Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І._____
« » червня 2023р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
спеціальність: 125 Кібербезпека

на тему: «Біометрична автентифікація за відбитками пальців»

оцінка « »

Голова ЕК

Лемешко О.В._____

Керівник доцент Мелкозьорова О.М.
(прізвище та ініціали/підпис)

Рецензент Д.т.н Краснобаєв В.А.
(прізвище та ініціали/підпис)

Виконавець студент групи КБ-42

Шрамко Н.В.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, висновків до кожного розділу, переліку посилань та додатків. Загальний обсяг 58 сторінки основного тексту, 21 рисунків, 4 таблиці, одного додатку. Перелік посилань містить 15 найменування. Загальний обсяг роботи 40 сторінок.

Метою роботи є розробка системи автентифікації на основі біометричної автентифікації за допомогою відбитків пальців.

Для досягнення поставленої мети необхідно розв’язати декілька задач. Потрібно проаналізувати методи біометричної автентифікації та визначити можливість застосування їх в системах керування доступом.

Розробити систему керування доступом на основі побудови системи автентифікації у якості сейфу.

Провести тестування розробленої системи керування доступом використанням біометричної автентифікації.

Об’єктами дослідження дипломної роботи є: процеси біометричної автентифікації, процеси керування доступом на основі системи доступу до сейфу з використанням сканування відбитків пальців.

Предметами дослідження дипломної роботи є: методи біометричної автентифікації, системи керування доступом.

Актуальність роботи полягає в побудуванні унікальної системи сейфу з використанням елементів та їх поєднання, котрих ще не використовували в у відомих ситуаціях та патентах.

Практична цінність роботи: Розроблено система керування доступом на основі сейфу з використанням біометричної автентифікації за відбитком пальця, яка дає змогу забезпечити санкціонований доступ користувачів до сейфу.

Ключові слова: АВТЕНТИФІКАЦІЯ, БІОМЕТРИЧНІ ДАНІ, МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ, ВІДБИТКИ ПАЛЬЦІВ, ПРОГРАМНИЙ ПРИСТРІЙ, ПРОГРАМОВАНА ПЛАТА, АРДУІНО.

ABSTRACT

The thesis consists of an introduction, three chapters, conclusions to each chapter, a list of references and appendices. The total volume is 57 pages of the main text, 21 figures, 4 tables, and one appendix. The list of references includes 15 items. The total volume of the work is 40 pages.

The aim of the work is to develop an authentication system based on biometric authentication using fingerprints.

To achieve this goal, it is necessary to solve several tasks. Analyze biometric authentication methods and determine whether they can be used in access control systems.

Develop an access control system based on the construction of an authentication system as a safe.

To test the developed access control system using biometric authentication.

The objects of research of the thesis are: biometric authentication processes, access control processes based on a safe access system using fingerprint scanning.

The subjects of the thesis are: biometric authentication methods, access control systems.

The relevance of the work is to build a unique safe system using elements and their combination that have not yet been used in known situations and patents.

Practical value of the work: A safe-based access control system using biometric fingerprint authentication has been developed, which allows for authorized user access to the safe.

Keywords: AUTHENTICATION, BIOMETRIC DATA, BIOMETRIC AUTHENTICATION METHODS, FINGERPRINT, SOFTWARE DEVICE, PROGRAMMABLE BOARD, ARDUINO.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК	портативний комп’ютер
ПЗЗ	прилад із зарядовим зв’язком
КМОН	комплементарна структура метал-оксид-напівпровідник
МК	мікроконтролер
ОЗП	оперативна пам’ять;
ПЗУ	постійний записуючий пристрій

ВСТУП

Системи автентифікації все більше стають частиною нашого повсякденного життя завдяки стрімкому розвитку інформаційних технологій. Існують такі основні типи систем автентифікації: парольні, та біометричні. На сьогоднішній день широкого розповсюдження набули біометричні системи.

Майже у кожного зараз є смартфони з функцією автентифікації за відбитком пальця або обличчям. Головною перевагою біометричних систем, безсумнівно, є наявність зразка «з собою». На відміну від парольних систем, користувачеві не потрібно пам'ятати пароль, який можна забути.

Однією з найпоширеніших систем біометричної автентифікації є система автентифікації за відбитками пальців. Вважається, що відбиток пальця є унікальним і незмінним протягом усього життя.

Біометрична система працює за наступним алгоритмом: спеціальний пристрій зчитує відмінні риси користувача, з яких витягуються необхідні характеристики і зберігаються в базі даних. Для входу в систему користувач знову надає свої дані, а з бази даних вибирається необхідний еталон і порівнюється з отриманим зразком. Після цього приймається рішення про успішність або неуспішність автентифікації. Метою дипломного проекту є розробка системи автентифікації на біометричної автентифікації на основі сканування відбитків пальців та аналіз даного виду автентифікації у порівнянні з іншими методами біометричної автентифікації. Для реалізації поставленої задачі було обрано основним мікроконтролером - ардуіно. Поставлена мета досягається шляхом вирішення таких основних завдань: - огляд та аналіз існуючих методів порівняння відбитків пальців; - розробка структури демонстраційного комплексу; - реалізація системи на практиці та його тестування.

1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

1.1 Загальні відомості біометричної автентифікації за відбитками пальців

Біометрична автентифікація - це процес підтвердження автентичності кожної окремої особи на основі біометричних даних.

Біометрична автентифікація передбачає використання певної частини фізичного вигляду для ідентифікації. Це може бути відбиток пальця, сканування райдужної оболонки ока, сітківки або якась інша фізична характеристика. Можна використовувати як одну характеристику, так і декілька. Все залежить від інфраструктури та бажаного рівня безпеки. При біометричній автентифікації фізична характеристика, що перевіряється, зазвичай зіставляється з іменем користувача. Це ім'я користувача використовується для прийняття рішень після того, як особа пройшла автентифікацію. У деяких випадках користувач повинен ввести ім'я користувача при спробі автентифікації; в інших випадках для визначення імені користувача проводиться пошук по біометричному зразку.

Біометрична автентифікація виконується шляхом порівняння фізичного аспекту, який надається для автентифікації, зі збереженою копією. Наприклад, коли прикласти палець до зчитувача відбитків пальців для порівняння зі збереженим зразком. Якщо відбиток збігається зі збереженим зразком, автентифікація вважається успішною.

Для того, щоб налаштувати біометричну автентифікацію, необхідна відповідна інфраструктура. Після налаштування інфраструктури потрібно реєструвати користувачів. Деякі продукти дозволяють користувачам реєструватися безпосередньо, в той час як інші вимагають, щоб реєстраційний агент виконував реєстрацію за користувача. Наприклад автентифікація за відбитками пальців. Під час процесу реєстрації система попросить користувача надати зразок, фактично вона створить кілька зразків. Користувач прикладає

палець до зчитувача відбитків пальців. Система записує зображення відбитків пальців користувача. Система використовує кілька зображень для визначення точкового шаблону для ідентифікації відбитків пальців користувача [1]. Ці точки в основному є точками, розміщеними на різних ділянках відбитка пальця. Ці точки використовуються для позначення візерунка, утвореного відбитком пальця. Після того, як було взято достатню кількість зразків, щоб сформувати послідовний візерунок точок, цей візерунок зберігається і використовується як основа для подальшого порівняння під час автентифікації.

1.2 Аналіз проблем методів біометричної автентифікації за відбитками пальців

Біометрична автентифікація є досить надійним методом автентифікації і сьогодні використовується багатьма організаціями, але вона не позбавлена проблем і недоліків. Однією з проблем біометричної автентифікації є те, що вона зазвичай вимагає спеціального обладнання, такого як зчитувач відбитків пальців, сканер сітківки ока тощо. Це обладнання має бути встановлене і налаштоване на кожній системі (або кінцевій точці), яка буде використовуватися для входу в систему. Це обмежує загальну зручність використання рішення. Тому ми не можемо просто підійти до будь-якої системи і використовувати її для автентифікації. Це може бути особливо проблематично, коли користувач перебуває поза межами своєї організації (тобто працює віддалено або в дорозі), оскільки потрібна система, в якій встановлено необхідне обладнання та налаштовано відповідно до корпоративної політики. Крім того, вартість також може бути проблемою з біометрією. Спеціалізоване обладнання, необхідне для біометричної автентифікації, може бути дорогим і має бути придбане для всіх кінцевих точок автентифікації. Тому початкові інвестиції, необхідні для біометричного рішення, можуть бути досить значними.

Другою потенційною проблемою, пов'язаною з біометрією, є безпека. Частиною налаштування біометричного рішення є налаштування рівня чутливості для зразка. Рівень чутливості визначає, наскільки близький збіг потрібен для успішної автентифікації. Налаштування рівня чутливості може бути дещо складним. Якщо він встановлений занадто низько, один записаний зразок може потенційно відповідати декільком фізичним зразкам. Якщо його встановити занадто високим, ви можете заблокувати доступ до системи для тих, хто має законний дозвіл на доступ до неї.

Були також випадки, коли людям вдавалося зламати біометричну автентифікацію. Основна проблема полягає в тому, що в багатьох випадках біометрична автентифікація покладається лише на зображення, надане під час автентифікації, тому її можна обдурити за допомогою підробленого зображення (побачити багато прикладів цього в сучасних шпигунських фільмах). Щоб боротися з цим, деякі виробники біометричних технологій додають інші вимоги до своїх рішень для біометричної автентифікації. Наприклад, зчитувач відбитків пальців може також перевіряти температуру пальця, з якого знімається відбиток. Якщо температура виходить за межі нормального діапазону для людського тіла, система вважає, що відбиток пальця надається якимось фальшивим методом, і автентифікація не пройде [2].

З цих причин ми не бачимо багато інтернет-додатків, що використовують біометричну автентифікацію. Ми бачимо її більше в корпоративному середовищі, і часто вона використовується лише для певних додатків або за особливих обставин [3].

Приклад розпізнавання відбитку пальців зображено на рисунку 1.1.

Рисунок 1.1 – Сканування відбитку пальців

1.3 Аналіз основних методів біометричної автентифікації та їх застосування

Сучасні методи біометричної автентифікації поділяються на різні типи, але всі вони мають схожі цілі. Більше того, принцип їхнього функціонування також схожий: вони вимірюють та аналізують унікальні характеристики, притаманні конкретній людині, для того, щоб підтвердити її особу.

Тому фізичні документи поступово відходять у минуле і замінюються біометричною ідентифікацією. Можна також сказати, що сучасні технології пішли далеко вперед, дозволяючи людям розблоковувати мобільні пристрої за допомогою відбитків пальців або переказувати гроші за допомогою голосових команд.

Наразі, можна виділити п'ять найпоширеніших типів біометричних ідентифікаторів:

1) відбитки пальців;
2) обличчя;
3) голос;
4) райдужна оболонка ока;
5) візерунки вен на долоні або пальцях.

Наприклад, банкам потрібні біометричні дані, щоб надавати різні послуги дистанційно. Якщо хочемо відкрити рахунок або взяти кредит, то раніше потрібно було йти до відділення, тоді як зараз можемо отримати доступ до багатьох послуг по телефону [4].

Найпоширеніші типи біометричних систем: фізична біометрія та поведінкова біометрія.

Фізична біометрія.

За допомогою спеціальних пристроїв (сканерів, сенсорів та інших зчитувачів) біометричні дані людини зберігаються в базі даних. Система зберігає цю інформацію, наприклад, відбиток пальця, і перетворює його в цифрові дані. Потім, коли палець знову прикладають до сканера, система порівнює нові дані з тими, що зберігаються в її базі даних. Нарешті, система або підтверджує особу людини і надає їй доступ, якщо є збіг, або відхиляє запит, якщо ні.

