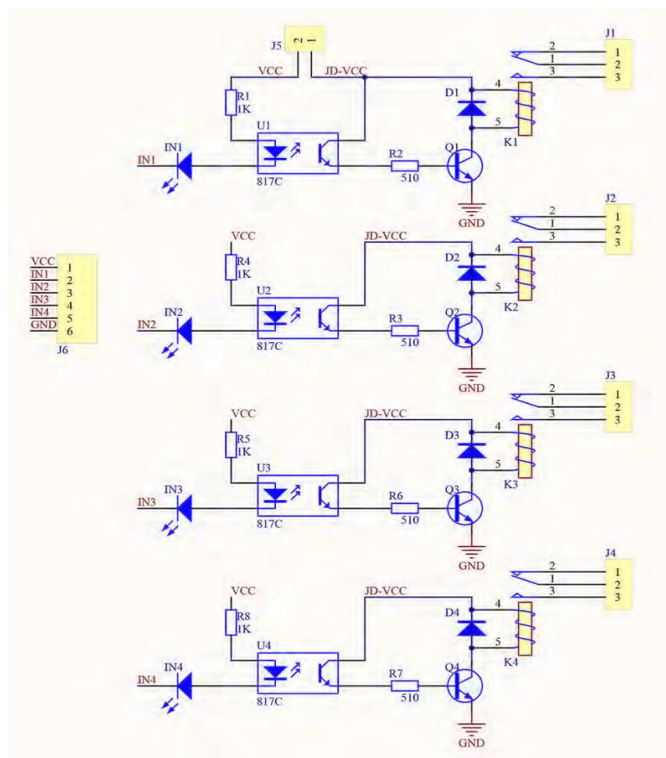


Рисунок 2.15: Схема 4-канального релейного модуля.

- *Серводвигун:*

Для цієї системи ми використали два серводвигуни; один для керування дверима, а інший для віконних штор.



Рисунок 2.16: Серводвигун SG90.

- *РК-дисплей 16x2:*

РК-дисплей 16x2 означає, що відображає 16 символів у рядку, і є 2 таких рядка. РК-екран (рідкокристалічний дисплей) — це електронний модуль відображення. Він економічний і легко програмується. Вони є кращими перед семисегментними та іншими багатосегментними світлодіодами.

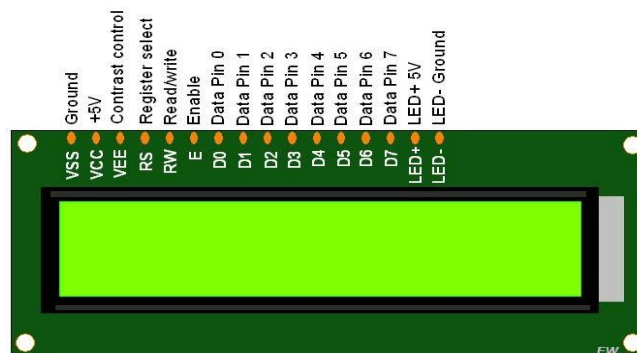


Рисунок 2.17: Конфігурація контактів РК-дисплея 16x2.

Функції контактів інтерфейсу: Уся конфігурація контактів інтерфейсу наведена в таблиці 4.2

- *Модуль розпізнавання відбитків пальців (FPM10A):*

Оптичний модуль відбитків пальців використовується для виявлення та перевірки особи за допомогою біометрії. Цей модуль виконує магічне

відтворення, обчислення, пошук об'єктів і пошук. Він сумісний з будь-яким мікроконтролером.

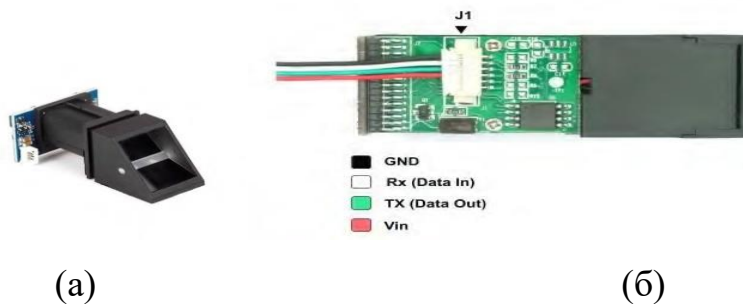


Рисунок 2.18: (а) Модуль розпізнавання відбитків пальців. (б) Розпиновка модуля.

Ознайомлення з модулем: Зазвичай працює при 100 мА з піковим 150 мА. Швидкість передачі даних $N \times 9600$ біт/с. Він має можливість зберігати 256 пробних відбитків. Розмір шаблону має бути 512 байт. Цей датчик займає менше 0,5 секунди, щоб зняти відбиток пальця. Крім того, він має найвищу точність з усіх біометричних процесів.

Принцип дії: Операція має 2 кроки: реєстрація та зіставлення (1.1 або 1.N). Система створить і збереже шаблон зображень пальців шляхом обробки зображення. Користувач повинен ввести палець два рази. Користувач вводить палець через оптичний датчик під час зіставлення. Система порівнює живий палець із конкретним шаблоном, розробленим у модулі, під час зіставлення 1:1. Система шукатиме відповідність 1:N у всій бібліотеці відбитків пальців. Нарешті система повертає результат, що збігається або не вдається в обох процесах.

Апаратне підключення: модуль зв'язується з MSU за допомогою живлення 3,3 В або 5 В через послідовний інтерфейс. TD (контакт 3 P1) з'єднується з RXD (приймальний контакт MCU), RD (контакт 4 P1) з'єднується з TXD.

Протокол послідовного зв'язку: це напівдуплексний асинхронний послідовний зв'язок. Швидкість передачі коливається від 9600-115200 біт/с.

Ми використовували 9600 біт/с. Формат кадру передачі 10 біт; 8-бітові дані з першим LSB і кінцевим бітом. Немає контрольного біта.

Час скидання: для ініціалізації потрібно 500 мс. Модуль наразі не може прийняти жодну команду.

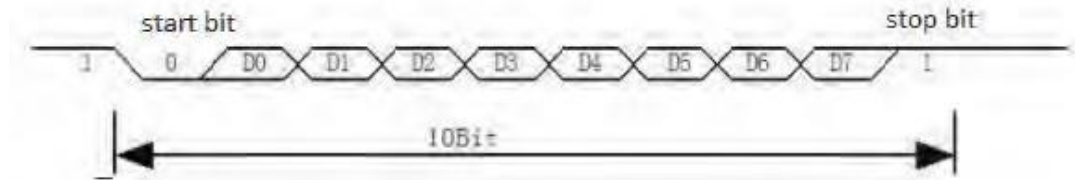


Рисунок 2.19: Передача формату кадру.

- *Модуль RTC DS1307:*

Ми використовували цей модуль у системі для вимірювання часу та дати. Він простий у використанні і дуже дешевий. Працює від акумулятора. Легко запрограмувати час як у 12-годинній, так і в 24-годинній системі.



Рисунок 2.20: Модуль RTC DS1307.

- *Звуковий сигнал:*

Цей модуль є недорогим зумером сигналізації під назвою п'єзозумер. Цей пристрій є сигналізацією для цієї системи. Він починає дзвонити, коли температура підвищується дуже високо та виявляється дим. Він також починає дзвонити, коли датчик PIR високий.



Рисунок 2.21: П'єзозумер.

З КОНСТРУКТОРСЬКА ЧАСТИНА

Відповідно до запропонованої системи ми розробили структуру системи, зображену на блок-схемі. Ми розробили модель таким чином, щоб її можна було зберігати в безпечному місці всередині будинку. Усе програмування та встановлення компонентів виконується та перевіряється в лабораторії та вдома. Є багато компонентів і проводів, які ми використовували для системи. Це робиться найпростіше і з найменшими витратами. Однак система є гнучкою і може бути налаштована користувачем. Зміна налаштувань одного з компонентів має бути сумісною з відповідним доступним програмним забезпеченням. Кожен компонент, який використовується в цій системі, був запрограмований і перевірений окремо на заходи безпеки та відповідність правильному драйверу. Кожен компонент було запрограмовано окремо як з Arduino Mega, так і з Arduino UNO з використанням різних Arduino IDE. Крім того, вони запускалися на різних комп'ютерах. Пізніше всі були об'єднані в єдину Arduino IDE. Без Wi-Fi і комп'ютера запустити систему неможливо.

Цей проект складається з двох частин: апаратна реалізація та програмна реалізація.

3.1 Апаратна архітектура та реалізація

Компоненти можна розділити на дві категорії: датчики та модулі. Усі вони описані нижче:

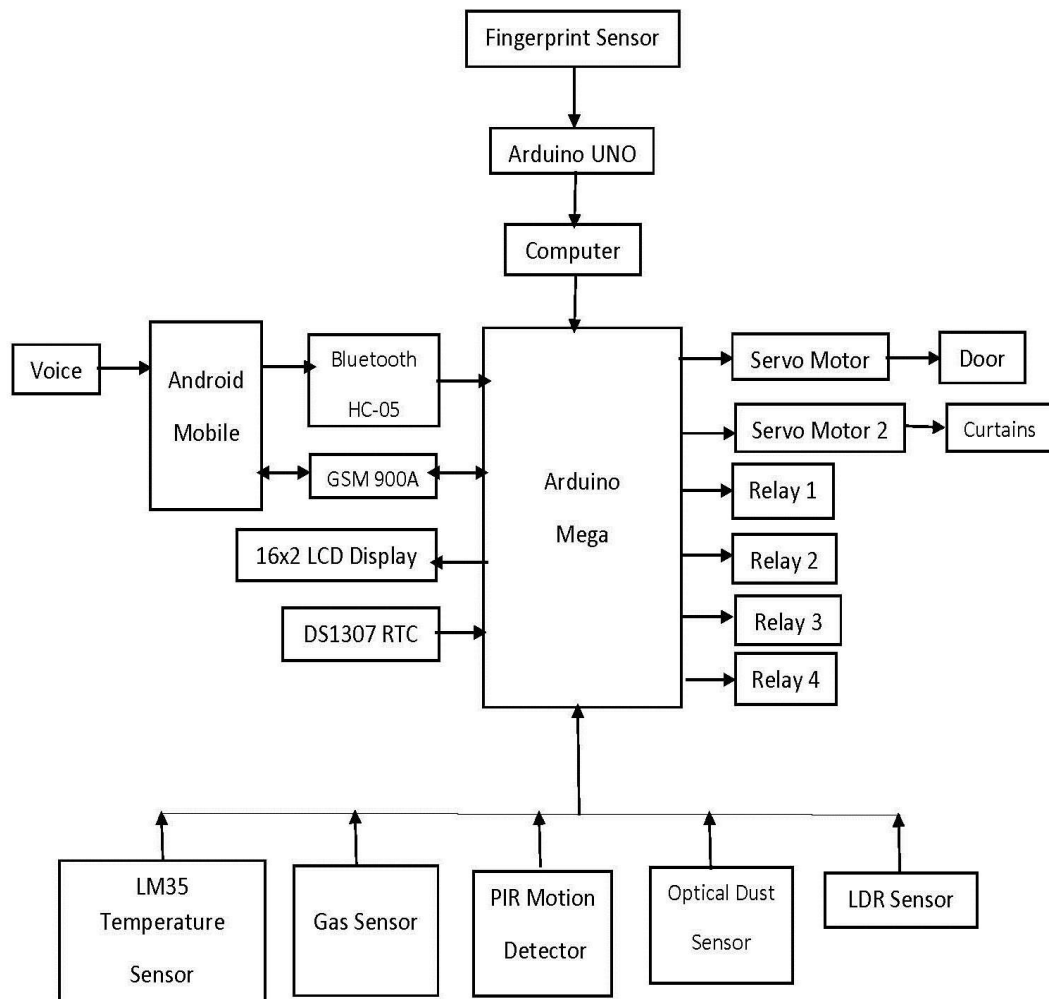


Рисунок 3.1: Блок-схема системи домашньої автоматизації.

Всі датчики з'єднані з мікроконтролером проводами. Всі входні напруги подаються від мікроконтролера з комп'ютером.

