Міністерство освіти і науки України
ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»
Кафедра комп'ютерної інженерії та електроніки
(повна назва кафедри)

Рудик Роман Данилович
Rudyk Roman

УДК 004:681.5

Спеціальність 6.050102 «комп'ютерна інженерія»
(шифр та назва спеціальності)

Кваліфікаційна робота
на здобуття освітньо-кваліфікаційного рівня бакалавр
(бакалавр, спеціаліст, магістр)

Система біометричної ідентифікації персони за відбитком пальця
The System of Biometrics Identification by Fingerprint

Науковий керівник:
кандидат технічних наук,
доцент Грига В.М.

Рецензент:
Кандидат фіз.-мат. наук,
професор кафедри фізики і
хімії твердого тіла
Никируй Л.І.

Івано-Франківськ
2020

Форм.	Зона	Поз.	Позначення	Найменування	К-ть	Прим.
			6.050102. УДК 004:681.5	Пояснювальна записка	66	

					6.050102. УДК 004:681.5			
Змн.	*Арк.*	*№ докум.*	*Підп.*	*Дата*				
Разробив		Рудик Р.Д.			Специфікація	*Літ.*	*Арк.*	*Аркушів*
Перевірив		Грига В.М.					2	66
Н. Конт.		Грига В.М.						
Затвердив		Когут І.Т.						

АНОТАЦІЯ

В бакалаврській кваліфікаційній роботі розроблено спеціалізовану мікропроцесорну систему біометричної ідентифікації персони за відбитком пальця на базі сканера відбитків пальця FPM10A та мікропроцесорної плати Arduino Uno.

У пояснювальній записці проведено аналіз різних методів біометричної ідентифікації, розглянуто характеристики відомих пристроїв ідентифікації за відбитком пальця та визначено їхні недоліки, обґрунтовано вибір засобів розробки, спроектовано пристрій ідентифікації особи за відбитком пальця, розроблено програмне забезпечення та описано алгоритм роботи пристрою та розраховано економічну ціну його реалізації.

Загальний обсяг роботи – 66 сторінок, 32 рисунки, 2 таблиці, 12 посилань.

Ключові слова: біометрична ідентифікація, Arduino Uno, сканер відбитків пальця, рідкокристалічний дисплей, скетч, блок-схема алгоритму.

ABSTRACT

In the bachelor's qualification, a specialized microprocessor biometric identification system for fingerprint based on FPM10A fingerprint scanner and Arduino Uno microprocessor board was developed.

The explanatory note analyzes various biometric identification methods, describes the characteristics of known fingerprint identification devices and defects them, justifies the choice of development tools, designed the device for identification of the person by the fingerprint, developed the software, and described the algorithm for operating the device economy .

Total volume of work - 66 pages, 32 drawings, 2 tables, 12 links.

Keywords: biometric identification, Arduino Uno, fingerprint scanner, LCD, sketch, algorithm flowchart.

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Прикарпатський національний університет імені Василя Стефаника»
Фізико-технічний факультет
Кафедра «Комп'ютерної інженерії та електроніки»

Пояснювальна записка

до кваліфікаційної роботи на тему:

Система біометричної ідентифікації персони за відбитком пальця

					6.050102.КІ-41.22		
Змін.	Арк.	№ докум.	Підпис	Дата			
Розробив		Рудик Р.Д.			Пояснювальна записка	Арк.	Аркуш 5 / Аркушів 66
Перевірив		Грига В. М.					
Н. Контр.							
Затверд.							

ЗМІСТ

ВСТУП

На сьогоднішній день з необхідністю ідентифікації особи, людина стикається все частіше і частіше. Посвідчення, паспорти, підписи, паролі, pin-коди, необхідні для авторизації чи то при вході в будівлю, чи при перетині міжнародного кордону, отриманні грошей в банку чи в банкоматі. Коли виникає потреба особистої ідентифікації, біометрія – є зручним та надійним інструментом.

Сучасні методи ідентифікації особи не спроможні забезпечити необхідний рівень надійності. Одним і з можливих рішень цієї проблеми є застосування біометричних технологій для ідентифікації особи. Біометричні технології, на відміну від парольної ідентифікації, є більш надійними та дозволяють значно підвищити певність процесу ідентифікації особи, для них вже створена розвинена база технічних рішень.

На сьогодні біометрія й основані на її принципах системи стали ефективним засобом забезпечення безпеки всіх видів власності, захисту від шахрайства, фальсифікації та криміналу. Їх подальше впровадження в різні галузі є актуальним завданням, адже забезпечить створення надійних засобів контролю різних промислових і комерційних об’єктів та окремих громадян.