Сучасні камери та відео-реєстратори смартфонів можуть легко розпізнавати обличчя за допомогою вбудованих сенсорів, що працюють на основі нейронних мереж. У цьому сенсі зображення стає ідентифікатором людини. Цю технологію можна використовувати не лише для розблокування телефонів, але й для більш складних завдань, таких як підтвердження покупок або доступ до фінансових послуг [5 - 8].

Поведінкова біометрія.

Поведінкова біометрія - це система розпізнавання, яка ідентифікує людину на основі динамічних або поведінкових характеристик. Ці характеристики можуть включати динаміку почерку та підпису, ритми голосу та мови, розпізнавання жестів, характеристики використання електронних пристроїв через швидкість набору тексту, те, як людина тримає смартфон або планшет, і навіть те, як вона ходить. Цей тип також відомий як пасивна біометрія, оскільки не вимагає активної участі користувача для проходження процесу автентифікації.

Ці динамічні методи автентифікації базуються на характеристиках поведінки людини. Вони оцінюють унікальну поведінку та підсвідомі рухи людини в процесі відтворення будь-якої дії.

Розпізнавання голосу - це технологія, яка поєднує в собі як фізичну, так і поведінкову біометрію, оскільки аналізує динамічні та статичні характеристики людського голосу одночасно.

Приклад розпізнавання голосу зображено на рисунку 1.2.

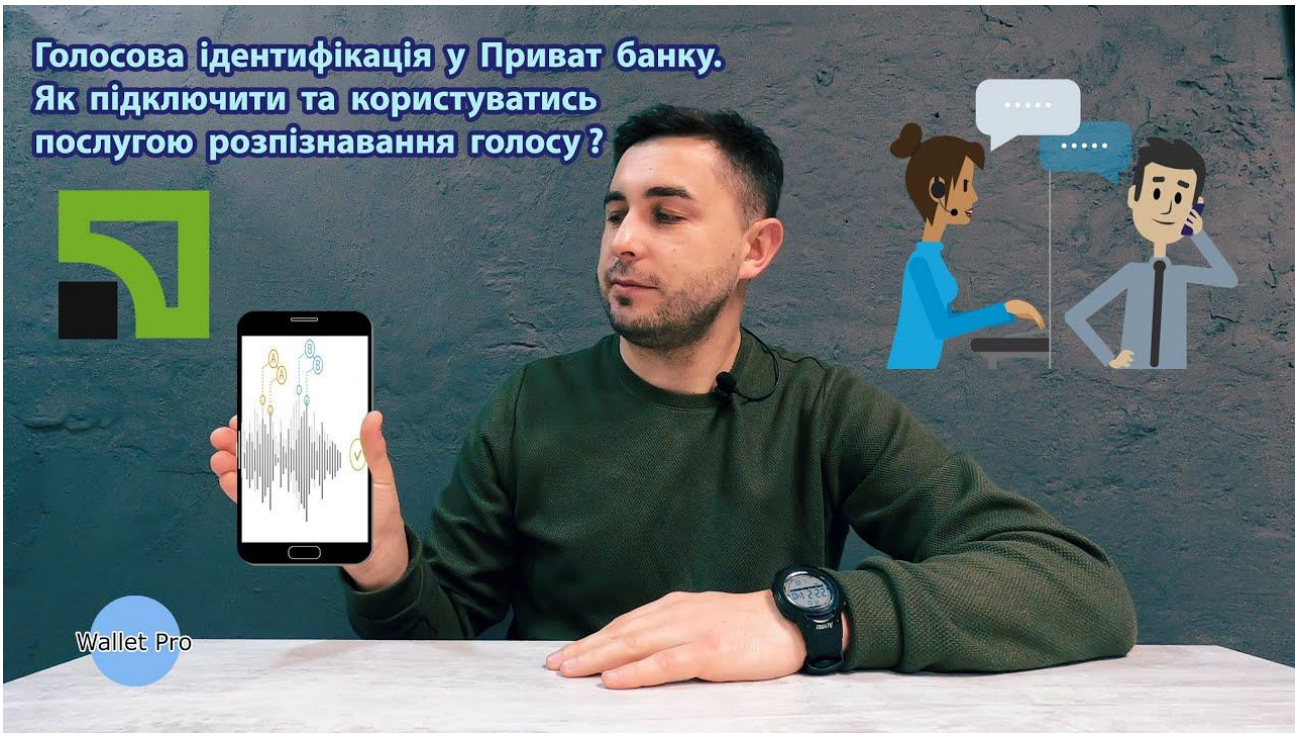


Рисунок 1.2 – Розпізнавання голосу у Приват банку

1.3.1 Аналіз біометричної автентифікації за допомогою розпізнавання голосу

Голос - це така ж невід'ємна риса кожної людини, як її відбитки пальців або обличчя. Той факт, що так багато компаній по всьому світу використовують телефони для спілкування, відкриває чудову можливість для використання цього методу біометричної автентифікації. Крім того, розпізнавання голосу є дуже зручним для користувачів і вимагає мінімальних зусиль з їхнього боку.

Технологія голосової біометричної автентифікації широко використовується в декількох сферах, безпосередньо пов'язаних з обробкою голосів користувачів, наприклад, в call-центрах. Впровадження цієї біометричної технології дозволяє прискорити обслуговування, полегшити роботу операторів і допомогти їм стати більш ефективними. Ця технологія може мати багато різних варіантів використання, таких як системи безпеки, верифікація кредитних карток, криміналістичний аналіз, телеконференції тощо. У великих проектах, особливо коли необхідно захистити конфіденційну інформацію, ідентифікація голосу може застосовуватися разом з іншим методом автентифікації, наприклад, скануванням відбитків пальців.

Переваги розпізнавання голосу:

1) не потрібно запам'ятовувати і потім використовувати пароль для автентифікації;
2) голос - це природний спосіб спілкування та взаємодії між людьми;
3) він економить час як для користувачів, так і для агентів, особливо при використанні пасивної голосової біометрії;
4) голос - це унікальна особливість, яку надзвичайно важко підробити;
5) це широко використовуваний метод, який добре знайомий користувачам.

Недоліки розпізнавання голосу:

1) користувачі можуть не розуміти, як зберігаються їхні дані, і мати занепокоєння щодо конфіденційності;
2) галасливі місця можуть перешкоджати успішній автентифікації;
3) важкі респіраторні захворювання можуть знизити відсоток успішної автентифікації.

1.3.2 Аналіз біометричної автентифікації за допомогою розпізнавання райдужної оболонки ока

Технологію сканування райдужної оболонки ока вперше запропонував у 1936 році офтальмолог Френк Бурш. На початку 1990-х Джон Дуфман з «Iridian Technologies» запатентував алгоритм виявлення відмінностей у райдужній оболонці ока. На даний момент цей метод біометричної автентифікації є одним з найточніших і здійснюється за допомогою спеціальних сканерів райдужної оболонки ока.

Дана технологія працює наступним чином: спочатку визначається місцезнаходження зіниці, потім - райдужна оболонка ока та повіки. Далі непотрібні частини, такі як повіки і вії, виключаються, щоб залишити тільки частину райдужної оболонки, яка ділиться на блоки і перетворюється в числові значення, що представляють зображення. Нарешті, порівняння з раніше зібраними даними виконується за допомогою тих же методів для перевірки ідентичності.

Переваги розпізнавання за райдужною оболонкою ока:

1) райдужка - це внутрішній орган, який добре захищений від пошкоджень високо прозорою і чутливою мембраною. Таким чином, навіть незначні пошкодження не можуть вплинути на скануючі пристрої;
2) райдужка є інваріантним органом з високим рівнем випадковості між окремими людьми;

3) не потрібно запам'ятовувати складні паролі.

Недоліки розпізнавання по райдужній оболонці ока:

1) ця технологія відносно нова і все ще потребує вдосконалення.
2) цей метод вимагає невеликої відстані між пристроєм і оком користувача.
3) в умовах низької освітленості шанси розпізнати райдужну оболонку ока дуже низькі.

Приклад розпізнавання радужної оболонки ока зображено на рисунку 1.3.

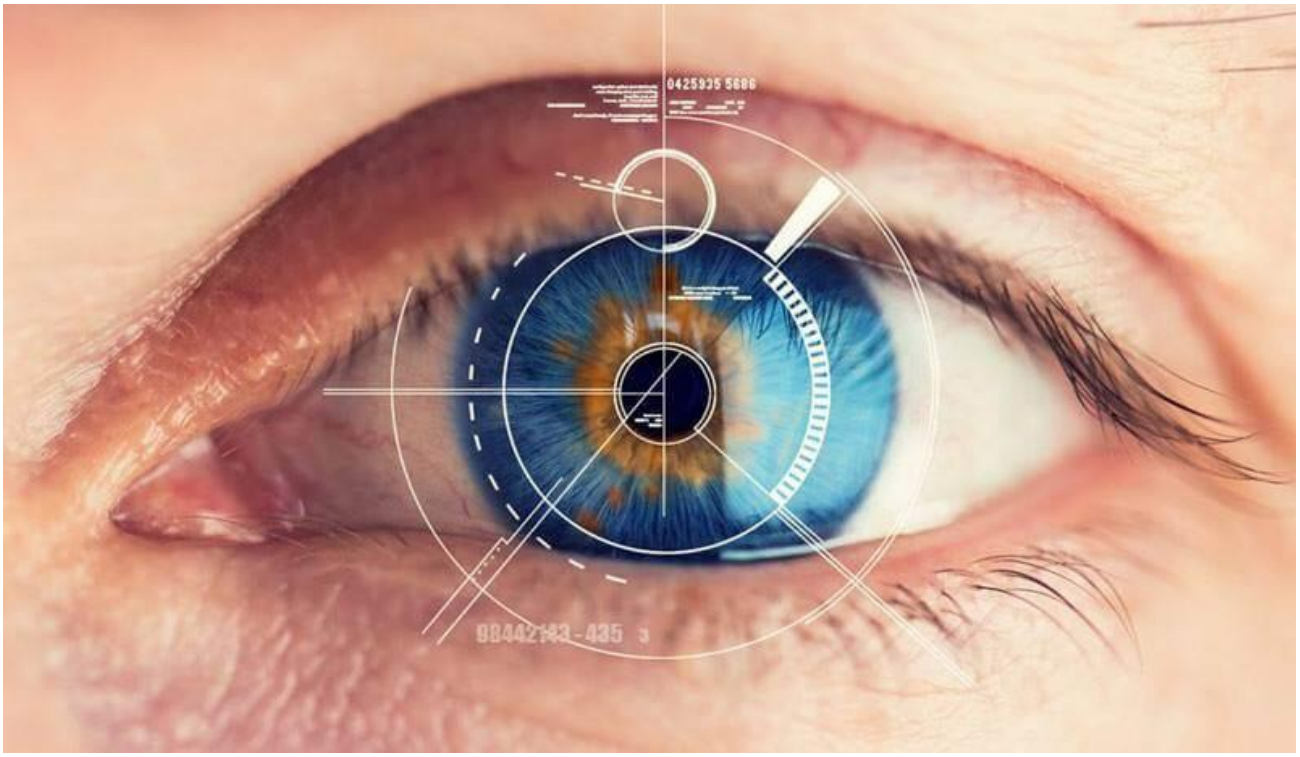


Рисунок 1.3 – Розпізнавання райдужної оболонки ока

1.3.3 Аналіз біометричної автентифікації за допомогою розпізнавання обличчя

Розпізнавання обличчя - це автоматична локалізація людського обличчя на зображенні або відео. При необхідності технологія розпізнавання обличчя може бути використана для підтвердження особи людини на основі наявних даних -

зображення обличчя людини, що зберігається в базі даних у вигляді математичного коду. Інтерес до цієї технології високий, оскільки цей метод можна застосовувати у відео-конференціях.