Вони описані нижче за допомогою схеми. У цьому розділі нижче описано апаратну реалізацію всіх датчиків:

Датчик газу: У газових датчиках серії MQ всередині є невеликий нагрівач з електрохімічним датчиком. З'єднайте контакти А разом і контакти В разом, а потім застосуйте VCC до зв'язаних контактів А або В. Ми застосували GND через змінний резистор RL (2K до 47K Ом) до решти пов'язаних контактів А або В. Контакти нагрівача Н і Н, з'єднані з VCC і GND. Контакти А і В не повинні бути з'єднані між собою. Датчик в

основному залежить від нагріву спіралі, нагрівач використовує живлення 5 В постійного струму. Датчик безпосередньо підключений до Arduino Mega. Вихід - аналоговий сигнал; він читається за допомогою аналогового входу. Вихідний контакт датчика газу з'єднаний із цифровим контактом arduino mega digital 22.

PIR детектор руху: Апаратна реалізація включає дві версії додатків з різними виходами перемикання потужності та джерелом живлення: версія релейного виходу живлення та версія виходу потужності симистора. У цій системі ми використовували 2 датчики PIR; один для незвичайного виявлення руху всередині кімнати, а інший для автоматичного вмикання та вимикання світла, коли хтось заходить у кімнату. PIR датчик безпеки підключений до цифрового контакту 26.

Оптичний детектор пилу: Налаштуємо пін наступним чином:

PIN 1: V-LED- 3,3 В (150 Ом між ними)

PIN 2: контакт LED-GND-GND

PIN 3: світлодіодний цифровий контакт

PIN 4: S-GND- GND Pin

PIN 5: VO – аналоговий контакт

PIN 6: VCC – контакт 3,3 В (прямий)

LM35 Прецизійний датчик температури: Шпильок всього три. Вихідний висновок (контакт 2) підключається до аналогового входу плати Arduino.

Модулі:

МОДУЛЬ GSM SIM900A: Цей модуль має 6 контактів, у яких два контакти є VCC і GND. Решта 3VR, 3VT (3 вольт RX і TX) і 5VR, 5VT (5 вольт RX і TX). З'єднання такі:

VCC до 5В

GND до GND

5VR до цифрового контакту

5VT до цифрового контакту

Перш ніж працювати з GSM, ми повинні перевірити наступні умови:

Вставте SIM: вставте SIM-картку в утримувач картки, позначений на малюнку. Переконайтеся, що на SIM-карті є баланс.

Підключаємо антену: кріпимо RF антену до роз'єму антени SMA і затягуємо її обертанням гайки.

З'єднуємо штирі: з'єднуємо штирі відповідно до нашої принципової схеми.

Живлення модему: Ми живимо модем для відповідного джерела живлення ($>1A$). Ми використовували адаптер для живлення.

Перевірте стан світлодіода: Світлодіод PWR: червоний світлодіод загоряється негайно ii. Світлодіод STS: зелений світлодіод загоряється через 1-2 секунди iii. NET LED: синій світлодіод спочатку швидко блимає протягом кількох секунд (пошук мережі) і повільно блимає, коли модем зареєструється в мережі.

Швидкість передачі даних: ми обрали швидкість передачі даних 9600 бод. З'єднання виконуються згідно з малюнком вище з ПК-монітором. Усі конфігурації контактів виконуються відповідно до конфігурації контактів.

Модуль Bluetooth HC-05: Модуль Bluetooth відіграє дуже важливу роль у взаємодії побутової техніки з телефоном Android, але він має лише чотири контакти для підключення. Нижче наведено контактні з'єднання:

Піни Arduino	Шпильки Bluetooth
RX (PIN-код 0)	TX
TX (PIN-код 1)	RX
5B	VCC
GND	GND

Таблиця 3.1: Штифтовий інтерфейс Bluetooth.

4-канальний релейний модуль: Всі компоненти разом з реле. Реле вмикається після того, як усі датчики та модулі мають високий рівень. У разі відмикання дверей, коли відбиток пальця збігається, реле включається, і двері відкриваються за допомогою серводвигуна. У випадку з усіма датчиками, коли вони високі, реле вмикається для надсилання текстового повідомлення на телефон. Реле, очевидно, як вимикач, підключається до всіх побутових приладів. Також можливе управління реле через GSM. Ми також керували кімнатними шторами за допомогою реле та сервомотора. Підключення виконується за принциповою схемою.

Модуль годинника реального часу DS1307: У модулі RTC є 4 контакти, які позначені, як на малюнку. Вони підключаються згідно з мітками безпосередньо до Arduino Mega.

РК-дисплей 16x2: Вивід вибору регістра (RS), який контролює, куди в пам'ять РК-дисплея будуть записуватися дані, з'єднаний з аналоговим виводом 9. Вивід увімкнення, який дозволяє записувати в регістри, з'єднаний з аналоговим виводом 8. Виводи даних (D4-D7) з'єднані з відповідними аналоговими контактами (4, 5, 6, 7). Контакти джерела живлення +5 В і GND підключені до макетної плати.

Е. Таблиця конфігурації PIN-коду: Нижче наведено всі підключення датчиків і модулів:

Контакти РК-дисплея:

SL	Ардіуно МЕГА	ЖК
1	4	D7
2	5	D6
3	6	D5
4	7	D4

5	8	Еп
6	9	рупій

Таблиця 3.2: З'єднання контактів РК-дисплея з мікроконтролером.

SL	Ардіуно Мега	Датчики
1	22	газ
2	26	PIR (безпека)
3	28	LDR
4	30	PIR (світло)

Таблиця 3.3: Інтерфейс датчиків із мікроконтролером.

Контакти модуля:

SL	Модулі	Ардіуно МЕГА
1	Sim900	2
2	Bluetooth	3
3	RTC	Цифровий пін
4	Серво (вікно)	3
5	Серво (двері)	7
6	П'єзо зумер	44, 45
7	Реле (вентилятор)	36
8	Реле (світло-2)	38
9	Реле (світло-1)	40

Таблиця 3.4: Інтерфейсні модулі з мікроконтролером.

Використовується 2 понижувальних перетворювача DC-DC на 6 В 3 А та 8 В 3 А відповідно. Також в схему додано адаптер 12V 5A. Для роботи SIM900A потрібен струм 3 А. Інакше текстове повідомлення не буде надіслано або отримано. Для підтримки стабільного стану використовуються ці додаткові модулі. Конфігурація високої або низької напруги та струму може пошкодити всю систему. Якщо є хоч якась ймовірність вилучення системи з живлення, вся система впаде. Щоб уникнути такої проблеми використовуються акумулятор і адаптер. Тому проблем із системою безпеки не буде.

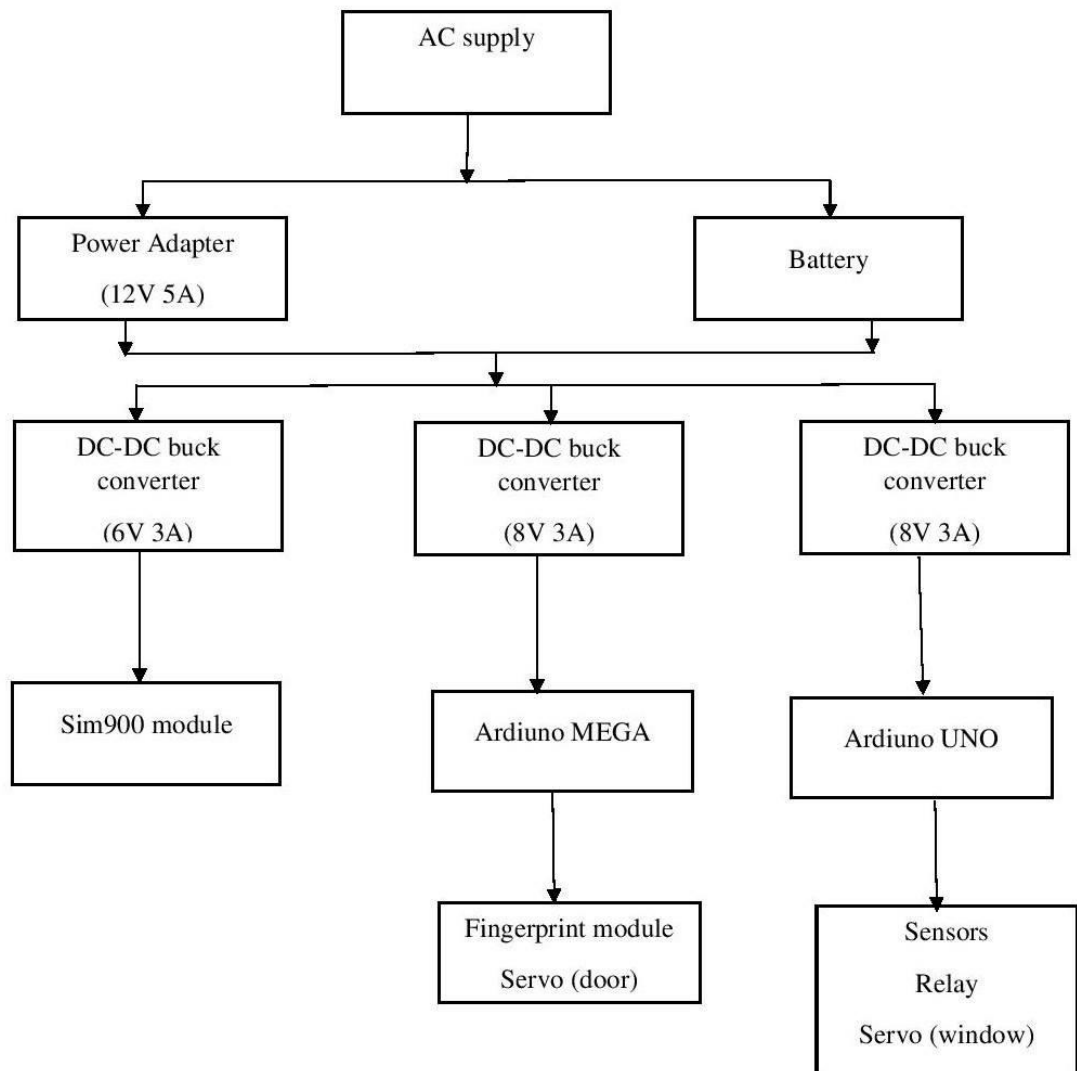


Рисунок 3.2: Блок-схема джерела живлення системи домашньої автоматизації.

3.2 Реалізація програмного забезпечення:

Ми використовували програмне забезпечення Arduino IDE 1.8.5. Весь код написаний в одній середі IDE під назвою sketch.

Усі компоненти сумісні з Arduino, тому ми включили відповідну бібліотеку Arduino Adafruit. Для цього розділу ми також розділили робочу процедуру на чотири частини: датчики, модулі, додаток Android і голосовий контролер.