Метою бакалаврської кваліфікаційної роботи є проектування спеціалізованого пристрою ідентифікації персони за біометричними даними, а саме відбитками папілярних візерунків на пальцях руки з наступними технічними характеристиками:

- споживана потужність 5Вт;
- висока швидкість обробки інформації;
- наявність додаткової периферії для зручності користування;
- можливість під’єднання до загального сервера;
- низька вартість пристрою.

1. ОГЛЯД ТА АНАЛІЗ ОСНОВНИХ МЕТОДІВ ІДЕНТИФІКАЦІЇ ПЕРСОНИ

1.1.Огляд основних методів ідентифікації

Для захистити інформації користувачів, яка зберігається на ресурсах інформаційних систем від несанкціонованого доступу, актуальною задачею є створення надійних систем, які будуть контролювати доступ до інформаційних ресурсів. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та автентифікації. Дані процедури виконуються кожного разу, коли користувачі вводять пароль для доступу до інформаційної системи, мережі, бази даних чи при запуску певних прикладних програм. В результаті їх виконання користувачу надається доступ до певних інформаційних ресурсів системи, або, у разі невірності введених даних, відмова в доступі.

Ідентифікація – процес розпізнавання користувача в інформаційній системі за допомогою наперед визначеного імені (ідентифікатора) або іншої наданої інформації про нього, яка сприймається системою. Вона є початковою процедурою надання доступу до системи, після якої здійснюється автентифікація та авторизація.

Автентифікація – це процес перевірки належності ідентифікатора об'єкту, тобто встановлення або підтвердження дійсності, і перевірка того чи є об'єкт або суб'єкт, що перевіряється, справді тим, за кого він себе видає.

Існує декілька методів ідентифікації, які відрізняються своєю складністю, надійністю, вартістю та іншими важливими показниками. Кожний з цих методів має свої переваги та недоліки, тому в даному розділі проведено класифікацію та детальний аналіз даних методів.

В загальному випадку можна виділити три методи ідентифікації:

- парольна ідентифікація;
- апаратна ідентифікація;
- біометрична ідентифікація.

На рисунку 1.1. подана класифікація методів ідентифікації, які поділяють на методи парольної ідентифікації, апаратної та біометричної ідентифікації [1].