Переваги розпізнавання обличчя:

1) потребує мало взаємодії з пристроєм;
2) широко використовується, і люди звикли до такого типу технологій;
3) висока ефективність у поєднанні з іншими біометричними методами;
4) не потрібно запам'ятовувати складні паролі.

Недоліки розпізнавання обличчя:

1) зміна освітлення може вплинути на роботу системи;
2) вираз обличчя може змінити сприйняття обличчя системою;
3) використання аксесуарів для обличчя може ускладнити розпізнавання користувача;
4) деяким користувачам може бути незручно часто дивитися на свій телефон, щоб розблокувати його.

Приклад розпізнавання обличчя зображений на рисунку 1.4.

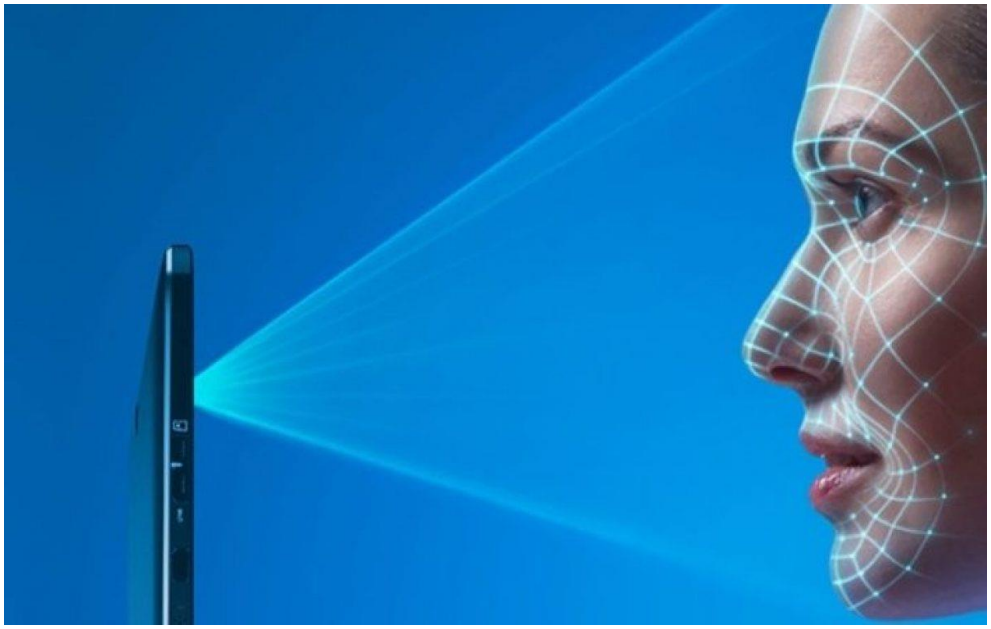


Рисунок 1.4 – Розпізнавання обличчя

1.3.4 Аналіз біометричної автентифікації за допомогою розпізнавання рукописного тексту

Динамічна перевірка підпису може застосовуватися в сферах, що вимагають автоматизації робочого процесу, наприклад, у банківській або судовій системах. Розпізнавання підписів базується на алгоритмах розпізнавання образів або математичних методах аналізу кривих, оскільки підпис може бути представлений набором точок. Тому ці системи часто використовують декомпозицію часових рядів або апроксимацію кривих.

Переваги розпізнавання рукописного тексту:

1) підписи використовувалися для підтвердження особи протягом століть. Тому ця технологія викликає довіру;
2) технологія не вимагає складних пристроїв для роботи (в наш час поширені пристрої з сенсорним екраном);
3) вона інтуїтивно зрозуміла, природна і не потребує багато пояснень.

Недоліки розпізнавання рукописного тексту:

1) багато людей мають непослідовні підписи;
2) травми, такі як зламані руки або пальці, можуть унеможливити використання цієї технології;
3) цей метод підходить лише для операцій з низьким рівнем безпеки.

Приклад Розпізнавання рукописного тексту зображено на рисунку 1.5

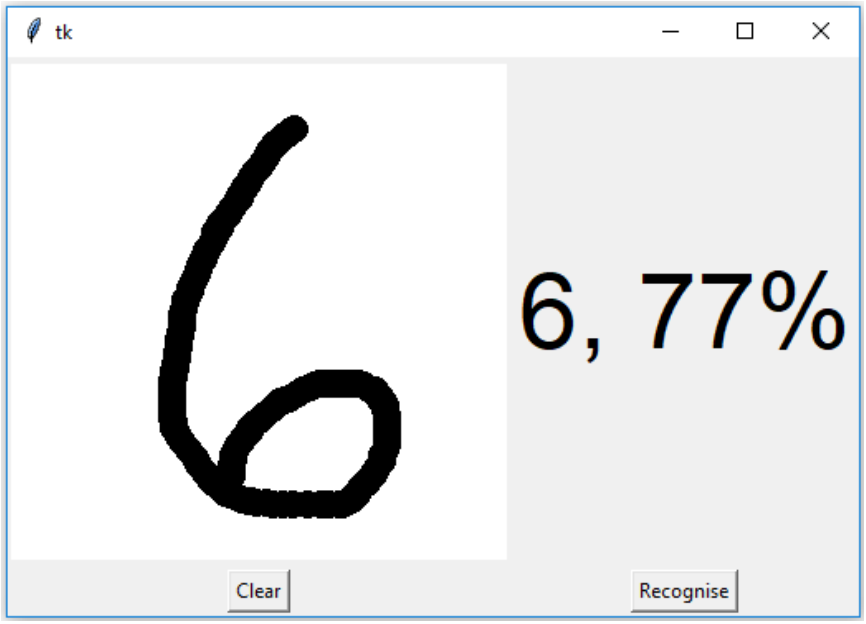


Рисунок 1.5 – Розпізнавання рукописного тексту

1.4 Порівняльний аналіз методів біометричної автентифікації

Для того щоб порівняти відносні характеристики треба зробити таблицю порівняння, більш точні показники: стійкість до фальсифікації даних, швидкість автентифікації, незмінність біометричних характеристик, можливість суворої автентифікації, вартості реалізації. Всі ці показники наведені нижче в таблиці 1.1.

Таблиця 1.1 – Порівняльний аналіз методів біометричної автентифікації

Біометричний метод	Стійкість до фальсифікації даних	Швидкість аутентифікації	Можливість суворої аутентифікації	Незмінність біометричних характеристик	Вартість реалізації
Відбиток пальця	Низька	Висока	Можлива	Низька	Низька
Розпізнавання обличчя	Низька	Середня	Ні	Низька	Середня

Продовження таблиці 1.1 – Порівняльний аналіз методів біометричної автентифікації

Райдужна оболонка ока	Висока	Висока	Можлива	Висока	Висока
Сітківка ока	Дуже висока	Дуже висока	Дуже висока	Дуже висока	Дуже висока

1.5 Висновки по розділу

Отже, було виділено основні методи біометричної автентифікації. Проаналізовано застосування цих методів на практиці та визначено основні недоліки та переваги цих методів. Можна виділити що найбільш доцільний з них є метод автентифікації за допомогою відбитків пальців, оскільки вона є досить надійним методом автентифікації і сьогодні використовується багатьма організаціями і згідно таблиці вона є найбільш кращої згідно виділених характеристик.

2 АНАЛІЗ МЕТОДІВ ПОРІВНЯННЯ ВІДБИТКІВ ПАЛЬЦІВ ТА МОДЕЛЮВАННЯ СИСТЕМИ

2.1 Аналіз характеристик відбитків пальців

Відбитки пальців рук - це унікальні візерунки, утворені гребнями тертя (піднятими) і борознами (заглибленими), які з'являються на подушечках пальців рук і великих пальців ніг. Відбитки долонь, пальців рук і ніг також є унікальними, але вони рідше використовуються для ідентифікації. Візерунок відбитку зображений на рисунку 2.1.

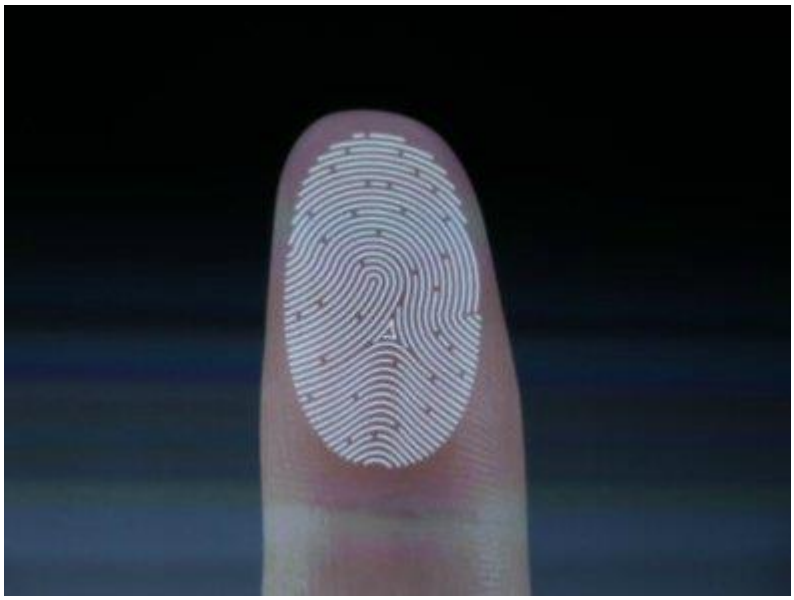


Рисунок 2.1 – Унікальний візерунок відбитку пальця

Візерунок відбитків пальців рук, наприклад, відбиток, що залишається при натисканні пальцем з чорнилом на папір, - це візерунок слідів тертя на даному пальці. Візерунки гребнів тертя поділяються на три різні типи - петлі, завитки та дуги - кожен з яких має унікальні варіації, залежно від форми та розташування гребнів:

Петлі - відбитки, які повторюються, утворюючи форму петлі. Поділяються на радіальні (спрямовані до променевої кістки, або великого пальця) і ліктьові

(спрямовані до ліктьової кістки, або мізинця), петлі складають приблизно 60 відсотків типів візерунків. Зображення такого виду зображено на рисунку 2.2.

Рисунок 2.2 – Зображення відбитків у формі петель

Завитки - утворюють кругові або спіральні візерунки, схожі на крихітні вири. Існує чотири групи завитків: звичайні (концентричні кола), центральна кишенькова петля (петля з завитком на кінці), подвійна петля (дві петлі, що створюють S-подібний візерунок) і випадкова петля (неправильної форми). Завитки складають близько 35 відсотків типів візерунків. Даний вид відбитків зображено на рисунку 2.3.

Рисунок 2.3 – Зображення відбитків у формі завитків

Арки - створюють хвилеподібний візерунок і включають в себе прості арки і шатрові арки. Шатрові арки піднімаються до більш гострої точки, ніж прості арки. Арки складають близько п'яти відсотків усіх типів візерунків. Даний вид відбитків зображено на рисунку 2.4.