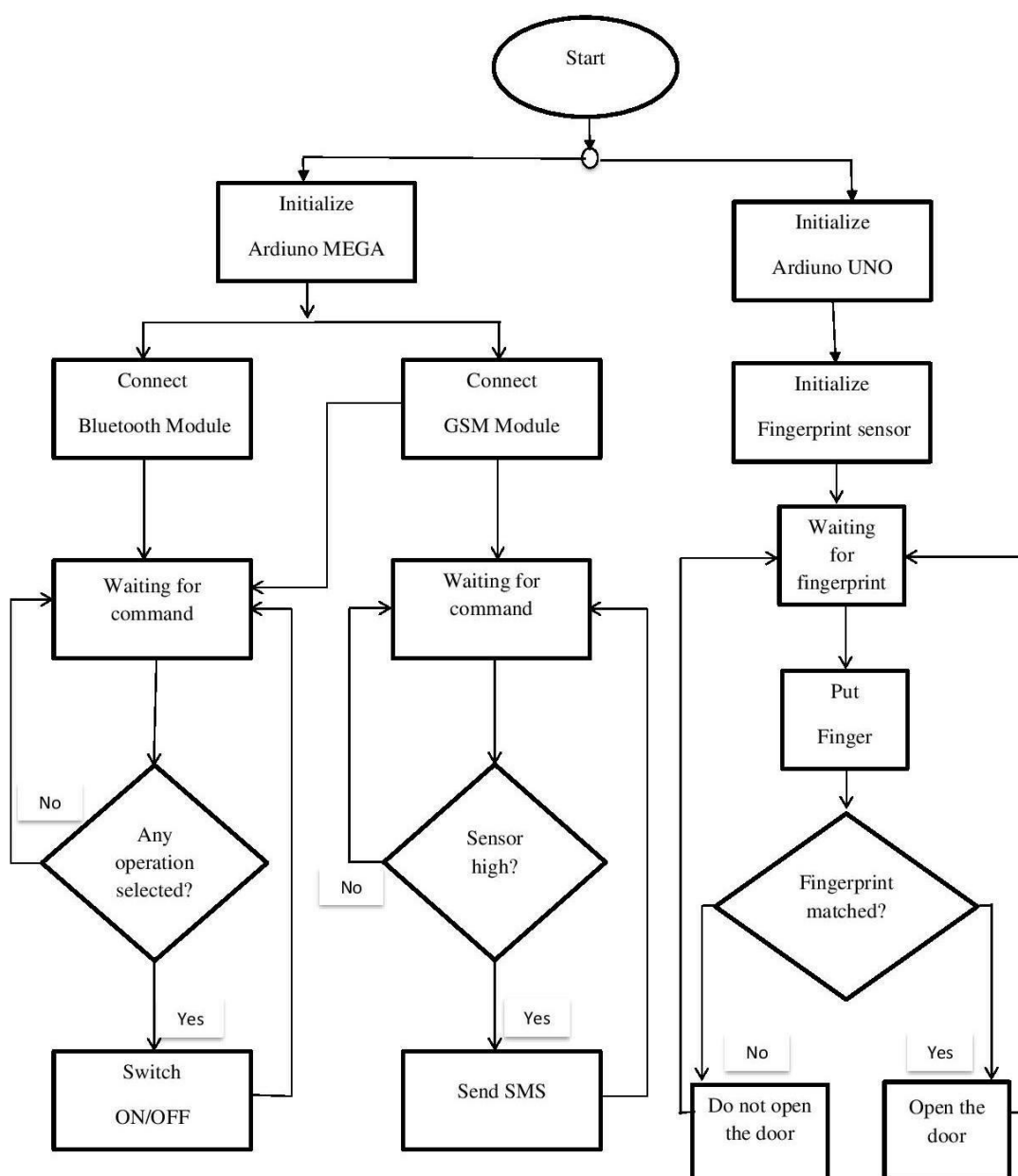


Рисунок 3.3: Блок-схема системи домашньої автоматизації.

Датчик: Датчик — це електронний пристрій, який реагує на будь-яку зміну фізичного явища або змінних навколишнього середовища, таких як тепло, тиск, вологість, рух тощо. Усі датчики є аналого-цифровими. Ці датчики виробляють безперервний вихідний сигнал. Комп'ютер не може зчитувати або аналізувати безперервні значення, тому для точного вимірювання всі датчики потрібно відкалібрувати відповідно до певного контрольного значення або стандарту. Після цього сигнал, створений датчиком, піддається аналізу. Одна з найважливіших характеристик датчиків полягає в тому, що вихідний сигнал повинен змінюватися лінійно з входом. Процес роботи датчиків, які ми використовували, наведено нижче:

Датчик газу (SEN 00091): Датчику потрібно три хвилини, перш ніж показання стануть стабільними. Це програмується за допомогою функції `analogWrite()` і затримка. У разі виявлення газу він надсилає повідомлення на мобільний телефон через модуль GSM і вмикає пожежну тривогу.

PIR детектор руху (HC – SR501): Основна частина алгоритму полягає в тому, щоб зосередитися на вимірюванні напруги від датчика PIR. Він також включає фільтрацію входних вимірювань `SWSD_DeInit()` і `SNSD_Init()` використовується для деініціалізації та ініціалізації, потім знайдіть вихідну напругу шляхом фільтрації сигналу від датчика PIR.

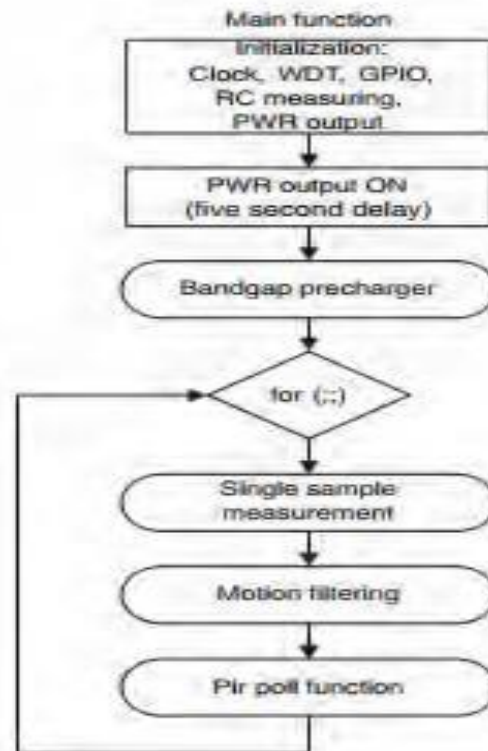


Рисунок 3.4: Блок-схема програмного забезпечення виявлення руху.

Оптический датчик пилу: Це аналоговий датчик. Для читання значення пилу використовується `analogRead()`. Для обчислення та перетворення в напругу: $\text{густина пилу} = 0,17 * \text{calcVoltage} - 0,1$. Він дає як вихідну напругу, так і щільність пилу. Результат буде показано на моніторі. Система надсилає текстове повідомлення на телефон, коли інтенсивність пилу підвищується.

LM 35 Прецизійний датчик температури: Цей датчик зчитує температуру в кімнаті та відображає її на ПК-моніторі. Система надсилає текстове повідомлення через GSM на телефон Android. Температура показана в градусах Цельсія. Починається з функції `analogRead()` і формула для Цельсія. Значення $\text{ADC} = \text{зразок} * 1024 / \text{еталонне значення}$.

Модулі: Назви інших модулів системи ми згадували раніше. Їхні програмні реалізації описані нижче: А. GSM Shield SIM900A:

Основні команди AT: для зміни режиму надсилання використовується така функція: `mySerial.println("AT+CMGF=1");`

Для читання SMS у текстовому режимі використовується така функція:
`mySerial.println("AT+CNMI=2,2,0,0,0");`

У цій системі GSM працює як двонаправлений передавач даних. Він має два типи функцій: відправник і одержувач.

Ми використовували GSM для керування будь-якою побутовою технікою на відстані. Bluetooth працює лише в персональній мережі (PAN). Ми можемо керувати всією побутовою технікою поза домом через GSM. Він працює як Bluetooth, але в більшій зоні мережі. Через Android ми можемо керувати світлом, вентиляторами, кондиціонером, телевізором, дверима тощо через GSM. Він отримує текстові повідомлення користувача та передає його мікроконтролеру для керування будь-яким приладом у будинку. Тут GSM працює як приймач.

Для системи безпеки GSM надсилає текстові повідомлення на основі всіх датчиків, які використовуються в цій системі. Якщо PIR-датчик відчуває будь-які незвичайні рухи всередині будинку, користувач отримує текстові повідомлення. Це означає, що хтось є в будинку за відсутності користувача. GSM також відіграє важливу роль у системі пожежної сигналізації за допомогою датчика температури LM35 і датчика газу. Коли температура піднімається дуже високо і виявляється СО (чадний газ), система надсилає текстові повідомлення через GSM.

Діапазони газових компонентів згадані вище у вступному розділі компонентів. Крім того, коли рівень запиленості приміщення підвищується, користувач отримує текстові повідомлення. Ці бездротові комунікації здійснюються як всередині, так і поза домом. Таким чином, користувач може отримати інформацію з усіх датчиків. Для цього не потрібна жодна програма Android або програма голосового керування. Тут GSM виступає як відправник.

Модуль Bluetooth HC-05: Швидкість передачі за замовчуванням для режиму AT становить 38400. Спочатку ми повинні вручну ввести режим AT.

Він продовжує читати дані після введення. Модуль Bluetooth передає команду та відображає її, коли команда надходить на монітор послідовного порту. Визначаючи швидкість зв'язку, ми використовували функцію налаштування () на місціпочати () ifindBaud(). Відправити команду в модуль функція cmd() використовується. Ключ (cmdPin) активується, щоб перевести модуль у командний режим, де розпізнаються команди «АТ». Стандартні функції запуску та завершення режиму використовуються для швидкості 38400. У нашій системі ми керуємо побутовою технікою через додаток Android через Bluetooth. Програма Android взаємодіє з мікроконтролером через Bluetooth. Перемикання побутової техніки – його основна функція. У цій системі ми лише надаємо команди системі з Android. Для керування побутовою технікою використовуються як програма голосового керування, так і програма Android. Жодна команда не повертається через Bluetooth.

4-канальне реле: Немає програмування для реле. Це лише частина апаратного підключення.

Модуль розпізнавання відбитків пальців (FPM10A): Однією з найважливіших частин цієї системи є модуль розпізнавання відбитків пальців. Розробляючи систему домашньої автоматизації, ми приділяли пріоритет питанню домашньої безпеки та намагалися знайти спосіб знайти рішення. Як ми знаємо, кожна людина має унікальний власний відбиток пальця, який відрізняється від усіх інших, і ми ставимо цю унікальність у завдання. Датчик відбитків пальців уже широко використовується для біометричної ідентифікації, і в нашому випадку ми використали ту саму технологію для забезпечення безпеки нашого проекту домашньої автоматизації. З інших біометричних даних ми вибрали цю, оскільки вона має найвищий рівень точності. Датчик, який ми використовували, досить легко отримати, і ми встановили датчик за допомогою Arduino Uno, оскільки він досить гнучкий у роботі. Як згадувалося раніше, ми дотримувалися алгоритму, який складається з двох кроків: реєстрації та відповідності друку.

Сканер, який ми використовуємо, розроблений для Arduino, і дані можна передавати на телефон Android. У цьому сканері алгоритм шукає виступи та лінії на кінці пальця там, де виступ розпадається на дві частини. Ці відмінні риси називаються дрібниціями. Замість того, щоб зіставляти цілий відбиток пальця, зіставлення цих деталей скорочує час обробки. Перше і головне, що потрібно зробити, це зареєструвати відбитки пальців, які ви хочете створити в базі даних. Щоб дозволити людям увійти в дім, їх відбитки пальців повинні бути зняті та збережені в системній пам'яті через процес реєстрації. Для цієї конкретної мети ми використовували коди Arduino під тією ж назвою, яка доступна в бібліотеці датчика. Сам датчик має внутрішню пам'ять для збереження до 256 типів різних відбитків пальців без зовнішньої пам'яті, що може навіть збільшити кількість. Дані користувача зберігаються на жорсткому диску комп'ютера як база даних.

Ми дали відбитки пальців трьом особам, щоб вони могли відкрити двері. Двері відкриваються лише тоді, коли відбитки пальців цих 3 осіб збігаються. Для повторного закриття дверей потрібна затримка 4-5 секунд. Для відкриття та закриття дверей є сервомотор. На наступному малюнку зображено крок:

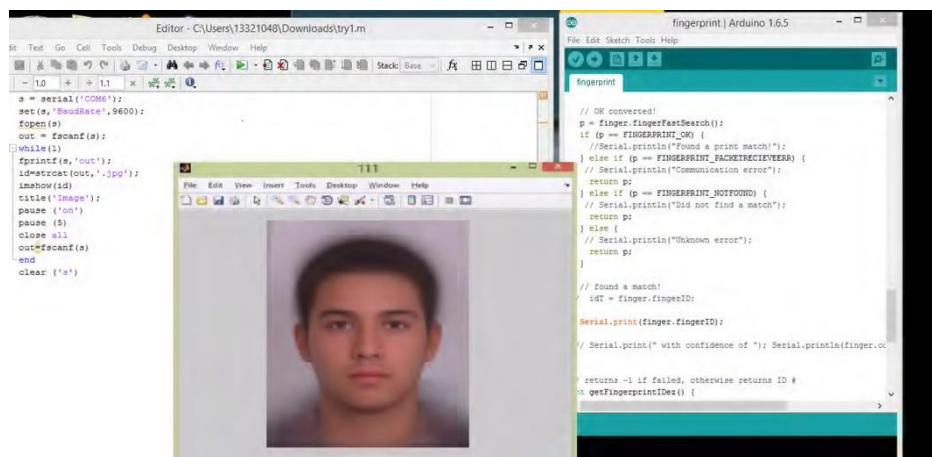


Рисунок 3.5: Скріншот коду програми у комп'ютері.