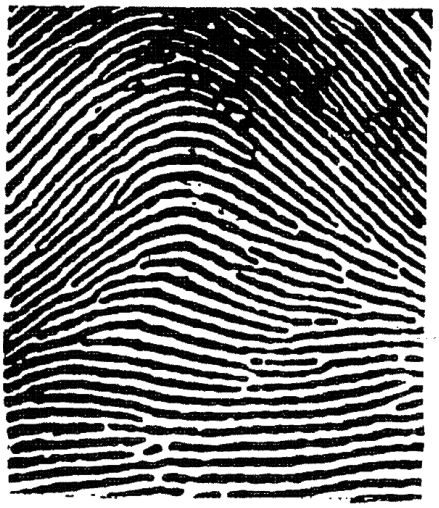


Рисунок 2.4 – Зображення відбитків у формі арки

Дві основні передумови ідентифікації за відбитками пальців - це унікальність і персистентність (незмінність). На сьогоднішній день ще не було виявлено двох людей з однаковими відбитками пальців, включаючи однояйцевих близнюків. Крім того, не було виявлено жодної людини, яка б мала однакові відбитки на кількох пальцях.

Персистентність, або перманентність, - це принцип, згідно з яким відбитки пальців людини залишаються практично незмінними протягом усього її життя. Коли утворюються нові клітини шкіри, вони залишаються зацементованими в існуючих гребнях і борознах тертя. Насправді, багато людей проводили дослідження, які підтверджують цю стійкість, записуючи одні й ті ж самі відбитки пальців протягом десятиліть і спостерігаючи, що їхні особливості залишаються незмінними. Навіть спроби видалити або пошкодити відбитки пальців будуть зірвані, коли нова шкіра відросте, якщо тільки пошкодження не

буде надзвичайно глибоким, в такому випадку нове розташування, викликане пошкодженням, збережеться і також буде унікальним.

2.2 Аналіз методів розпізнавання відбитків пальців

Розпізнавання відбитків пальців (іноді його називають дактилоскопія) - це процес порівняння досліджуваного і відомого відбитка пальця з іншим відбитком пальця, щоб визначити, чи є вони відбитками одного і того ж того самого пальця або долоні.

Існує велика кількість підходів до зіставлення відбитків пальців, які класифікуються в основному на три сім'ї.

На основі візерунків (на основі зображень) зіставлення - алгоритми на основі візерунків порівнюють основні шаблони відбитків пальців (дуга, спіраль і петля) між раніше збереженим шаблоном і відбитком пальця кандидата. Це вимагає, щоб зображення були вирівняні в одній орієнтації.

Для цього алгоритм знаходить центральну точку на зображенні відбитка пальця і центрує його на ній. В алгоритмі на основі шаблонів - шаблон містить тип, розмір і орієнтацію візерунків на вирівняному зображення відбитків пальців. Зображення відбитків пальців кандидата графічно порівнюється з шаблоном, щоб визначити ступінь вони збігаються.

Зіставлення на основі кореляції - два зображення відбитків пальців накладаються і обчислюється кореляція між відповідними пікселями обчислюється для різних вирівнюванню (наприклад, різних зсувів і поворотів).

Алгоритм сегментації - сегментація є одним з перших і найбільш невід'ємних етапів попередньої обробки для будь-якої перевірки відбитків пальців і визначає результат аналізу та розпізнавання відбитків пальців.

Роберт Гастінгс розробив метод для посилення гребеневого візерунка за допомогою процесу орієнтованої дифузії шляхом адаптації анізотропної дифузії для згладжування зображення у напрямку, паралельному потоку хребта.

Інтенсивність зображення плавно змінюється при проходженні вздовж хребтів або долин, видаляючи більшість дрібних нерівностей видаляючи більшість дрібних нерівностей і розривів, але при цьому ідентичність окремих хребтів і долин зберігається.

Бхупеш Гур та ін. розробили метод вилучення дрібних деталей із зображень відбитків пальців, використовуючи середню точку хребта контурного представлення. Першим кроком є сегментація для відокремлення переднього плану від фону зображення відбитків пальців. Із зображення виділяється область 64x64. Інтенсивність градацій сірого в областях 64x64 нормалізуються до постійного середнього значення та дисперсії, щоб усунути вплив шуму датчика шуму датчика та варіацій відтінків сірого, спричинених різницею різниці тиску пальців. Після нормалізації контрастність хребтів підвищується шляхом фільтрації нормалізованих вікон 64x64 за допомогою відповідним чином налаштованим фільтром Габора. Обробка зображення відбитків пальців сканується зверху вниз донизу і зліва направо, а також переходи від білого (фон) до чорного (передній план) і визначаються переходи від білого (задній план) до чорного (передній план). Вектор довжини обчислюється у всіх восьми напрямках контуру. Кожен елемент контуру представляє собою піксель на контурі, містить поля для x, y координат пікселя.

Запропонований метод займає менше часу і не виявляє помилкових дрібниць.

Алгоритми на основі шаблонів порівнюють основні шаблони відбитків пальців (дуга, котушка і петля) між раніше збереженим шаблоном і потенційним відбитком пальця. Для цього потрібно, щоб зображення були вирівняти в однаковій орієнтації. Для цього алгоритм знаходить центральну точку на зображенні відбитка пальця і центрується на ній. В алгоритмі на основі шаблону заснованому на шаблоні, шаблон містить тип, розмір і орієнтацію візерунків на вирівняному зображенні відбитків пальців.

Зображення відбитків пальців кандидата порівнюється графічно з шаблоном, щоб визначити ступінь їх збігу.

2.3 Аналіз вразливостей в системі біометричної ідентифікації

Оскільки ідентифікація головна частина автентифікації то всі вразливості повинні бути розглянуті в рамках даної дипломної роботи.

Внутрішні збої - це порушення безпеки через неправильне рішення прийнятого біометричною системою. Датчик може не отримати біометричні дані користувача через обмеження або умови технології вимірювання.

Варіації в умовах зйомки впливають на збір біометричних даних, і, таким чином, витягнуті ознаки зазвичай показують значну схожість між користувачами та внутрішньо-користувацькі відмінності.

Наприклад, зображення обличь двох однояйцевих близнюків дуже схожі між собою, і це може призвести до один до одного, і це може призвести до неправильного рішення при перевірці особи одного з близнюків.

При перевірці особи одного з близнюків. Частота помилок, з якою система біометричної верифікації неправильно зіставляє два не пов'язаних між собою біометричними шаблонами, називається частотою помилкових спрацьовувань(MTF).

І навпаки, система також може не зіставити два біометричні шаблони, отриманих з одних і тих самих біометричних даних, через значні внутрішньо-користувацькі варіації система - частота помилкових відмов (FRR).

Адміністративні атаки - це стосується всіх вразливостей через неправильного адміністрування біометричної системи. Це може статися через зловживання зловмисником функціями системи шляхом змови з системним адміністратором системи, або примушуючи його дозволити людині зареєструватися, бути прийнятою як реальний користувач.

Незахищена інфраструктура - тут зловмисник може маніпулювати біометричною інфраструктурою в апаратному, програмному забезпеченні та каналах зв'язку програмне забезпечення та канали зв'язку між різними модулями.

Доступ до біометричних характеристик - зловмисник таємно знімає біометричні дані легітимного користувача і використовує їх для створення фізичних артефактів. Так, якщо система не здатна відрізнити «живу» біометричну інформацію від штучної підробки, зловмисник може обійти систему, надавши їй фальшиві дані. Усі вразливості показані на рисунку 2.5.

Рисунок 2.5 - Вразливості в системі біометричної ідентифікації

2.4 Висновки по розділу

В розділі було переглянуто основні характеристики відбитків пальців. До основних характеристик можна віднести – візерунки, котрі поділені на основні три типи: петлі, завитки, арки. Також було розглянуто основні методи порівняння відбитків пальців, та проаналізовано вразливості в системі біометричної ідентифікації. Основуючись на всій необхідній інформації можна приступити до розробки самої системи автентифікації за відбитками пальців.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

3.1 Постановка вимог до системи

В даній роботі розробляємо та збираємо систему автентифікації за допомогою відбитків пальців.

Ця система повинна бути запрограмована, мати невисоку собівартість та задовольняти всі вимоги щодо характеристики точності та безпеки.

Ця система має представляти собою – систему автентифікації у вигляді сейфу.

Ця система повинна надавати фізичний доступ до об’єкту.

3.2 Принцип роботи системи автентифікації

Дана система надає доступ користувачеві, основою системи є мікроконтролер. Автентифікація користувача відбувається після того коли система отримала зображення відбитка пальця завдяки сканеру відбитків пальців.

Вся обробка інформації відбувається завдяки передачі та збереженні даних, котрі опрацьовуються за допомогою програмного забезпечення в мікроконтролері.

Структурну схему роботи зображено на рисунку 3.1, на якій відображено всі елементи готової системи.

Ця схема включає повністю готовий сейф з підключеними датчиками. Всі елементи ілюструють базові елементи котрі виконують основну роботу даної системи.

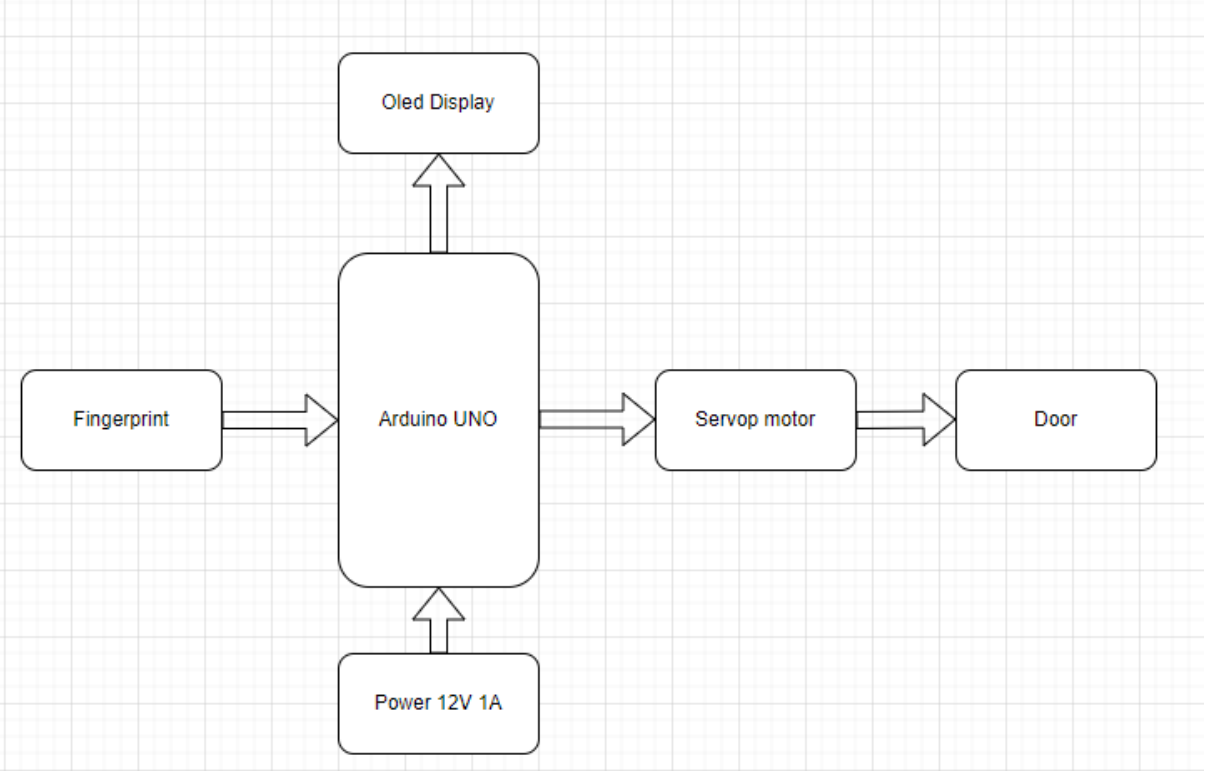


Рисунок 3.1 – Структурна схема системи сейфу

3.3 Обґрунтування та вибір елементів

Для вибору елементів було проведено дослідження ринку та базових статей про датчики котрі застосовуються для реалізації таких систем.

Виходячи з отриманих результатів дослідження найбільш кращі елементи та компоненти системи, були вибрані наступні:

1) Arduino UNO;
2) Servo sg922;
3) OledDisplayi2c;
4) R305 Fingerprint.

Дані компоненти виконуються всі базові вимоги даної системи та мають основні вимоги щодо безпеки. Завдяки цим елементам можемо створити повноцінну систему автентифікації.

3.3.1 Сканер відбитків пальців R305 Fingerprint

Оскільки технологія сканування відбитків пальців є одним з найпопулярніших біометричних методів підтвердження особи. При зіставленні відбитків пальців порівнюються унікальні особливості, такі як характеристики гребнів або дрібних візерунків, які містяться у візерунку відбитка ми використовуємо оптичний біометричний зчитувач/датчик відбитків пальців з модулем R305 та інтерфейсом TTL UART для прямого підключення до мікроконтролера UART. Користувач може зберігати дані відбитків пальців в модулі і може налаштувати його в режимі 1:1 або 1:N для ідентифікації особи. Цей модуль може безпосередньо взаємодіяти з будь-якими мікроконтролерами з напругою 3,3 або 5 В, але для підключення до послідовного порту ПК потрібен відповідний перетворювач рівня/послідовний адаптер.

Процес зчитування відбитків пальців зазвичай складається із захоплення зображення відбитка пальця, вилучення характерних рис відбитка, а потім зберігання цифрового шаблону відбитка пальця або порівняння поточного зображення зі збереженими шаблонами відбитків пальців.

Виходячи з усього вказано даний сканер можна застосувати для: блокування відбитків пальців, для розробки сейфу для відбитків пальців, для контролю доступу за відбитками пальців та інші випадки.

В таблиці 3.1 зображено основні характеристики даного датчика.

Таблиця 3.1 – Характеристики R305 датчика.

Вхідна напруга	4.2 В ~ 6.0 В
Робочий струм	110 мА
Час введення зображення відбитка пальця	<0.3 секунди
Рівень безпеки	П'ять (від низького до високого: 1,2,3,4,5)

3.3.2 Компонент системи Oled Display i2c

Оскільки система показуватиме що користувач успішно пройшов автентифікацію і отримав доступ до сейфу використовуватимемо дисплей котрий можна поєднувати з даними елементами системи.

Модель, яку ми використовуємо тут, має лише чотири контакти і зв'язується з Arduino за допомогою протоколу зв'язку I2C.

Для керування OLED-дисплеєм вкиористовуємо бібліотеки adafruit_SSD1306.h та adafruit_GFX.h.

Ці функцій, які можемо використати при роботі з системою завдяки бібліотеки OLED-дисплеїв для написання тексту або малювання простих графічних зображень:

1) display.clearDisplay() - вимкнути всі пікселі;
2) display.drawPixel(x,y, color) - намалювати піксель у координатах x,y;
3) display.setTextSize(n) - встановити розмір шрифту, підтримує розміри від 1 до 8;
4) display.setCursor(x,y) - встановити координати для початку написання тексту;
5) display.print(message) - виводить символи у позиції x,y;
6) display.display() - виклик цього методу для того, щоб зміни набули чинності.

3.3.3 Елемент системи Servo sg922

Для того щоб наша система надавала фізичний доступ використаємо сервопривід.

Цей елемент працює так само, як стандартні сервоприводи, але менші за розміром. Можемо використовувати будь-який код сервоприводу, апаратне забезпечення або бібліотеку для керування цим сервоприводом. Звичайно, він не такий потужний, як стандартні сервоприводи. Чудово працює з Motor Shield для

Arduino або просто підключивши бібліотеку сервоприводів. Поставляється з кількома рупорами та апаратним забезпеченням.

Для керування за допомогою Arduino підключимо помаранчевий дріт керування до контакту 9 або 10 і використаємо бібліотеку Servo, що входить до складу Arduino IDE.

В таблиці 3.2 вказано основні характеристики сервоприводу.

Таблиця 3.2 – Характеристики сервоприводу

Тип шестерні	Нейлон з вуглецевим волокном
Робоча швидкість	0.1 сек / 60 градусів (4.8v)
Робоча напруга	4.8v
Ширина зони нечутливості	1us

3.3.4 Мікроконтролер системи Arduino UNO

Arduino UNO - це стандартна плата Arduino. Ця плата вважається потужною платою, яка використовується в різних проектах. Arduino.cc розробила плату Arduino UNO .

Arduino UNO базується на мікроконтролері ATmega328P. Вона проста у використанні в порівнянні з іншими платами, такими як Arduino Mega тощо. Плата складається з цифрових і аналогових входів/виходів (I/O), екранів та інших схем [8, 9, 10].

Arduino UNO має 6 аналогових входів, 14 цифрових виводів, роз'єм USB, роз'єм живлення та заголовок ICSP (внутрішньо-схемне послідовне програмування). Вона програмується на основі IDE, що розшифровується як інтегроване середовище розробки. Вона може працювати як на онлайн, так і на офлайн-платформах.

IDE є спільним для всіх доступних плат Arduino.

Сама плата зображена на рисунку 3.2.

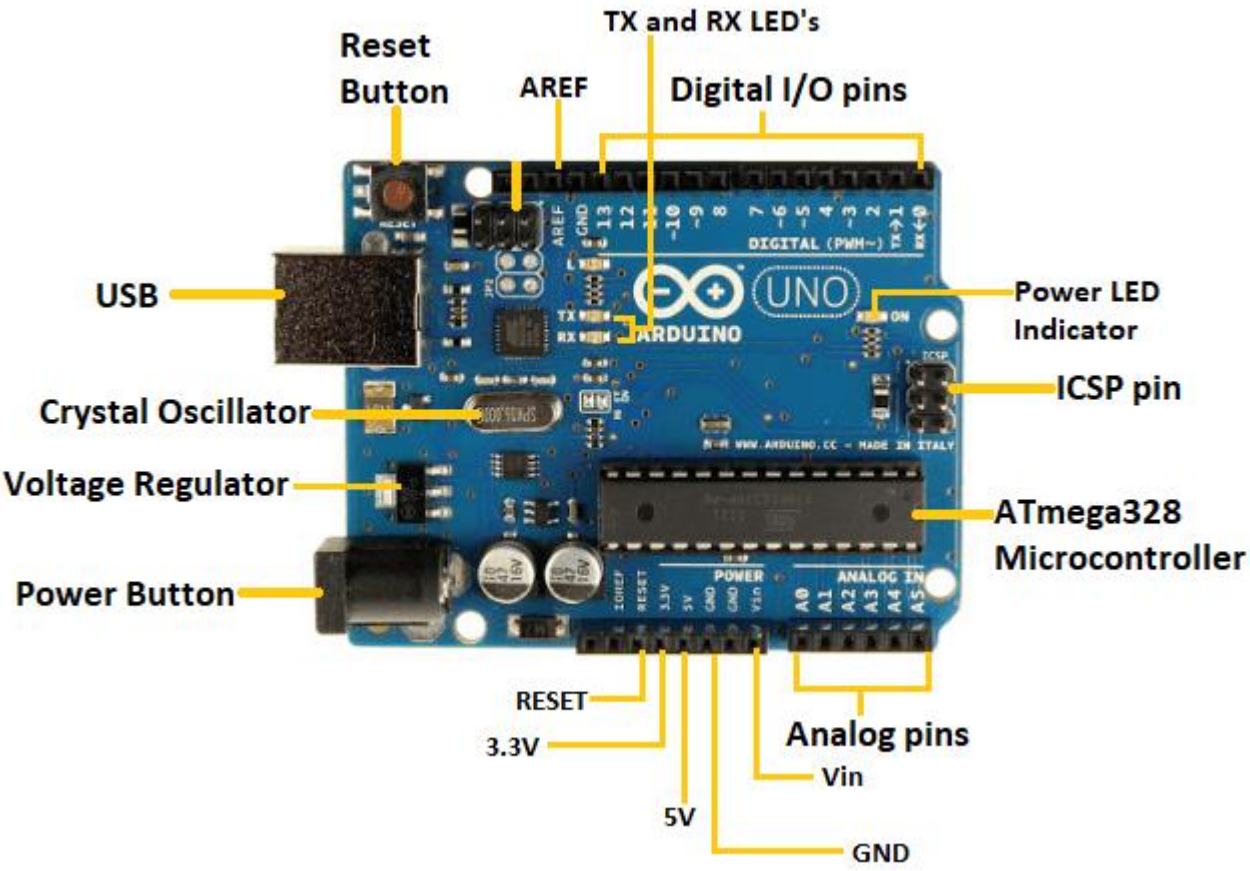


Рисунок 3.2 – Плата Arduino UNO

Ця плата складається з основних елементів зображених на рисунку 3.2, де:

1) ATmega328 Microcontroller - це однокристальний мікроконтролер сімейства ATmel. Процесорний код всередині нього 8-розрядний. Він поєднує в собі пам'ять (SRAM, EEPROM і флеш-пам'ять), аналого-цифровий перетворювач, послідовні порти SPI, лінії вводу/виводу, регістри, таймер, зовнішні і внутрішні переривання і осцилятор;
2) ICSP pin - вивід для внутрішньо-схемного послідовного програмування дозволяє користувачеві програмувати за допомогою прошивки плати Arduino;
3) Power LED Indicator - Увімкнений стан світлодіода показує, що живлення активоване. Коли живлення вимкнено, світлодіод не світиться;

4) Digital I/O pins - цифрові виводи мають значення HIGH або LOW. Виводи, пронумеровані від D0 до D13, є цифровими;
5) TX and RX LED's - успішний потік даних відображається світінням цих світлодіодів;
6) AREF - вивід аналогового опорного сигналу (AREF) використовується для подачі опорної напруги на плату Arduino UNO від зовнішнього джерела живлення;
7) Reset button - використовується для додавання кнопки скидання до з'єднання;
8) USB - дозволяє підключити плату до комп'ютера. Він необхідний для програмування плати Arduino UNO;
9) Crystal Oscillator - Кристалічний генератор має частоту 16 МГц, що робить Arduino UNO потужною платою;
10) Voltage Regulator - Стабілізатор напруги перетворює вхідну напругу в 5В;
11) GND - виводи заземлення. Вивід заземлення діє як вивід з нульовою напругою;
12) Vin - це вхідна напруга;
13) Analog Pins - виводи, пронумеровані від A0 до A5, є аналоговими виводами. Функція аналогових виводів полягає в зчитуванні аналогового датчика, що використовується в підключенні. Вони також можуть діяти як контакти GPIO (General Purpose Input Output).

USB-порт на платі Arduino використовується для підключення плати до комп'ютера за допомогою USB-кабелю. Кабель працює як послідовний порт і як джерело живлення для інтерфейсу плати. Таке подвійне функціонування робить його унікальним і простим у використанні.

Технічні характеристики Arduino UNO наведені нижче.

На платі Arduino UNO є 20 виводів вводу/виводу. Ці 20 виводів включають 6 ШІМ виводів, 6 аналогових виводів і 8 цифрових виводів вводу/виводу.

Виводи ШІМ - це виводи з підтримкою широтно-імпульсної модуляції.

Кристалічний генератор, присутній в Arduino UNO, працює на частоті 16 МГц.

Він також має інтегрований в Arduino модуль WiFi. Така плата Arduino UNO базується на інтегрованому модулі WiFi ESP8266 та мікроконтролері ATmega328P.

Вхідна напруга плати UNO варіюється від 7В до 20В.

Arduino UNO автоматично отримує живлення від зовнішнього джерела живлення. Він також може отримувати живлення від USB.