Модуль годинника реального часу DS1307: Код написаний в Arduino IDE 1.8.5. Нам потрібно імпортувати бібліотеку RTC DS1307 і Wire у ескіз. У цьому модулі немає аналогового зчитування. Цей модуль обчислює час, число, день, місяць і рік. Функції, які використовуються для цього модуля:

Щоб почати: `RTC.start( )`

Щоб зупинити: `RTC.stop( )`

Читання годинника: `RTC.readClock( )`

Читання часу: `RTC.getHours( )` `RTC.getDate( )` тощо. Час запису: `RTC.setHours( )`

`RTC.setMinutes( )` і так далі.

Нарешті, дата, день і час відображаються на РК-дисплеї та записуються всіма датчиками.

Програма Android: У цій системі ми маємо додаток Android для керування всією побутовою технікою. На телефоні Android ми вибираємо будь-який побутовий прилад із параметрів, які з'являються в програмі, а потім вибираємо УВІМК. або ВІМК. Це можна зробити лише тоді, коли користувач знаходиться в будинку. Для програми має бути з'єднання Wi-Fi. Користувач не може запустити програму поза домом, навіть якщо в телефоні є підключення до Інтернету. Це пов'язано з модулем Bluetooth. Це дозволяє встановлювати з'єднання точка-точка з пристроями підтримки Bluetooth. Ця технологія відома завдяки підтримці Android мережевого стека Bluetooth, який дозволяє обмінюватися даними без проводів.

Android Software Development Kit (SDK) надає всі необхідні інструменти для розробки Android Application (API). Ця програма є програмою на основі Java. Android використовує файл .apk для встановлення програми. Код написаний в Android Studio IDE. Першим з'явиться список кнопок усіх приладів. Потім користувачеві потрібно вибрати варіант. Пізніше з'являється кнопка дії УВІМК. і ВІМК. Є 2 макети структури коду, два коди

класу та код дозволу користувача. Вони написані в Android Studio IDE. Код пишеться відповідно до вигляду опцій в телефоні.

Щоб відкрити списки пристроїв:

```
import android.widget.Button; import android.widget.ListView;
```

Щоб створити змінні для Bluetooth:

```
private BluetoothAdapter myBluetooth = null; private Set<PairDevice>
```

Після ініціалізації записуються методи Java, які закінчуються кодом дозволу користувача. Потім код пишеться в Arduino IDE. Код починається з ініціалізації символів як "Рядок".

Програма для Android із голосовим керуванням: У цьому проекті ми також використовували додаток Android Voice для керування побутовою технікою. Усі побутові прилади можна **УВІМКНУТИ** або **ВИМКНУТИ** за допомогою голосової команди. Ми не називаємо це системою розпізнавання голосу, оскільки ця програма дозволяє кожному говорити. Це легко та гнучко для користувача, який можна використовувати з будь-яким мікроконтролером. Система отримує голосові команди від будь-кого. Голосовий додаток Google Assistant отримує звукову хвилю як «рядок» через спарені послідовні модулі Bluetooth і перетворює її на текст. Потім команда обробляється для роботи реле.

Якщо ми кажемо «Hello» телефону Android, він повертає рядок *Hello# до модуля Bluetooth.

«*» і «#» позначають початкові та стопові біти.

3.3. Принцип роботи системи

Після підключення та програмування всіх компонентів ми провели експеримент. Ми запустили всі компоненти відповідно до запропонованої системи. Ми розробили прототип будинку з розміщенням внутрішньої кімнати та зовнішніх дверей. Всі модулі та мікроконтролер зберігаються разом з великою кількістю проводів. Ця частина є головним центром системи

домашньої автоматизації. Датчики розміщуються всередині приміщення. Усі команди подаються з програми Android і голосової команди.

Вентилятор вмикається і вимикається за допомогою голосової команди.

Світло вмикається та вимикається за допомогою голосової команди. За допомогою датчика PIR визначається присутність людини, вмикається світло.

Коли рівень пилу зростає, на ньому відображається «потрібне очищення».

Штори закриваються та відкриваються завдяки інтенсивності світла, виміряній за допомогою LDR.

Система безпеки працює наступним чином:

Користувач прикладає палець до сканера; двері відкриваються, коли відбитки пальців збігаються. При скануванні відбитка пальця є затримка 3-4 секунди.

Текстове повідомлення надсилається на мобільний, коли температура дуже висока; температура вимірюється датчиком LM35. Для тестування системи оповіщення про пожежу ми використовували запальничку та тримали її біля LM35. РК-дисплей показує «витік газу» при виявленні диму та шкідливого газу. Одночасно сповіщається текстовим повідомленням. РК-дисплей показує виявлення крадіжки від другого датчика PIR. Сповіщення про зловмисника також надсилається за допомогою текстового повідомлення. Коли всі датчики знаходяться на високому рівні, п'єзозумер починає дзвонити. Коли в будинку виникає пожежа, сповіщення про високу температуру та задимлення надсилається через SMS.

Система надсилає текст, а також відображає його на моніторі, коли в будинку є витік газу.

Ще одна особливість цього проекту – автоматичне вмикання та вимикання світла. Коли датчик PIR виявляє присутність людини в будинку, світло вмикається автоматично. Світло вимикається, коли людина йде.

Останньою особливістю цього проекту є керування технікою за допомогою GSM та Voice App. Ми використовували спеціальні символи для окремого вмикання та вимикання світла та вентилятора. Мобільний телефон отримує команду як рядок із зазначенням стартового та стопового бітів. На обробку команди та роботу потрібно приблизно 2 секунди.

4. НАУКОВО-ДОСЛІДНА ЧАСТИНА

4.1 Дослідження розпізнавання особи.

В дослідженні були обрані волонтери. Десять користувачів зголосилися та запропонували відбитки пальців, щоб перевірити описані вище протоколи. Після отримання зображень відбитків пальців було згенеровано оцінки відповідності. Щоб краще відобразити результати тестування, були використані різні методи відображення результатів тестування.

На рисунках 4.1–4.8 створено графіки, які показують середню кількість точок артефактів, що збігаються для всіх десяти справжніх користувачів, і середні результати справжнього збігу для всіх десяти користувачів. Жоден користувач не помітив серйозних захворювань і мав середній вік 33 роки. Передбачалося, що користувачі не звикли до системи, оскільки кожен зразок був взятий у різних позиціях. На малюнку 4.1 показано середній результат збігу для всіх десяти користувачів під різними кутами повороту в порівнянні зі справжнім відбитком пальця користувача під кутом повороту 90 градусів. Слід зазначити, що кути повороту 85, 90 і 95 дають найвищі середні оцінки відповідності, а кут повороту 95 дає найвищу середню оцінку відповідності.

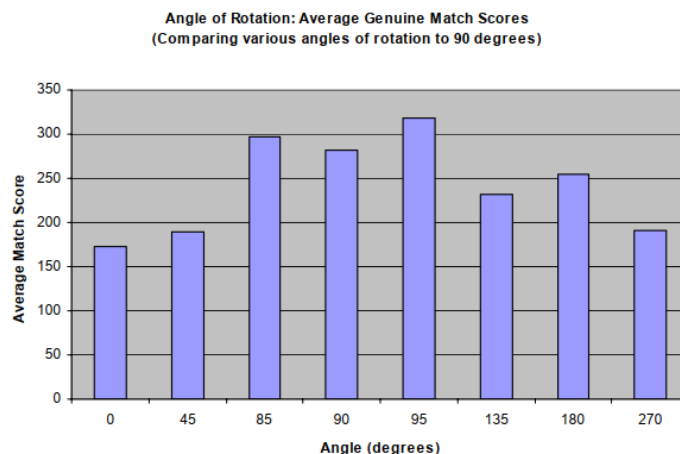


Рисунок 4.1. Середня оцінка справжньої відповідності від кута повороту

На рис. 4.2 показано середню кількість контрольних точок, зіставлених для всіх десяти користувачів під різними кутами повороту, у порівнянні зі справжнім відбитком пальця користувача під кутом повороту 90 градусів. Слід зазначити, що кути повороту 85, 90, 135 і 95 призвели до найбільшої середньої кількості збігів контрольних точок.

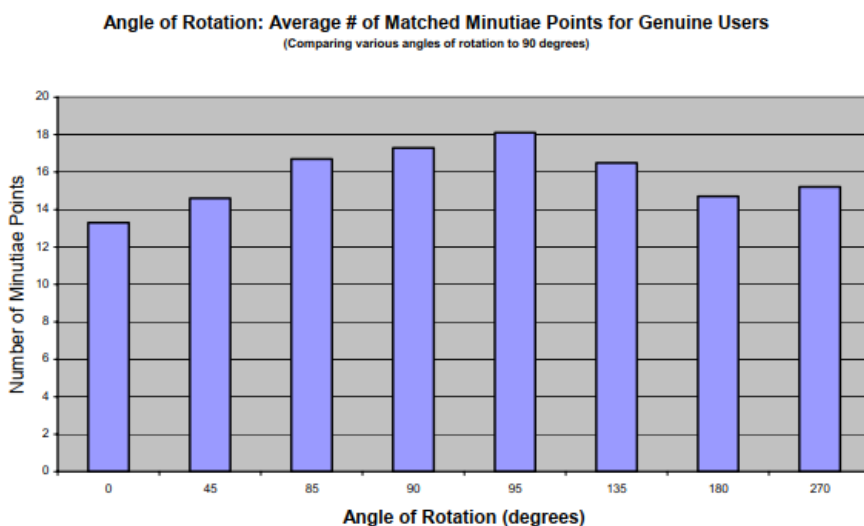


Рисунок 4.2. Середня кількість точок дрібниць, що зіставляються від кута повороту

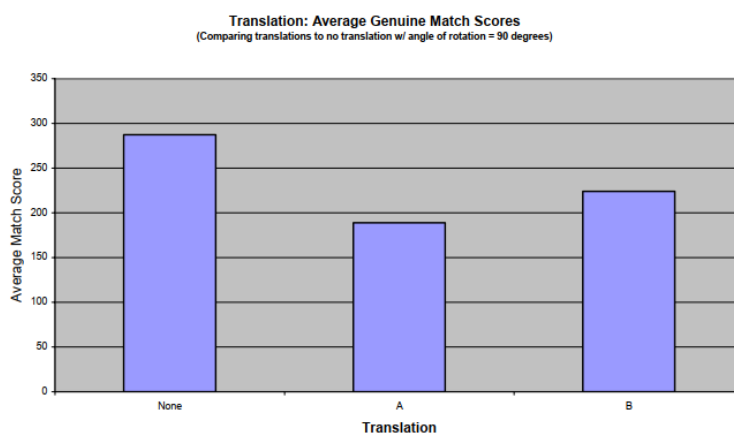


Рисунок 4.3. Середня оцінка справжньої відповідності для розпізнавання

На малюнку 4.3 показано середню оцінку збігу для всіх десяти користувачів у схемах перекладу в порівнянні зі справжнім відбитком пальця користувача під кутом повороту 90 градусів і без перекладу.

Коли використовувалися маски перекладу, як зазначено, датчик не зміг виявити палець, що призвело до FTA 100. Слід зазначити, що коли введено переклад, середній бал відповідності зменшується.

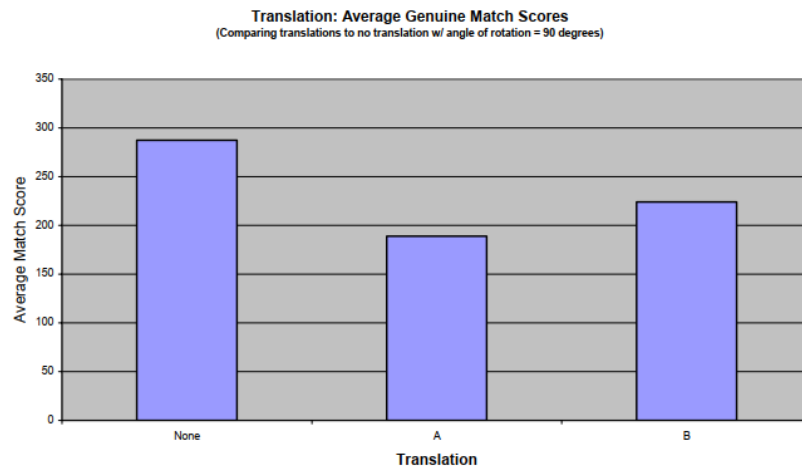


Рисунок 4.4. Середня кількість балів дрібниць, відповідних для розпізнавання

На рисунку 4.5 показано середню кількість точок артеактів для всіх десяти користувачів у схемах перекладу в порівнянні зі справжнім відбитком пальця користувача при куті повороту 90 градусів і без перекладу. Коли використовувалися трансляційні маски, як зазначено, датчик не зміг виявити палець, що призвело до FTA 100. Слід зазначити, що коли введено трансляцію, середня кількість узгоджених точок дрібниць зменшується.

На рисунку 4.5 показано середню оцінку збігу для всіх десяти користувачів при кутах розташування пристрою панорамування та нахилу +/- 20 градусів у порівнянні з справжнім відбитком пальця користувача при куті обертання 90 градусів і нульових градусах панорамування та нахилу. Коли датчик відбитків пальців було розміщено під кутом повороту та нахилу -20 градусів, це призвело до кращих вищих середніх балів відповідності.

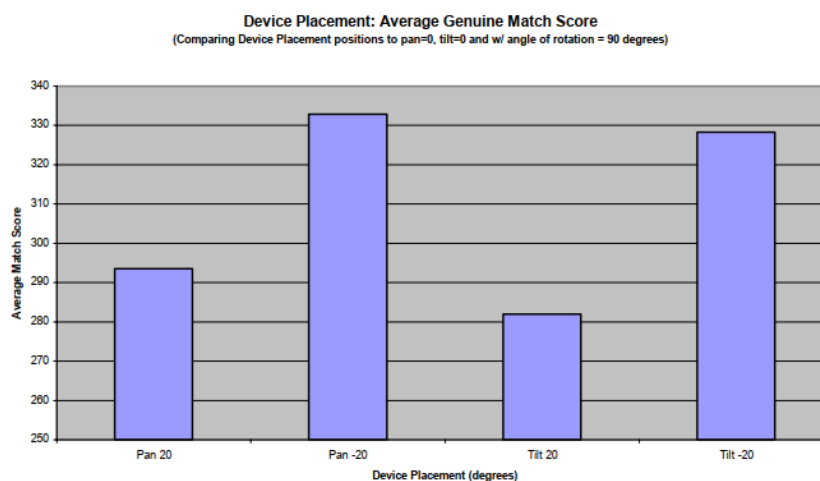


Рисунок 4.5. Середня оцінка справжньої відповідності від розміщення пристрою

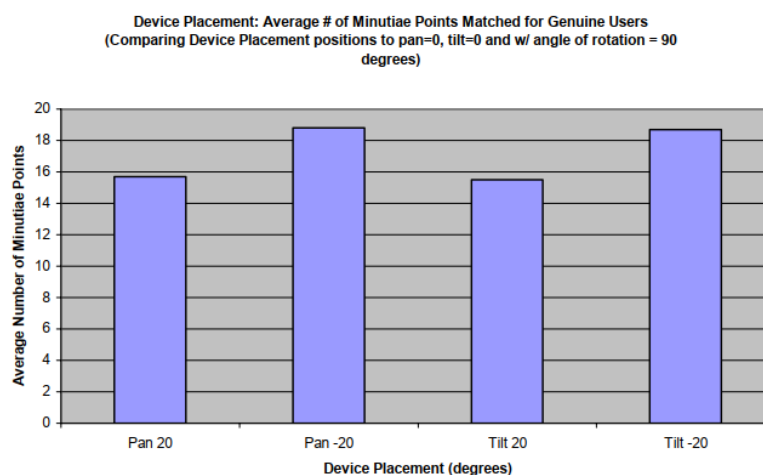


Рисунок 4.6. Середня кількість точок артефактів, які відповідають розміщенню пристрою

На рисунку 4.7 показано середню кількість контрольних точок для всіх десяти користувачів при кутах розташування пристрою панорамування та нахилу +/- 20 градусів у порівнянні з справжнім відбитком пальця користувача при куті обертання 90 градусів і нульових градусах панорамування та нахилу. Коли датчик відбитків пальців було розміщено під кутом повороту та нахилу -20 градусів, це дало більшу середню кількість узгоджених точок.

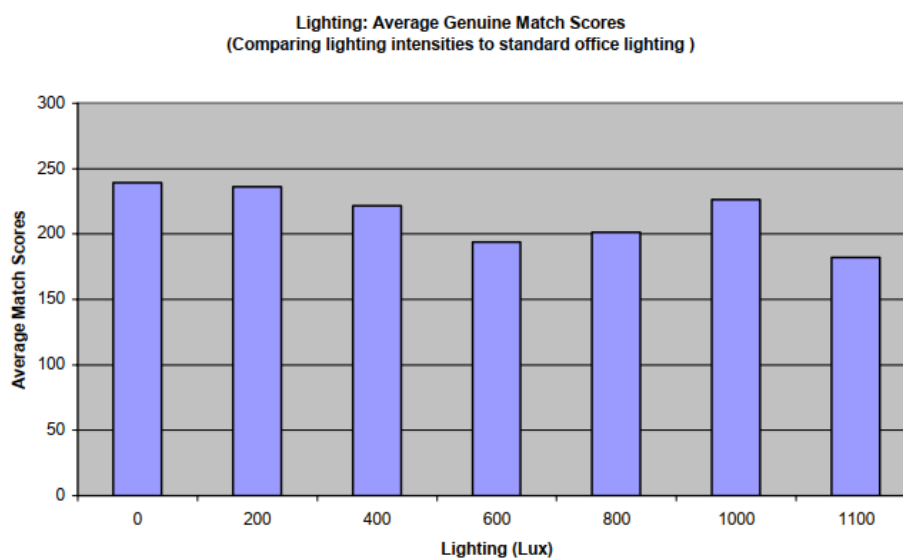


Рисунок 4.7. Середня оцінка справжньої відповідності від освітлення

На малюнку 4.8 показано середній результат збігу для всіх десяти користувачів за різних умов освітлення порівняно зі справжнім відбитком пальця користувача під кутом повороту 90 градусів і за нормального освітлення. Коли датчик відбитків пальців був представлений у різних умовах освітлення, була помічена мінливість середніх результатів дослідження.

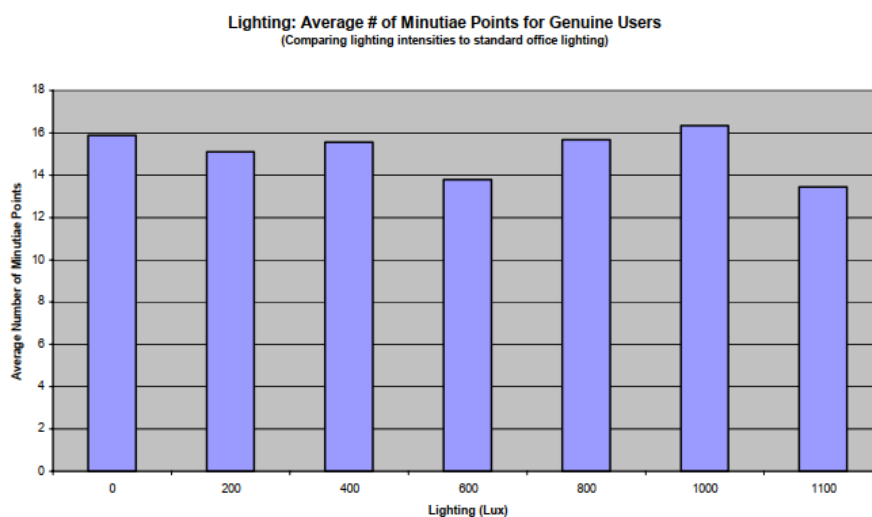


Рисунок 4.8. Середня кількість точок дрібниць, зіставлених від освітлення

На рисунку 4.8 показано середню кількість точок дрібниць для всіх десяти користувачів за різних умов освітлення порівняно зі справжнім

відбитком пальця користувача під кутом повороту 90 градусів і за нормального освітлення. Коли датчик відбитків пальців був представлений у різних умовах освітлення, була помічена мінливість у середній кількості точок, що збігаються.

Щоб показати відсоткову зміну середньої оцінки збігу в порівнянні зі справжніми зображеннями з кутом повороту 90 градусів, без перекладу та без розміщення пристрою для всіх чотирьох протоколів, перегляньте рисунки 4.9–4.12. На малюнку 4.9 показано відсоткову зміну середньої оцінки збігу для різних кутів повороту в порівнянні зі справжнім результатом збігу користувача під кутом повороту 90 градусів. Кути повороту 85, 90 і 95 демонструють невелику відсоткову зміну середнього результату матчу, тоді як інші кути повороту спричиняють зниження середнього результату матчу більш ніж на 10%.

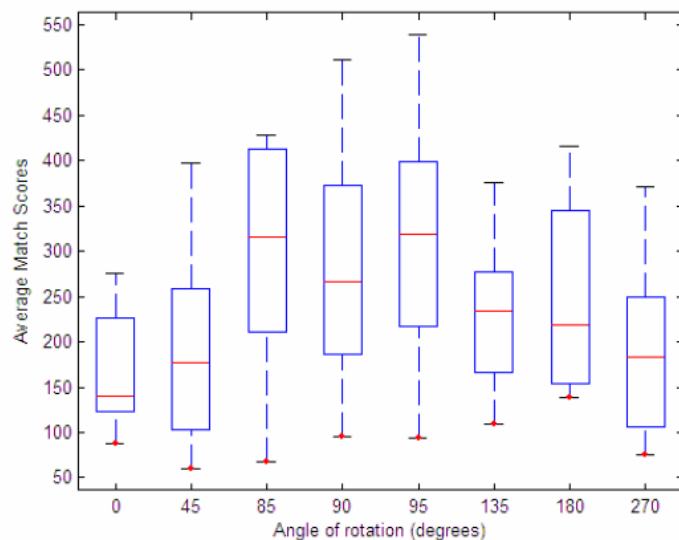


Рисунок 4.9. Відсоткова зміна середнього результату справжньої відповідності для кута повороту

На рисунку 4.10 показано відсоткову зміну середньої оцінки збігу для різних масок перекладу в порівнянні з оцінкою збігу справжнього користувача за кута повороту на 90 градусів і без перекладу. Переклад із

застосуванням масок А і В призвів до зниження середнього результату відповідності більш ніж на 20 відсотків.