Ми можемо програмувати Arduino UNO за допомогою Arduino IDE. Arduino IDE - це інтегрована програма розробки, яка є спільною для всіх плат [11 - 15].

Можемо використовувати Arduino Web Editor, який дозволяє завантажувати ескізи і писати код з нашого веб-браузера на будь-яку плату Arduino. Це онлайн-платформа.

USB-з'єднання необхідне для з'єднання комп'ютера з платою. Після підключення штирі PWR загоряться зеленим кольором. Це зелений світлодіод живлення.

Для початку роботи з Arduino UNO встановимо драйвери плати.

Як тільки підключимо плату до комп'ютера, Windows автоматично встановить драйвери плати.

3.4 Вибір макету системи

Для реалізації системи, виберемо та розробимо корпус. Цей корпус повинен вміщувати основні елементи системи та ілюструвати увесь принцип роботи. Збірка сейку складається з двох етапів. Перший це створення 3D моделі

сейфу або завантаження безкоштовних. В даному випадку використовується 3д модель сейфу з сайту Thingeverse з додаванням задньої стінки для приховування ардуіно. Сейф складається з 3 частин. Основна частина із стінкою для ардуіно, дверцята з отвором для дротів дисплею, та замковий механізм який буде рухати сервопривід.

3.5 Конструкція та збірка системи

Основуючись на всіх вимогах, маючи всі компоненти деталей. Котрі повинні бути вмонтовані в даний корпус, збираємо всі деталі котрі без корпусу виглядатимуть так як зображено на рисунку 3.3.

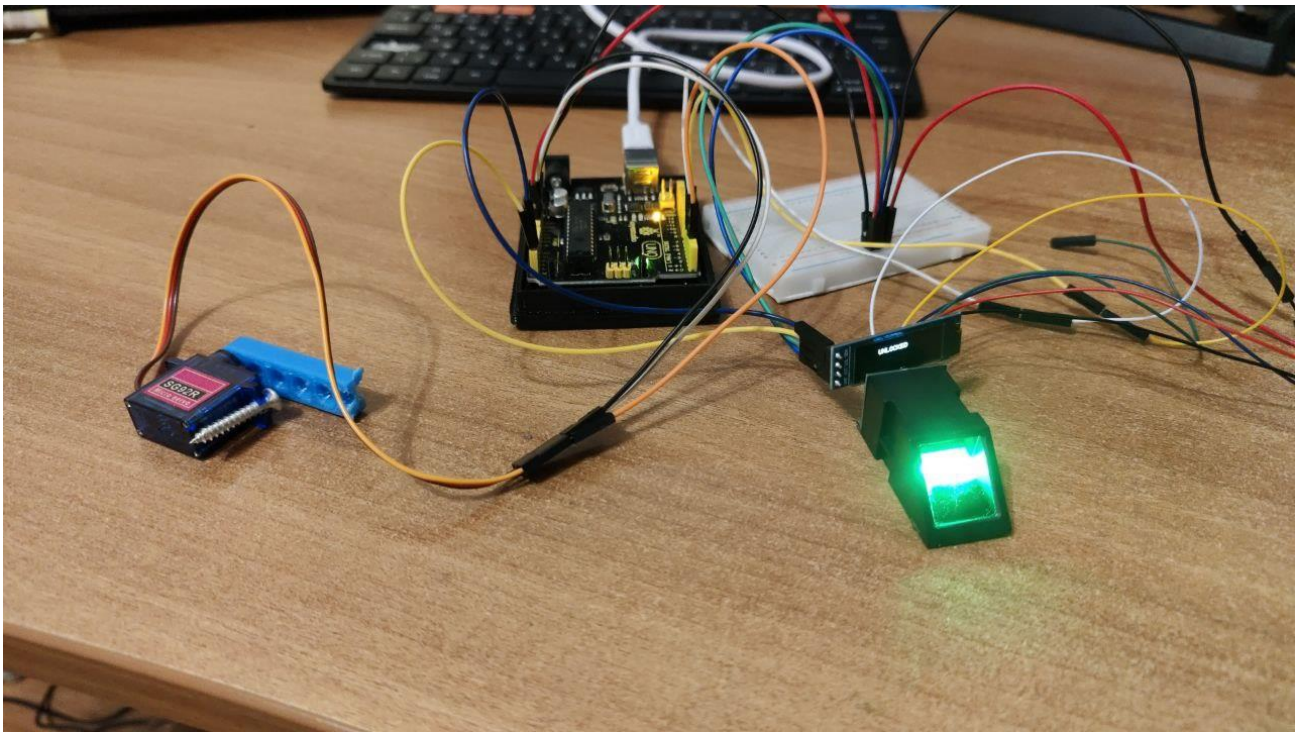


Рисунок 3.3 – Компоненти системи без корпусу

Далі приступаючи до збірки вмонтовуємо всі елементи в корпус сейфу.

Даний сейф вміщує всі елементи системи і необхідні компоненти для повноцінної роботи.

Зібрана система сейфу має компактний вигляд, та може повноцінно функціонувати та виконувати всі поставлені вимоги.

Готова система у зібраному вигляді зображена на рисунку 3.5.

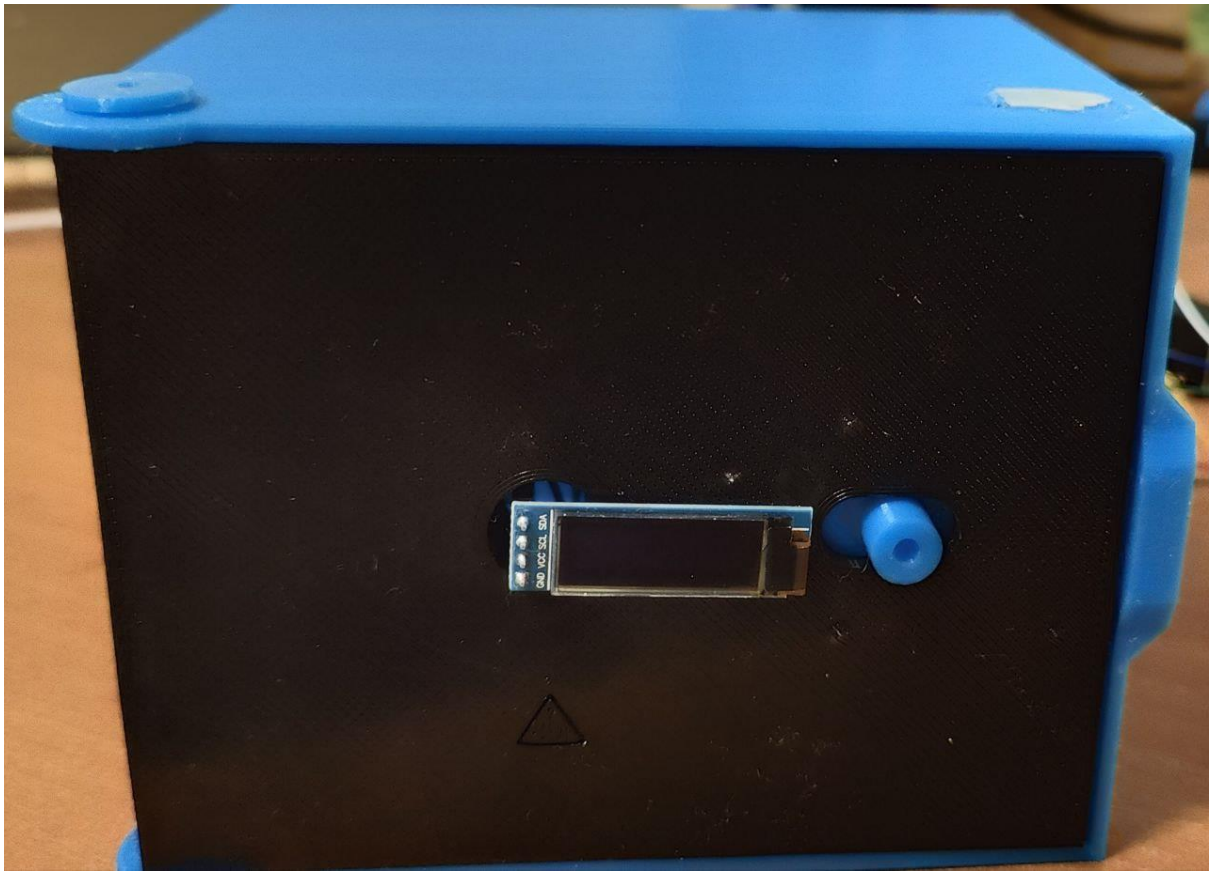


Рисунок 3.4 – Зібрана система сейфу

Другий етап це підключення всіх компонентів до ардуіно, живлення, та монтування в корпус. Схема підключення зображена на рисунку 3.1. Сканер відбитків пальців підключається до ардуіно до портів живлення 3.3V та GND, а також до цифрових портів 4,5 для передачі даних датчика відбитків пальців.

OLED дисплей підключається до портів живлення 3V та GND, а також до аналогових портів 4,5.

Сервопривід підключається до портів живлення 3V та GND, та одного порта 2 для керування мотором.

Кріпиться сервомотор та дисплей до дверей сейфу, серво рухає замковий механізм при відкриванні та закриванні, як зображено на рисунку 3.5.

Живлення виведене назовні, і може живитись від павербанку.

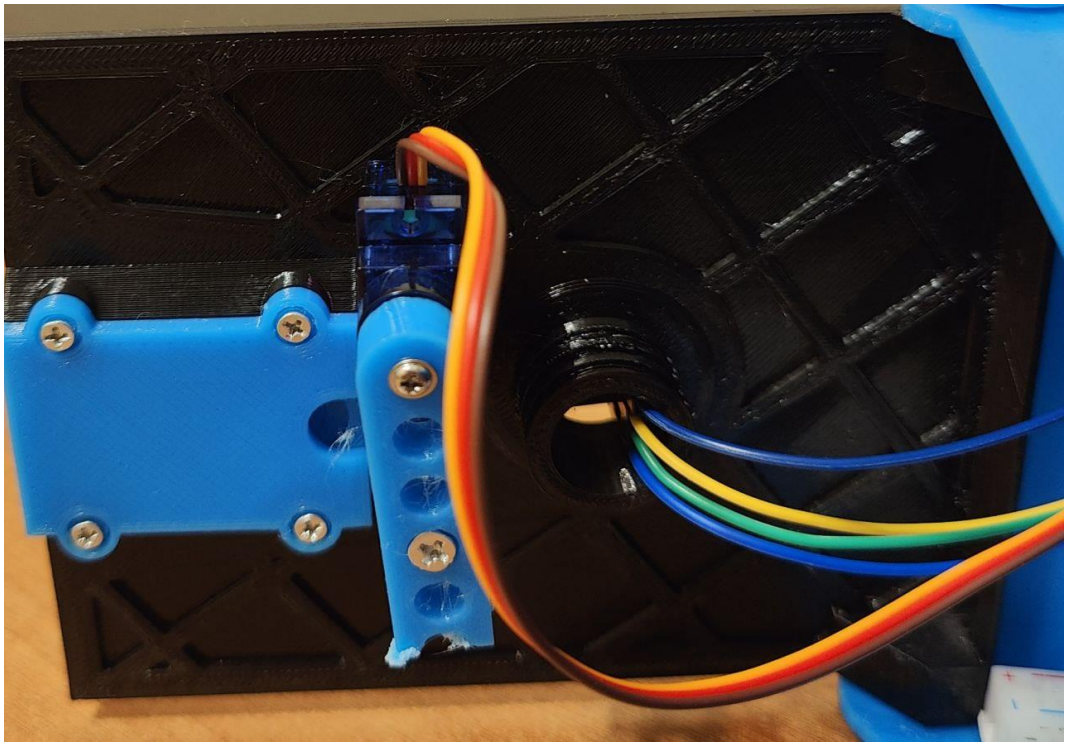


Рисунок 3.5 - Кріплення сервомотору та дисплею до дверці сейфу

Повноцінний сейф зображений на рисунку 3.6.