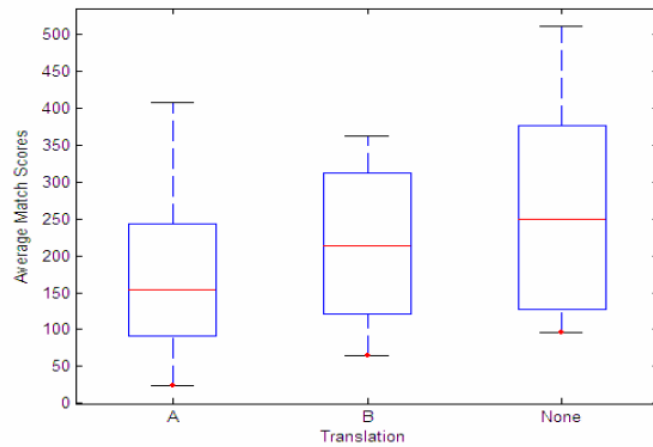


Рисунок 4.10. Відсоткова зміна оцінки справжньої відповідності порівняно

На малюнку 4.11 показано відсоткову зміну середнього результату збігу для різних кутів розташування пристрою в порівнянні зі справжнім показником відповідності користувача при куті повороту 90 градусів і кутах панорамування та нахилу 0 градусів. Кути панорамування та нахилу -20 градусів спричинили збільшення середніх результатів збігів у всіх користувачів більш ніж на 14 відсотків. У той час як кути панорамування та нахилу

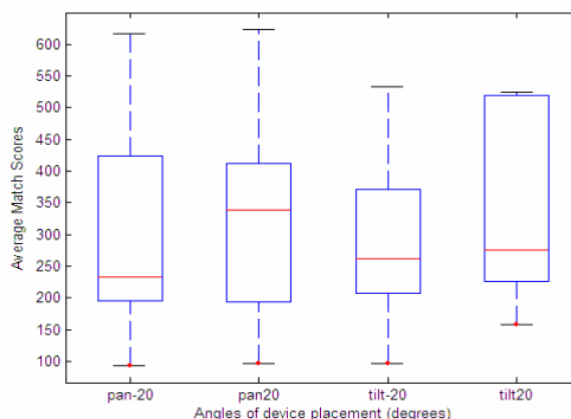


Рисунок 4.11. Відсоткова зміна середнього результату відповідності зі змінами в пристрої розміщення

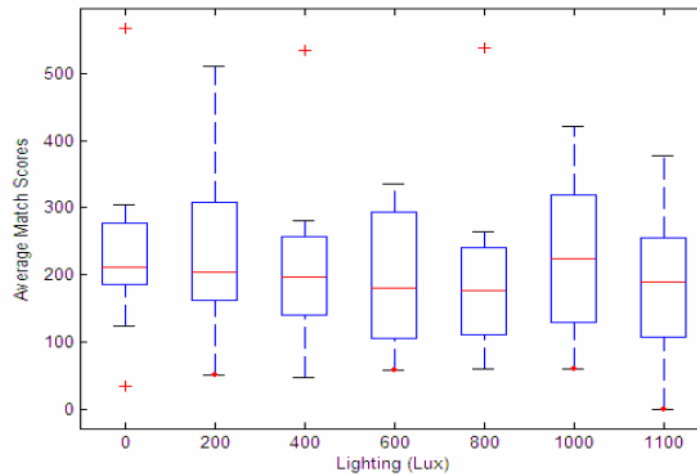


Рисунок 4.12. Відсоткова зміна середнього результату збігу зі змінами інтенсивності світла

На малюнку 4.12 показано відсоткову зміну середнього результату збігу для різних умов освітлення в порівнянні зі справжнім результатом збігу користувача під кутом повороту 90 градусів за нормального офісного освітлення. Ці результати показують, що коли джерело світла вводиться в цьому випадку, це призводить до зниження середньої оцінки відповідності. Коли люкс було встановлено на 1100, було виміряно зниження оцінки відповідності більш ніж на 35%.

Потім, щоб отримати більш детальне уявлення про результати збігів, для кожного протоколу було створено коробкові графіки. Boxplots створюють коробку та вусову ділянку. Рамка має лінії у верхньому та нижньому кuartилях, а також у медіані. Вуса — це лінії, що виходять із коробки, щоб показати решту даних. Дивіться малюнки 46-49 для цих коробкових діаграм. На малюнку 46 показана коробкова діаграма середніх результатів справжньої відповідності під різними кутами повороту для всіх десяти користувачів у порівнянні з відбитком пальця, розміщеним під кутом повороту 90 градусів. Як згадувалося раніше, кути обертання 85, 90 і 95 дали набагато високі оцінки збігу, ніж кути обертання на більшій відстані.

На рисунку 4.9 показана коробкова діаграма середніх оцінок справжнього збігу при різних перекладах для всіх десяти користувачів у порівнянні з відбитком пальця, розміщеним під кутом обертання 90 градусів і без перекладу. Як згадувалося раніше, переклад на точках А і В дав набагато нижчі оцінки відповідності, ніж відсутність перекладу.

На рисунку 4.10 показана коробкова діаграма середніх оцінок справжнього збігу під різними кутами розміщення пристрою для всіх десяти користувачів у порівнянні з відбитком пальця, розміщеним під кутом обертання 90 градусів і кутом панорамування та нахилу нуль градусів. Існує деяка помітна мінливість середнього результату відповідності, коли кути панорамування та нахилу були змінені.

На рисунку 4.12 показана коробкова діаграма середніх результатів справжньої відповідності за різних умов освітлення для всіх десяти користувачів у порівнянні з відбитком пальця, розміщеним під кутом обертання 90 градусів, і за нормального офісного освітлення.

5. СПЕЦІАЛЬНА ЧАСТИНА

5.1 Програмне забезпечення для збору даних

Програмне забезпечення для збору даних використовувалося в цьому дослідженні, щоб допомогти в документуванні інформації про користувача та навколишнього середовища, важливої для тестування. Мета цього програмного забезпечення – допомогти зменшити кількість помилок збору даних, що, сподіваємось, призведе до більш точних результатів тестування.

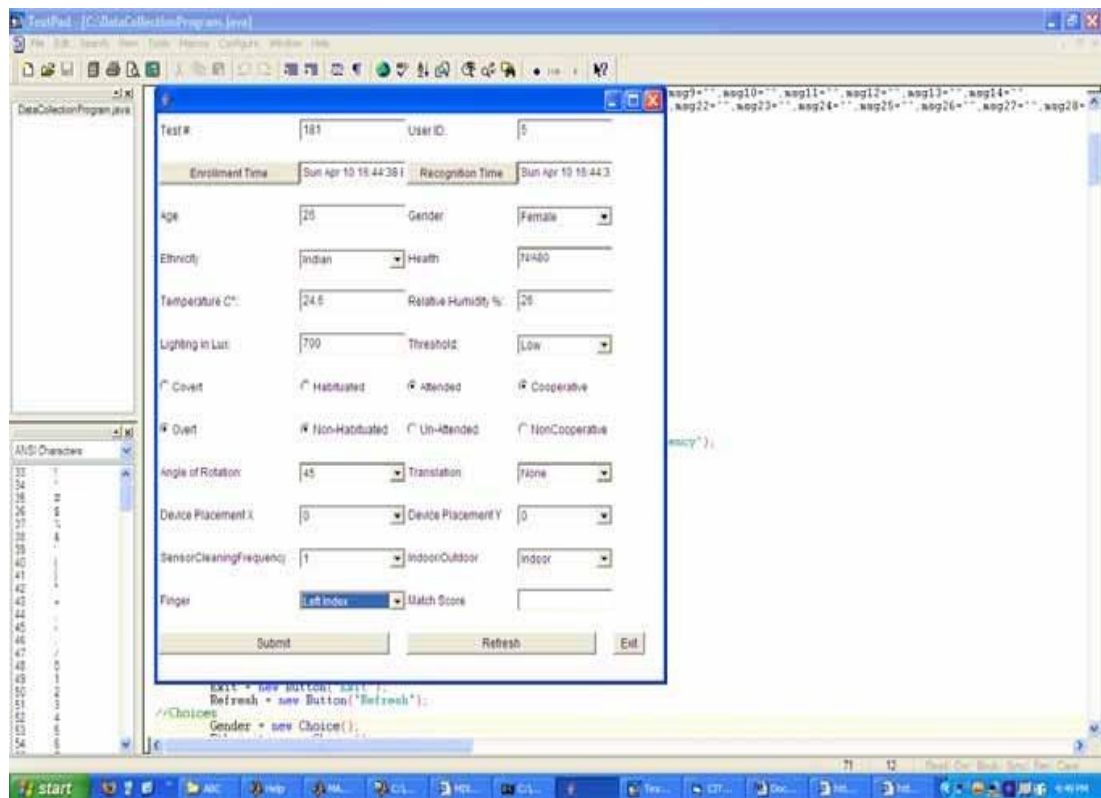


Рисунок 5.1. Знімок екрана програми збору даних

- Verifinger: модифікована версія

Після того, як необроблене зображення було зроблено, модифікована версія програмного забезпечення Verifinger версії 4.1 компанії Neurotechnology була використана для генерації результатів відповідності та визначення кількості точок дрібниць, що збігаються між двома відбитками пальців. Дивіться рисунок 5.2 для знімка екрана.

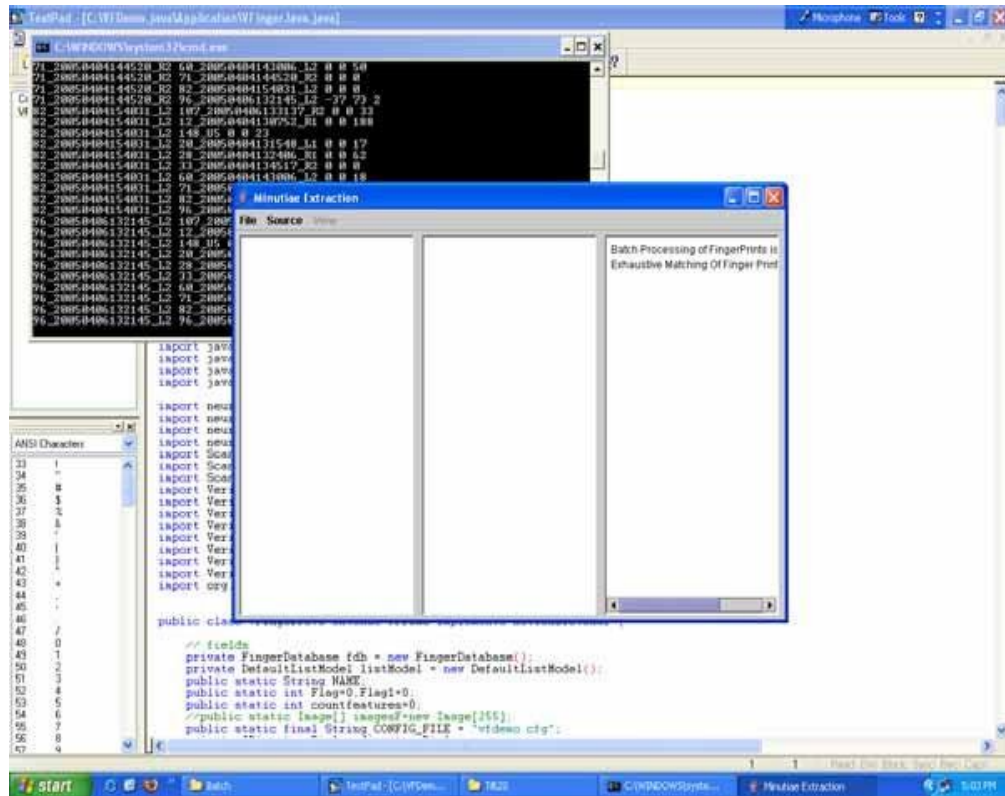


Рисунок 5.2. Знімок екрана програмного забезпечення Verifinger

- SecuGen SDK

Набір для розробки програмного забезпечення, використаний у цьому дослідженні, був для оптичного датчика відбитків пальців SecuGen Hamster. Програмне забезпечення називається FDX Development Kit від SecuGen.

- Програмне забезпечення для роботизованого штатива

Це програмне забезпечення поставляється разом із роботизованим штативом «Trackerrod», як зазначено вище. Програмне забезпечення має назву: TrackerCam, версія 5.12. Це програмне забезпечення керує «Trackerrod» через порт USB.

- Програмне забезпечення для захоплення необроблених зображень CITER

У цьому дослідженні програмне забезпечення для захоплення необроблених зображень, розроблене CITER (Центр досліджень технологій

ідентифікації), використовувалося для захоплення необроблених зображень у поєднанні з

SDK (набір для розробки програмного забезпечення) для оптичного датчика відбитків пальців Secugen Hamster. Це програмне забезпечення також використовувалося для збору даних для роботи, описаної в: [4]. Дивіться малюнок 27 для знімка екрана.



Рисунок 5.3. Знімок екрана програми збору необроблених даних

5.2 Протоколи

У цьому дослідженні були розроблені протоколи тестування на основі сценаріїв для незвичних і спільних користувачів у тестуванні, яке є присутнім і відкритим. Дослідження Розієка та Гупти визначили близько 50 змінних, які можуть впливати на продуктивність біометричної системи. У цьому сценарії тестування режим отримання зображення було обрано як основу для всіх протоколів тестування. Його було вибрано для тестування протоколів у режимі отримання зображень, оскільки зображення відбитків пальців низької якості важко зіставити та пропонують гіршу точність, ніж зображення відбитків пальців хорошої якості. Іншою причиною такого

вибору є те, що вихідні дані режиму отримання зображення використовуються режимами реєстрації, ідентифікації та перевірки, що розширює сферу тестування. Тому при розробці протоколів тестування важливо визначити, які змінні можуть впливати на режим отримання зображення, тобто впливати на датчик відбитків пальців під час отримання.

Протоколи були написані для зменшення систематичних помилок і врахування змінних, які можуть впливати на датчик відбитків пальців під час отримання зображення. Протоколи в Додатку А були написані для перевірки наступних змінних:

1. Біометрична презентація: кут повороту та переміщення
2. Освітлення
3. Розміщення пристрою

Протоколи були реалізовані таким чином:

- Екологічні палати

В ідеалі слід використовувати камери з контрольованим навколишнім середовищем, щоб допомогти контролювати фактори навколишнього середовища та покращити повторюваність тестування. У цьому дослідженні таких камер не було.

- Повторюваність тестування

Було зроблено багато кроків, щоб покращити повторюваність тестування. Було створено різні маски, щоб допомогти у повторюваності протоколів тестування. Програмний інструмент використовувався для документування умов навколишнього середовища, характеристик користувача (не імені) та інших змінних, щоб відстежувати кожен біометричний зразок і зменшити ймовірність помилок у звіті про дані тестування. Це програмне забезпечення було розроблено Gaurav Gupta.

- Збір даних

У цьому тестуванні використовувалося програмне забезпечення для захоплення необроблених зображень, розроблене для CITER, яке дозволяло

отримувати необроблені зображення відбитків пальців для датчика відбитків пальців SecuGen. Необроблені дані були зібрані для 10 користувачів для всіх протоколів, згаданих вище. Через обмеження часу та обмежену доступність користувачів для цієї роботи було можливе лише 10 користувачів. Було виконано кроки для наступних протоколів з деякими незначними змінами, як зазначено в цьому розділі: освітлення, біометричне представлення: кут обертання та трансляції та розміщення пристрою.

- Генерація рахунку збігів

Після того, як усі біометричні зразки були зібрані, аналіз цих зразків проводився в автономному режимі. Тестування в автономному режимі дозволяє проводити кілька тестів без повторного збору даних і більш глибокого аналізу. Використовуючи модифіковану версію програмного забезпечення Verifinger, згадану вище, на основі даних тесту було обчислено справжні та фальшиві результати. Результат кожного порівняння дає оцінку збігу, перенесення вздовж осей x і y , кут і кількість узгоджених контрольних точок. Для оцінки справжньої відповідності кожне зображення, зроблене кожним користувачем за протоколом, зіставляється із зображенням справжнього відбитка пальця користувача, зробленим під кутом обертання

У цьому дослідженні я обчислив показники збігу самозванців, порівнявши відбитки пальців справжнього користувача за кожним протоколом з іншими користувачами, відбитки пальців яких було розміщено під кутом обертання 90 градусів і без трансляції.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Організація охорони праці при роботі з системою управління

Охорона праці розглядає проблеми забезпечення здорових і безпечних умов праці. Виявляє і вивчає можливі причини нещасних випадків, професійних захворювань, аварій, вибухів, пожеж і розробляє систему заходів і вимог з метою виключення цих причин і створення безпечних і сприятливих для людини умов праці.

Завдання охорони праці є зведення до мінімуму імовірності пошкодження або захворювання працівників з одночасним забезпеченням комфорту при максимальній продуктивності праці.

Навчання працівників безпеці праці проводять відповідно до вимог ГОСТ 12. 0.004 - 79, який встановлює порядок і види навчання. На всіх підприємствах і в організаціях незалежно від характеру і ступеню небезпеки виробництва навчання працівників проводять при підготовці нових робітників, проведенні різноманітних видів інструктажів і підвищенні кваліфікації.

Контроль за своєчасним і якісним навчанням виконує відділ охорони праці чи інженер з охорони праці, або ІТП, на якого наказом керівника підприємства покладено ці обов'язки. Ті, що вперше поступають на роботу, навчання проходять згідно з "Типовим положенням про підготовку і підвищення кваліфікації робітників". В журналі обліку навчальної роботи реєструють навчальну тему, за якою проводилось навчання.

Інструктаж працюючих поділяють на вступний, початковий, на робочому місці, повторний, позаплановий і початковий.

Вступний інструктаж з усіма, хто поступає на роботу незалежно від їх освіти і стажу роботи по даній професії, проводить інженер з охорони праці за програмою, затвердженою головним інженером підприємства, про

проведення вступного інструктажу з обов'язковим підписом того, хто проводив інструктаж і того, хто його отримував.

Початковий інструктаж на робочому місці, повторний, позаплановий і поточний проводить керівник робіт.

Початковий інструктаж на робочому місці проводять при прийомі на роботу нових робітників за інструкцією з охорони праці, розробленою для окремих професій або видів робіт. Всі робітники після цього інструктажу і перевірки знань 2-5 змін (залежно від навичок і стажу роботи) працюють під наглядом бригадира чи майстра, потім оформляється допуск до їх самостійної праці.

Повторний інструктаж проходять всі працівники незалежно від кваліфікації, освіти і стажу роботи через три місяці. Його проводять з метою перевірки знання робітниками правил і норм з охорони праці.

Позаплановий інструктаж проводять коли змінилися правила охорони праці або технологічний процес, обладнання, інструмент та інші фактори, що впливають на безпеку праці; коли працівники порушують правила охорони праці, що можуть призвести чи призвели до травм, аварій чи пожежі, вибуху. Його проводять індивідуально чи з групою робітників однієї професії за програмою початкового інструктажу на робочому місці. При його реєстрації вказують причину, яка спричинила його проведення.

Умови праці мають велике значення практично для всіх виробничих показників - продуктивності праці, якості робіт, безпеки працівників та інше.

Санітарно-гігієнічні умови праці характеризуються показниками виробничого середовища - рівнем освітлення, мікрокліматичними параметрами, загазованістю і запиленістю повітряного середовища, рівнем шуму і вібрації, наявністю іонізуючого випромінювання та інше.

6.2 Електробезпека

Електричні установки, з якими доводиться мати справу практично всім працюючим по встановленню та налагодженню засобів автоматизації, виявляють для людини велику потенційну небезпеку, яка збільшується у зв'язку з тим, що органи чуття людини не можуть на відстані виявити присутність електричної напруги на обладнанні.

Степінь ураження електричним струмом залежить від цілого ряду факторів: значення сили струму, електричного опору тіла людини та тривалості протікання через неї струму, виду та частоти струму, індивідуальних властивостей людини та умов навколишнього середовища.

Конструкція електроустановок має відповідати умовам їх експлуатації та забезпечувати захист персоналу від дотику з струмоведучими та рухомими частинами, а обладнання - від попадання всередину посторонніх твердих тіл та води.

Конструкція, вид виконання, спосіб встановлення, клас ізоляції застосовуваних провідників, кабелів, пристроїв та іншого електрообладнання відповідають вимогам електробезпеки. За ступенем ураження людей електричним струмом котельня відноситься згідно ПУЕ 1.1.13 до категорії приміщень з підвищеною небезпекою (висока температура, можливість одночасного дотику до металевих елементів технологічного обладнання або металоконструкцій будинку та металевих корпусів електрообладнання).

У нормальному режимі роботи обладнання - можливість ураження працівників електричним струмом виключена. Але на випадок аварії для запобігання ураження струмом людей передбачене захисне заземлення. Згідно ПУЕ 1.7.65 допустимий опір заземлення повинен бути не більшим 10 Ом.

При виконанні монтажних робіт використовуються переносні електроінструменти (електродрилі, електрошліфувальні установки, тощо). Для забезпечення безпечної праці корпуси однофазних електроприймачів повинні занулюватись.

Захист людини від ураження електричним струмом в мережах з зануленням здійснюється тим, що при замиканні одної з фаз на занулений корпус в ланці цієї фази виникає струм короткого замикання, що діє на струмовий захист (плавкий запобіжник, автомат), в результаті чого відбувається відключення аварійної ділянки від мережі. Крім того, ще до спрацювання захисту струм короткого викликає перерозподіл напруги в мережі, що приводить до зниження напруги корпусу відносно землі. Таким чином, занулення зменшує напругу дотику та обмежує час, на протязі якого людина, що доторкнулася до корпусу, може потрапити під дію напруги.

Для того, щоб забезпечити швидке (на протязі декількох секунд) відключення аварійної ділянки, струм короткого замикання повинен бути достатньо великим. Відповідно до вимог ПУЕ струм короткого замикання повинен не менше ніж в три рази перевищувати номінальний струм плавкої вставки найближчого запобіжника або номінальний струм нерегульованого розчеплювача автоматичного вимикача. При використанні автоматичних вимикачів, що мають тільки електромагнітний розчіплювач (відсічку), струм короткого замикання повинен перевищувати значення струму встановлення миттєвого спрацювання в 1,25-1,4 рази в залежності від номінального струму.

В однофазних електроприймачів, що включені між фазним та нульовим робочим проводами, занулення корпусів слід виконувати з допомогою окремого (третього) провідника, який повинен з'єднувати корпус електроприймача з нульовим захисним проводом. В таких випадках під'єднувати корпуси електроприймачів для забезпечення електробезпеки до нульового робочого проводу недопустимо, оскільки при його розриві

(перегоранні запобіжника) всі під'єднані до нього корпуси виявляться під фазною напругою відносно землі.

В мережі з зануленням недопустимо використовувати заземлення окремих електроприймачів, не під'єднавши їх перед цим до нульового захисного провідника. В цьому випадку при замиканні фази на заземлений, але не приєднаний до нульового захисного провідника корпус створюється коло струму через заземлення цього корпусу та заземлення нейтралі джерела струму. Такий випадок небезпечний, оскільки засоби захисту не зможуть відключити такий електроприймач через мале значення струму і тому небезпечна напруга на всіх корпусах може зберігатися тривалий період, поки заземлений приймач не буде відключений вручну.

Важливо відмітити, що якщо занулений корпус одночасно заземлений, то це тільки покращує умови безпеки, оскільки забезпечує додаткове заземлення нульового захисного проводу.

Для ізоляції людини від частин електроустановок, що знаходяться під напругою, використовуються основні та допоміжні ізолюючі засоби, а саме слюсарно-монтажний інструмент з ізольованими ручками, коврики, ізолюючі підставки, тощо.

У приміщеннях, де знаходяться вимірювальні прилади, необхідно забезпечити виконання заходів по боротьбі з статичною електрикою (тобто прилади повинні бути заземлені). Найпростішим засобом є підтримка відносної вологості повітря на рівні 50 - 60 % за допомогою побутового електрозволожувача.

Підлогу слід виконувати відповідно до ГОСТ 12.4.124-83, використовуючи антистатичне покриття на проходах і біля робочих місць.

Робітникам рекомендовано носити одягу з природних матеріалів або з комбінованих - природних і штучних волокон. Для зняття електростатичних зарядів з одягу слід використовувати антистатики побутового призначення.

Оскільки корпуси приладів виконані з металу, то для усунення небезпеки ураження людини електричним струмом (можливий пробій на корпус приладу) використовується захисне заземлення.

6.3 Розрахунок заземлення

Розрахуємо систему заземлення для електроустаткування, яке працює від напруги 220 В.

$$R_{\text{заз}} \leq \frac{U}{I_p} = \frac{220}{66} = 3.3 \leq 4 \text{ Ом}$$

Визначаємо опір ґрунту: $\rho = \kappa_n * \rho_n = 2 * 200 = 400 \text{ Ом м}$,

де κ_n - коефіцієнт підсилення;

ρ_n — питомий опір ґрунту (вибирається з довідкової літератури).

Визначаємо опір одиночного вертикального заземлювача:

$$R_B = \frac{\rho}{2\pi} \left(\ln \frac{2l}{d} + \frac{1}{2} * \frac{4t+1}{4t-1} \right)$$

де t - відстань від середини заземлювача до поверхні ґрунту, м;

l, d - довжина і діаметр стержня заземлювача, м;

$$R_B = 96 \text{ Ом.}$$

Визначаємо опір сталевій полоси, що з'єднує стержневі заземлювачі:

$$R_{\text{л}} = (\rho / 2\pi l) * \ln(l^2 / dt) = 61 \text{ Ом.}$$

Визначаємо орієнтовне число стержневих заземлювачів:

$$n = R_B / [r_B] \eta_B = 96 / 4 * 1 = 24 \text{ шт.};$$

r_B - допустимий по нормам опір заземляючого пристрою,

η_B - коефіцієнт використання вертикальних заземлювачів (для орієнтовного розрахунку приймається рівним 1).