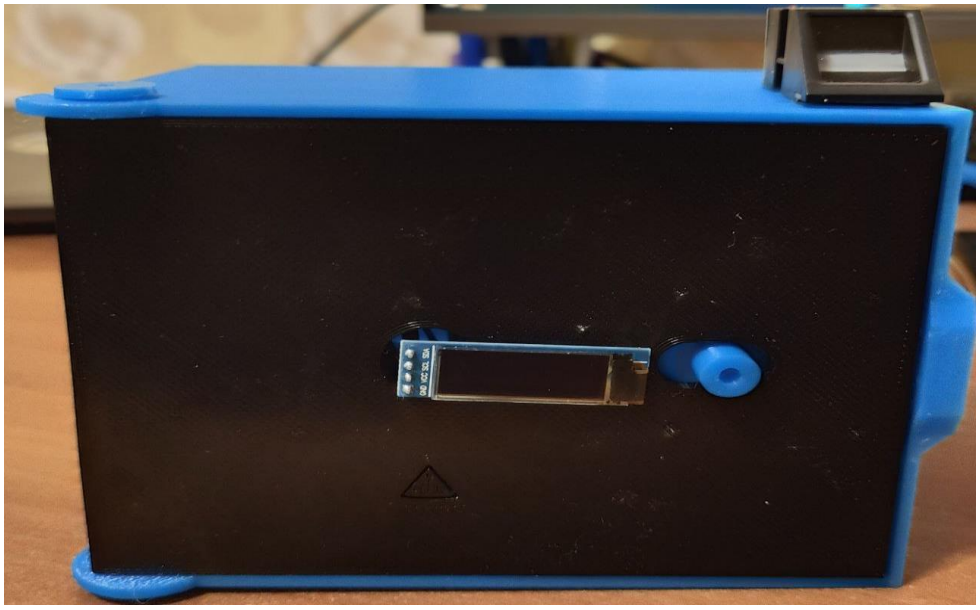


Рисунок 3.6 - Готовий сейф з підключеними датчиками

3.6 Навчання сканеру для розпізнавання

Для навчання сканеру відбитків пальців було використано метод додавання сканеру за допомогою підключення ардуіно до пк, і додавання відбитку пальців після чого ардуіно більше не підключається до пк.

Для управління сканером була використана бібліотека - Adafruit Fingerprint Sensor Library [16 - 20]. Бібліотека дозволяє зберегти 127 відбитків.

Також має функції видалення, зміни відбитків пальців.

Повний список можливостей бібліотеки зображений на рисунку 3.7.

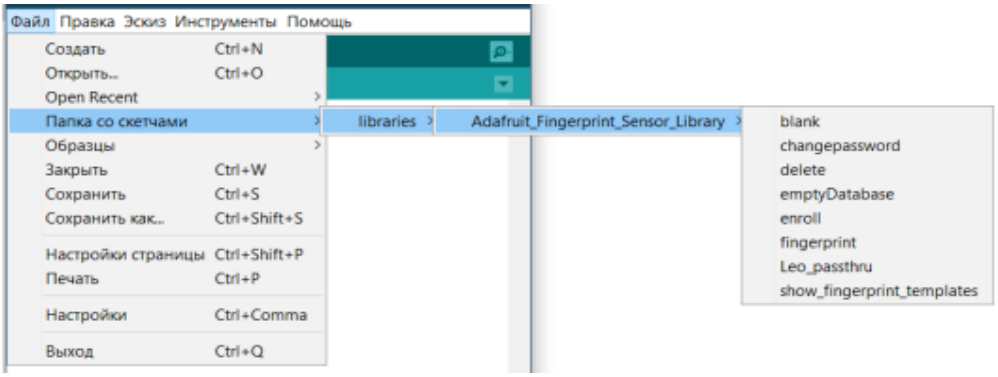


Рисунок 3.7 - Перелік можливостей бібліотеки Adafruit Fingerprint Sensor Library

Далі треба запустити функцію з додавання сканеру відбитків пальців, та ввести номер під яким ми хочемо зберегти відбиток пальця, на рисунку 3.8 показано додавання відбитку за номером 1. На рисунку 3.9 показано успішне додавання відбитку пальця.

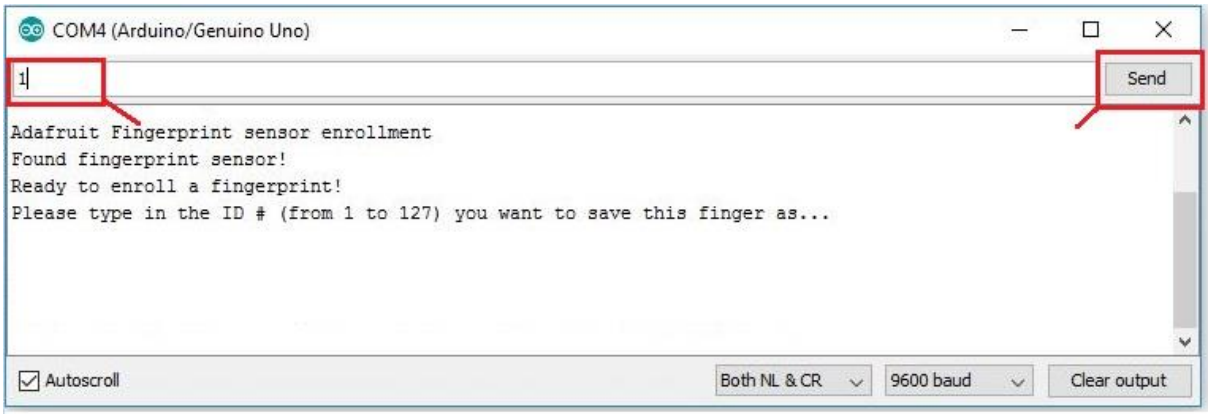


Рисунок 3.8 - Додавання відбитку пальця під номером 1

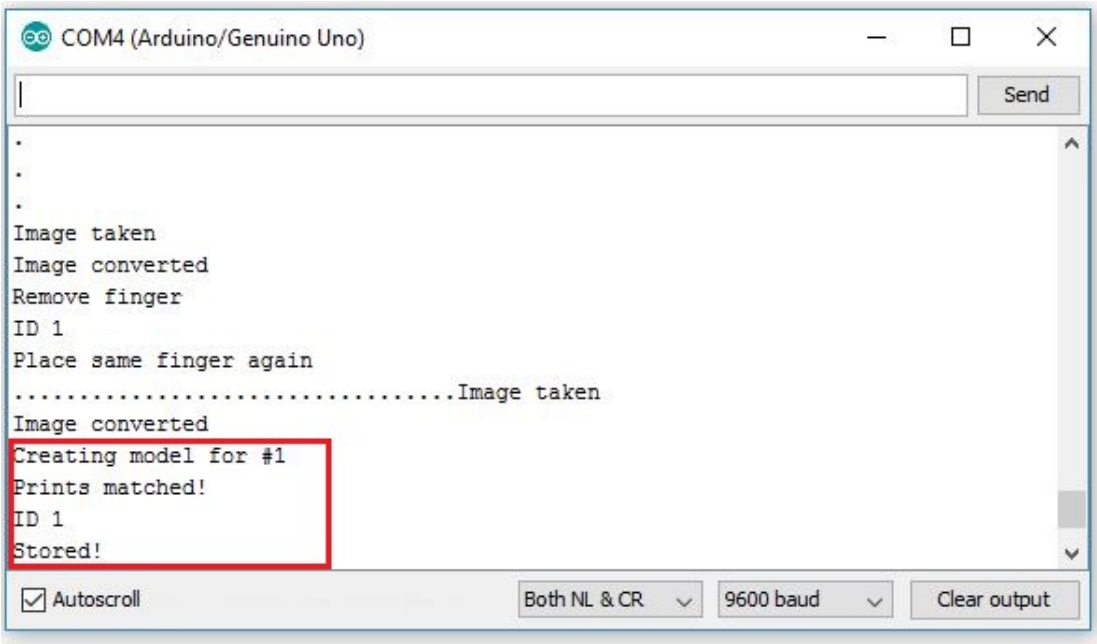


Рисунок 3.9 - Успішне додавання відбитку пальця

3.7 Алгоритм роботи та перевірка працездатності системи контролю доступу

Для використання системи контролю з першим додаванням відбитку пальця необхідно притримуватись наступного алгоритму:

1) підключити ардуіно до пк кабелем USB;
2) запустити скечт додавання відбитків пальці, та доторкнутись до сканеру для додавання відбитку пальця, тримати палець поки не буде команди завершення в консолі;
3) увімкнути кабель живлення до ардуіно;
4) почекати поки ардуіно запуститься та дисплей показує LOCK;
5) перевірити спрацювання системи можна приклавши палець до сканеру відбитків, замочний механізм відкривається та дисплей показує UNLOCK;
6) після спрацювання система заблокує автоматично сейф через 5 секунд.

Для використання системи контролю необхідно притримуватись наступного алгоритму:

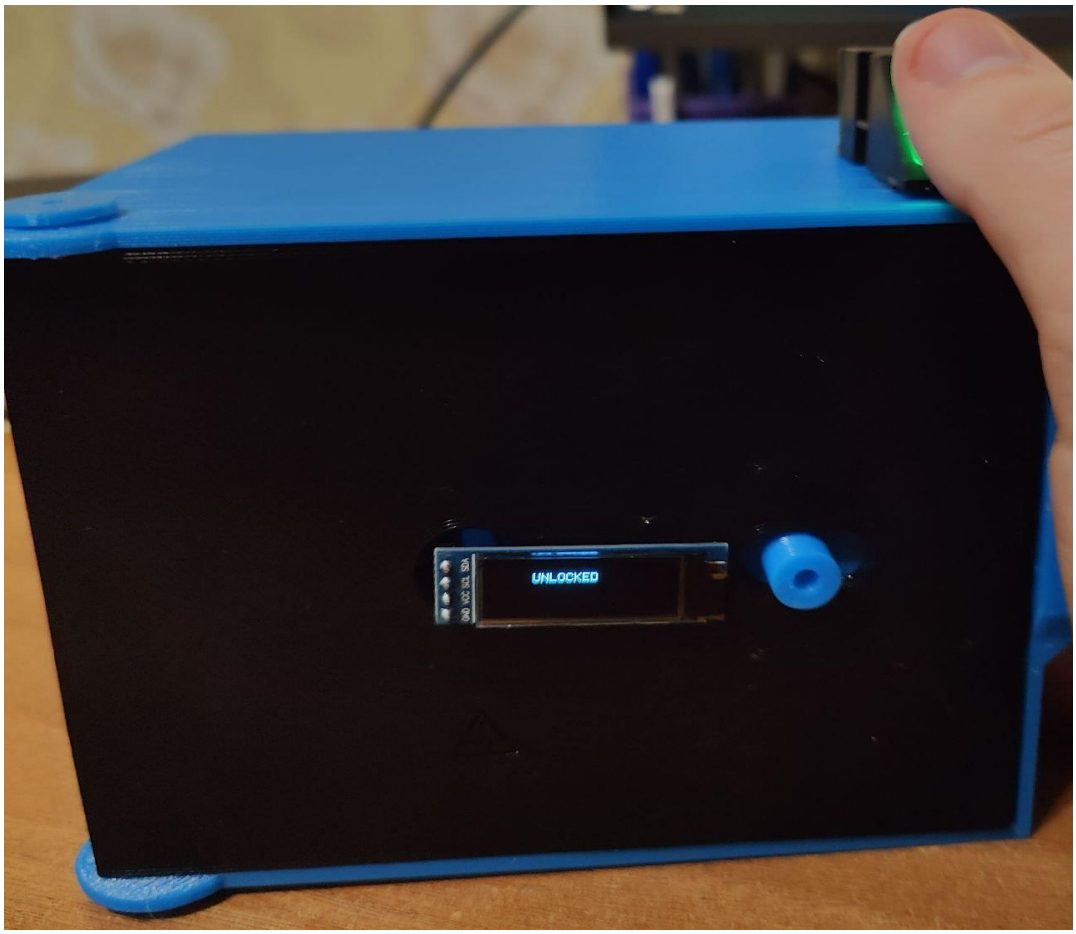
1) для роботи необхідно ввімкнути кабель живлення до ардуіно ;
2) дисплей включається і показує LOCK;
3) перевірити спрацювання системи можна приклавши палець до сканеру відбитків, замочний механізм відкривається та дисплей показує UNLOCK;
4) після спрацювання система заблокує автоматично сейф через 5 секунд.