Приймаємо розміщення вертикальних заземлювачів по контуру з відстанню між стальними заземлювачами рівним 21. З довідкової літератури визначаємо $\eta_B = 0,66$ і $\eta_r = 0,39$.

Визначаємо необхідну кількість вертикальних заземлювачів

$$n = R_B / [r_B] \eta_B = 96 / (4 * 0.66) = 36$$

Розраховуємо загальний розрахунковий опір аземлюючого пристрою R з врахуванням з'єднувальної полоси

$$R = R_B R_{II} / (R_B \eta_r + R_{II} \eta_B n) = 3.9 \text{ Ом.}$$

Розрахунок проведено правильно, оскільки виконується умова $R \leq [r_B]$.

Розрахунок штучного заземлення:

Приймаємо, що опір захисного заземлення не повинен перевищувати 4 Ом:

$$R_{33} = \frac{R_c R_n}{R_c + R_n} \leq 4 \text{ Ом}$$

де R_{33} – опір захисного заземлення;

R_c – опір стержневих заземлювачів;

R_{II} – опір поперечних заземлювачів.

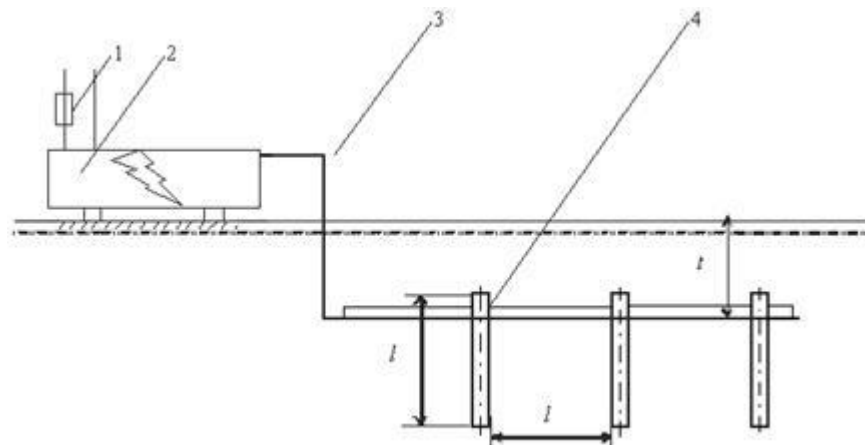


Рисунок 6.1 - Пристрій заземлення

4 – плавка вставка; 2 – електроустановка; 3 – з'єднувальна штаба; 4 – трубчатий заземлювач

Опір одиночного стержневого заземлювача розтіканню електричного струму:

$$R_{oc} = \frac{\rho_p}{2\pi l} \left(\ln \frac{2l}{d} + \ln \frac{4h' + l}{4h' - l} \right)$$

де h – відстань від поверхні ґрунту до заземлювача і становить 0,8 м;

l – довжина стержневого заземлювача 3 м;

d – діаметр стержневого заземлювача 50 мм.

$$R_{oc} = \frac{750}{2 \cdot 3,14 \cdot 3} \left(\ln \frac{2 \cdot 3}{0,05} + \ln \frac{4 \cdot 0,8 + 3}{4 \cdot 0,8 - 3} \right) = 39,8 \cdot (0,18 + 3,43) = 143,8 \text{ Ом}$$

Опір одиночного поперечного заземлювача:

$$R_{on} = \frac{\rho_p}{2\pi l} \ln \frac{2l^2}{bh'}$$

де l – довжина поперечного заземлювача 2,5 м;

b – ширина полоси заземлювача 30 мм;

ρ_p – розрахунковий опір ґрунту: для поперечних електродів 1000 Ом·м, для стержневих електродів 750 Ом·м.

$$R_{on} = \frac{1000}{2 \cdot 3,14 \cdot 2,5} \ln \frac{2 \cdot 2,5^2}{0,03 \cdot 0,8} = 63,7 \cdot 6,25 = 398,1 \text{ Ом}$$

В наслідок взаємовпливу вводимо коефіцієнт використання заземлювачів:

$$\eta = \frac{R_0}{nR_d}$$

де R_d – допустимий опір заземлення, що становить 4 Ом;

R_0 – опір одиночного заземлювача.

З цієї формули методом ітерацій підбирають n , при якому $\eta = 1$:

n	R_n	R_c	R_o	η
1	398,1	143,8	105,6	26,1
5	398,1	143,8	105,6	5,2
10	398,1	143,8	105,6	2,6
15	398,1	143,8	105,6	1,7
20	398,1	143,8	105,6	1,3
25	398,1	143,8	105,6	1,1
26	398,1	143,8	105,6	1,0
27	398,1	143,8	105,6	0,9

Отже приймаємо кількість одиночних заземлюючих електродів рівною

26.

ОСНОВНІ ВИСНОВКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

У роботі було розроблено автоматизовану систему ідентифікації особи з використанням ПЛК.

Було розглянуто основні аспекти процесу ідентифікації особи, основні параметри, як необхідно контролювати. Встановлено, що процес має характерні особливості та вимагає активного процесу керування в режимі реального часу.

Для побудови системи було описано технічні характеристики обладнання, розроблено конфігурацію системи, описано основні функції керування.

В роботі було розроблено систему ідентифікації особи з використанням ПЛК. На основі аналізу основних залежностей та моделей ідентифікації було розроблено ефективну систему розпізнавання на базі контролера ARDUINO.

Впровадження розробленої системи забезпечить захист будинків, офісів.

ПЕРЕЛІК ПОСИЛАНЬ

1. (2001). Interpreting Fingerprint Authentication Performance Technical White Paper. Fidelica Microsystems Inc.
2. Ashbourn, J. (2000). Biometrics: Advanced Identity Verification. Springer, London.
3. Bolle, R. M., Pankanti, S., & Ratha, N. K. (2000). Evaluation Techniques for Biometrics-Based Authentication systems (FRR). Yorktown Heights, NY: IBM.
4. Crihalmeanu, S., Ross, A., Govindarajan, R., Hornak, L., & Schuckers, S. A. C. (2004). A Centralized Web-Enabled Multimodal Biometric Database. Retrieved April 16, 2005 from <http://www.wvu.edu/~bknc/2004%20Abstracts/A%20Centralized%20Web-Enabled%20Multimodal%20Biometric%20Database.pdf>
5. Doddington, G. R., Pryzbocki, M. A., Martin, A. F., & Reynolds, D. A. (2000). The NIST Speaker Recognition Evaluation: Overview Methodology, Systems, Results, Perspective (31). Speech Communications.
6. Doddington, G., Liggett, W., Martin, A., Przybocki, M., & Reynolds, D. (1998). Sheep, Goats, Lambs, and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation. International Conference on Spoken Language Processing.
7. Fingerprint Verification Competition. Retrieved on 04/12/2005 from: <http://bias.csr.unibo.it/fvc2004/default.asp>
8. The Fingerprint Vendor Technology Evaluation (FpVTE). Retrieved on 04/12/2005 from: <http://fpvte.nist.gov>
9. Haas, N., Ratha, N. K., & Bolle, R. M. (2002). Pre-enhancing Non-uniformly Illuminated Fingerprint Images. Retrieved April 2, 2005 from <http://www.research.ibm.com/ecvg/pubs/norm-enhance.pdf>

10. Jain, A. K., & Ross, A. (September 2002). Learning User-specific Parameters in a Multibiometric System, Proc. of IEEE International Conference on Image Processing (ICIP), (Rochester, NY), pp. 57-60.
11. Jain, A. K., Ross, A., & Prabhakar, S. (Eds.) (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14 (4).
12. Kim, H. (2003). Evaluation of Fingerprint Readers: Environmental factors, Human Factors, & Liveness Detecting Capability. Retrieved April 2, 2005
13. Lawrence, O. (1999). Fingerprint Verification. In Jain, A., Bolle, R., & Pankanti, S. (Eds.),
14. Biometrics: Personal Identification in Networked Society (p. 43). Boston: Kluwer.
15. Maltoni, D., Dario, M., Jain, A., & Prabhakar, S. (2003). Handbook of Fingerprint Recognition. London: Springer.
16. Mansfield, A. J., & Wayman, J. L. (August 2002). Best Practices in Testing and Reporting Performances of Biometric Devices, Version 2.01 (NPL Report CMSC 14/02). UK: National Physical Laboratory.
17. Ratha, N. K., Connell, J. H., & Bolle, R. M. (Oct. 2001). Secure Fingerprint-Based User Authentication for Lotus Notes (). : ACM Multimedia and Security Workshop.
18. Rosiek, T., & Gupta, G. (2005). Generic Biometric System. West Virginia University Internal Technical Report.
19. Ross, A., & Jain, A. (2004). Biometric Sensor Interoperability: A Case Study In Fingerprints. Paper presented at the meeting of the International ECCV Workshop on Biometric Authentication (BioAW). Prague, Czech Republic.
20. Ross, A., Jain, A. & Qian, J. (June 2001). Information Fusion in Biometrics, Proc. of 3rd International Conference on Audio- and Video-Based Person Authentication (AVBPA), (Halmstad, Sweden), LNCS vol. 2091, pp. 354-359, Springer Publishers.

21. Ross, A., Dass, S., & Jain, A. (2004). Estimating Fingerprint Deformation. Paper presented at the meeting of the International Conference on Biometric Authentication. Hong Kong.
22. Ross, A., Dass, S., & Jain, A. (2005). A Deformable Model for Fingerprint Matching. *Pattern Recognition*, 38, 95-103.
23. Sandström, M. Liveness Detection in Fingerprint Recognition Systems. Retrieved on 04/14/2005 from <http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf>
24. Schuckers, M. E., Hawley, A., & Livingstone, K. (2004). A Comparison of Statistical Methods for Evaluating Matching Performance of a Biometric Identification Device- a Preliminary Report .
25. Speaks, D., Anderson, L., & Hutson, J. (2004). Biometric Performance Operational Testing and Reporting (M1/04-0216).
26. Tabassi, E., Wilson, C., & Watson, C. (2004). Fingerprint Image Quality (NIST 7151). Retrieved April 15, 2005 from http://fingerprint.nist.gov/NFIS/ir_7151.pdf
27. Valencia, V. (2004). Biometric Testing: It's Not as Easy as You Think. http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/bc076_ValenciaBrief.pdf
28. Whois.com. (2001, April 18). Retrieved April 16, 2005, from http://whatis.techtarget.com/definition/0,,sid9_gci542011,00.html
29. Wilson, C., Hicklin, K., Bone, M., Korves, H., Grother, P., Ulery, B., et al. (2004). Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report (NISTIR 7123).
30. Woodward, J. D., Webb, K. W., Newton, E. M., Bradley, M., & Rubenseon, D. (2001).
31. Army Biometric Applications: Identifying and Addressing Sociocultural Concerns. : RAND Corporation.

32. Woodward, J. D., Orlans, N. M., Higgins, P. T., (2003). Biometrics: Identity Assurance in the Information Age. (p. 187). Osborne: McGraw Hill.

33. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, "Магнолія 2006", 2013. – 256 с.

34. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) - Львів, "Магнолія 2006", 2014. – 312 с.

35. Микитишин А.Г., Митник, П.Д. Стухляк. Комплексна безпека інформаційних мережевих систем: навчальний посібник – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 256 с.

36. Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі: навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.

37. Введення в комп'ютерну графіку та дизайн: Навчальний посібник для студентів спеціальності 174 "Автоматизація, комп'ютерно-інтегровані технології та робототехніка"/Укладачі: О.В. Тотосько, П.Д. Стухляк, А.Г. Микитишин, В.В. Левицький, Р.З. Золотий - Тернопіль: ФОП Паляниця В.А., 2023 - 304с. <http://elartu.tntu.edu.ua/handle/lib/41166>.