Проведені вище дослідження демонструють, що система працює коректно та ефективно, відповідно до задачі яка вимагалась для успішної автентифікації та роботи. Результат роботи зображено на рисунках 3.10-3.11.

Базовий код програми знаходиться в додатку А.

Рисунок 3.10- Сейф заблоковано

Перевірка працездатності системи доступу до сейфу за допомогою сканеру відбитку пальців, були проведені тести за описаним вище алгоритмом. Швидкість розпізнавання датчику приблизно дорівнює 1.5 секунди. При відсутності у завантажених відбитків пальців, система ніяк не реагує на дотик до датчику, що відповідає опису характеристик системи.



3.11 - Сейф розблоковано за допомогою сканеру

3.8 Висновки до розділу

Отже, в даному розділі була повністю розроблена система автентифікації за допомогою відбитків пальців та повністю протестована. Тести показали успішно роботу системи.

Швидкість розпізнавання датчику приблизно дорівнює 1.5 секунди. При відсутності у завантажених відбитків пальців, система ніяк не реагує на дотик до датчику, що відповідає опису характеристик системи.

ВИСНОВКИ

Результатом та метою даного дипломного проекту було створення системи автентифікації користувача за допомогою сканування відбитків пальців на основі дактилоскопічного датчика з пам'яттю 127 відбитків.

Проведено огляд та аналіз існуючих технологій дактилоскопічних датчиків, сучасних моделей сканерів відбитків пальців та обрано оптичний дактилоскопічний датчик, який є оптимальним для використання, оскільки його характеристики відповідають вимогам системи, а саме: вартість, швидкість розпізнавання та надійність.

В ході роботи була створена система контролю доступу на базі оптичного сканера відбитків пальців та контролера Arduino Uno. Дверний замок відкривається за допомогою електроприводу. Доданий інформаційний екран для відображення сповіщень для покращення взаємодії з користувачем. Модель корпусу була розроблена за допомогою 3д моделі сейфу з сайту Thingeverse з додаванням задньої стінки для приховування ардуіно.

Проведено огляд методів запису та пошуку відбитків пальців, а саме використання спеціального програмного забезпечення та використання Arduino IDE. Розроблено програмне забезпечення для мікроконтролера. Прошивка виконана з використанням Arduino IDE та функціоналу бібліотеки Adafruit-Fingerprint-Sensor-Library. Прошивка реалізує роботу системи в двох режимах: «Робота» та «Навчання». Під час тестування працездатності було виявлено, що система є ефективною та працездатною і функціонує відповідно до вимог початкового завдання.

В майбутньому можна покращити систему додавши додаткові системи захисту за допомогою додаткових датчиків. Також дану систему можна

використати в реальному житті, при доступі до сейфу, алое в цьому випадку потрібно буде використати звісно інші деталі, котрі відповідатимуть вимогам.

ПЕРЕЛІК ПОСИЛАНЬ

1 Відбиток пальців // Юридична енциклопедія : [у 6 т.] / ред. кол. Ю. С. Шемшученко (відп. ред.) [та ін.] — К. : Українська енциклопедія ім. М. П. Бажана, 1998 — 2004. URL: http://cyclop.com.ua/content/view/997/58/1/13/#24694 (дата звернення 11.03.2023)

2 Папілярні лінії та візерунки // Юридична енциклопедія : [у 6 т.] / ред. кол. Ю. С. Шемшученко (відп. ред.) [та ін.] — К.: Українська енциклопедія ім. М. П. Бажана, 2002. — Т. 4 : Н — П. — 720 с. URL:http://leksika.com.ua/18540516/legal/papilyarni_liniyi_ta_vizerunki (дата звернення11.03.2023)

3 Fingerprint Verification vs. Fingerprint Identification [Електронний ресурс] / 2015 - 2019. URL: https://www.touchngoid.com/fingerprint-verification-vsfingerprint-identification/ (дата зверення 11.03.2023)

4 Fingerprint scanner – Wikipedia [Електронний ресурс] URL: https://en.wikipedia.org/wiki/Fingerprint_scanner (дата зверення 12.03.2023)

5 Сканеры отпечатков пальцев [Електронний ресурс]. URL:http://fingerprint.com.ua/article/reader.htm (дата звернення 12.03.2023)

6 Fingerprint Scanners 101: Capacitive vs. Optical vs. Ultrasonic [Електронний ресурс] URL:https://www.konsyse.com/articles/fingerprintscanners-101-capacitive-vs-optical-vs-ultrasonic/ (дата звернення 12.03.2023)

7 Датчик відбитків пальців R307 и Arduino [Електронний ресурс] URL:http://www.electronica52.in.ua/proekty-arduino/datchik-otpechatkov-palcev-iarduino- (дата звернення 14.03.2023)

8 Uno Плати Ардуіно [Електронний ресурс]
URL: https://doc.arduino.ua/ru/hardware/Uno Зм. Арк. № докум. Підпис Дата Арк 63 ДП ПГ6104.1730.00 ПЗ (дата зверення 14.03.2023)

9 Центральний замок автомобіля: принцип роботи [Електронний ресурс] URL:https://auto.today/bok/2930-ustroystvo-centralnogozamka-kak-on-otkryvaet-vse-dveri.html (дата звернення 14.03.2023)

10 SolidWorks – Вікіпедія [Електроний ресурс] URL:https://uk.wikipedia.org/wiki/SolidWorks (дата звернення 19.03.2023)

11 Мірошниченко Е. А. Технології програмування: навчальний посібник / Е. А. Мірошниченко. — 2-е изд., испр. і дод. — Томськ: Изд-во Томського політехнічного університету, 2008. — 128 с. (дата звернення 20.03.2023)

12 Мікроконтролерні пристрої : навч. посіб. для студ. спец. «Мікро- та наноелектроніка» / О. С. Тонкошкур, І. В. Гомілко, О. В. Коваленко; Дніпропетровський нац. ун-т ім. О. Гончара. – Д. : Вид-во ДНУ, 2011. – 264 с. (дата звернення 22.03.2023)

13 Програматор – Вікіпедія [Електронний ресурс] / 27.05.2020. URL:https://uk.wikipedia.org/wiki/Програматор (дата звернення 23.03.2023)

14 Arduino IDE – Вікіпедія [Електронний ресурс] URL:https://ru.wikipedia.org/wiki/Arduino_IDE (дата звернення 23.03.2023)

15 Датчик відбитків пальців і Arduino||Arduino-diy.com [Електронний ресурс] URL: http://arduino-diy.com/arduino-datchik-otpechatka-paltsa (дата звернення 23.03.2023)

ДОДАТОК А

```
#include "Wire.h"
#include<SoftwareSerial.h>
#include "Adafruit_GFX.h"
#include <Adafruit_Fingerprint.h>
#include "Adafruit_SSD1306.h"
#include <Servo.h>


int getFingerprintIDez();


Servo myservo;


Adafruit_SSD1306 display(128, 64, &Wire, 4); // указываем
размер экрана в пикселях
// pin #2 is IN from sensor (GREEN wire)


// pin #3 is OUT from arduino  (WHITE wire)


SoftwareSerial mySerial(4, 5);


Adafruit_Fingerprint finger =
Adafruit_Fingerprint(&mySerial);


void setup()


{
```

```
  Serial.begin(9600);

  // Serial.println("fingertest");

  pinMode(13, OUTPUT);

  digitalWrite(13, LOW);

  // set the data rate for the sensor serial port

  finger.begin(57600);

  display.begin(SSD1306_SWITCHCAPVCC, 0x3C); // указываем
адрес устройства на шине
  display.clearDisplay();

  if (finger.verifyPassword()) {

    Serial.println("Found fingerprint sensor!");

  } else {

    Serial.println("Did not find fingerprint sensor :(");

    while (1);

  }
```

```
  Serial.println("Waiting for valid finger…");

}

void loop()                     // run over and over
again

{

  getFingerprintIDez();

  delay(50);            //don’t ned to run this at full
speed.

}

uint8_t getFingerprintID() {

  uint8_t p = finger.getImage();

  switch (p) {

    case FINGERPRINT_OK:

      Serial.println("Image taken");

      break;

    case FINGERPRINT_NOFINGER:
```

```
      Serial.println("No finger detected");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return p;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      return p;
    default:
      Serial.println("Unknown error");
      return p;
  }

  // OK success!

  p = finger.image2Tz();
```

```
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image converted");
      break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("Image too messy");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return p;
    case FINGERPRINT_FEATUREFAIL:
      Serial.println("Could not find fingerprint
features");
      return p;
```

```
    case FINGERPRINT_INVALIDIMAGE:

      Serial.println("Could not find fingerprint
features");

      return p;

    default:

      Serial.println("Unknown error");

      return p;

  }

  // OK converted!

  p = finger.fingerFastSearch();

  if (p == FINGERPRINT_OK) {

    Serial.println("Found a print match!");

  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {

    Serial.println("Communication error");

    return p;
```

```
  } else if (p == FINGERPRINT_NOTFOUND) {

    Serial.println("Did not find a match");

    return p;

  } else {

    Serial.println("Unknown error");

    return p;

  }

  // found a match!

  Serial.print("Found ID #");
  Serial.print(finger.fingerID);

  Serial.print(" with confidence of ");
  Serial.println(finger.confidence);




}

// returns -1 if failed, otherwise returns ID #
```

```
int getFingerprintIDez() {

  uint8_t p = finger.getImage();

  if (p != FINGERPRINT_OK)  return -1;

  p = finger.image2Tz();

  if (p != FINGERPRINT_OK)  return -1;

  p = finger.fingerFastSearch();

  if (p != FINGERPRINT_OK)  return -1;

  // found a match!

   display.clearDisplay();
   display.setTextSize(1, 2); // указываем размер шрифта
   display.setTextColor(SSD1306_WHITE); // указываем цвет
надписи

   display.setCursor(30, 10);
   display.println("UNLOCKED");
   display.display();

  Serial.print("Found ID #");
Serial.print(finger.fingerID);

  Serial.print(" with confidence of ");
  Serial.println(finger.confidence);
```

```
  digitalWrite(13, HIGH);


  delay(3000);


  digitalWrite(13, LOW);


  display.clearDisplay();
   display.setTextSize(1, 2); // указываем размер шрифта
   display.setTextColor(SSD1306_WHITE); // указываем цвет
надписи


   display.setCursor(30, 10);
   display.println("UNLOCKED");
   display.display();




  return finger.fingerID;


}
```