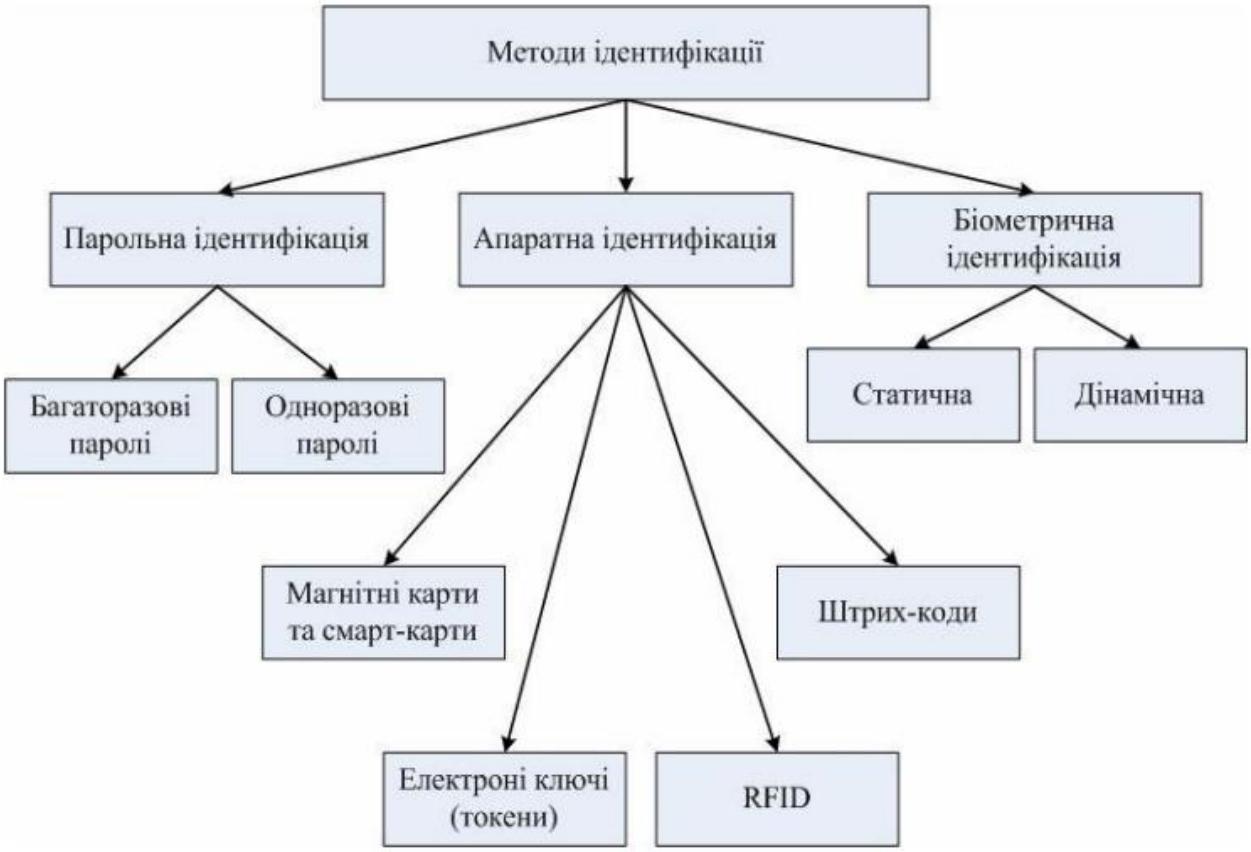


Рис. 1.1. Класифікація методів ідентифікації.

Найдавніші методи ідентифікації мали механічний характер та будувалися в основному на використанні певних технічних правил. Такий же принцип застосували в основу до новіших технологій та методів апаратної ідентифікації з використанням пластикових бейджиків, магнітних смарт-карток з електронним та оптичними пристроями запам'ятовування. Смарт-карта може використовуватися для безпечного зберігання закритих ключів користувача, а також для безпечного виконання різноманітних криптографічних перетворень. Інтелектуальні пристрої ідентифікації, як правило, не забезпечують абсолютний захист, але застосовані технології їх захисту перевершують можливості захисту звичайних персональних комп'ютерів. Для зберігання і використання закритих ключів різні фірми-розробники використовують різні методи. Найпростіший з них — використання інтелектуального пристрою, як дискети: при необхідності

карта експортує закритий ключ, і криптографічні операції здійснюються на системній робочій станції. Цей метод є досить надійним з точки зору безпеки, але відносно легко реалізовується і висуває невисокі вимоги до інтелектуального пристрою.

В таких системах передбачено досить високий рівень захисту від можливості підробити пароль, копіювання чи фальсифікації важливої інформації. Технічним системам властива також одна дуже суттєва вада – орієнтування на верифікацію визначеного предмета, який буде наданий при ідентифікації а не тільки на персону-власника. Система контролю доступу в такому разі відстежує проходження карток без підтвердження ідентичності користувача, що скористався ними. Тобто, картка може бути втрачена чи загублена, викрадена, передана і використана іншою особою чи зловмисником.

Такі спеціалізовані системи захисту, які базуються на ідентифікаторах захисту, намагаються виключити описані вище недоліки. Разом з картками вони дозволяють значно підвищити рівень безпеки для надання користувачу дозволу на з'єднання з комп'ютерною системою та визначення його прав доступу до інформаційних ресурсів. Проте іноді паролі забуваються користувачами та за допомогою засобів зв'язку можуть бути викрадені через нагляд за допомогою прихованих відеокамер, «клавіатурних шпигунів», тощо. Але з’являються все новіші та удосконалені технологічні рішення, які розвиваються за тими ж законами, що і людське суспільство. Важливою складовою методів ідентифікації особи є автоматичне визначення характеристик, які властиві тільки кожній окремі людині і називаються біометричними.

1.2. Класифікація методів біометричної ідентифікації

До переваг біометричної ідентифікації відносять те, що біометричні ідентифікатори на відміну від інших розроблених методів не можливо втратити чи забути; біометричні ідентифікатори складно підробити, тому даний метод є найбільш надійним; унікальні біометричні ознака кожної людини, тому точність біометричної ідентифікації дуже висока. До недоліків біометричної ідентифікації можна віднести те, що реалізація системи біометричної

ідентифікації потребує відносно великих фінансових витрат, та можливості підробки деяких біометричних ідентифікаторів, наприклад (відбитків пальців, підпису або голосу).

На рис. 1.2 подана класифікація статичних та динамічних методів біометричної ідентифікації [1,2].

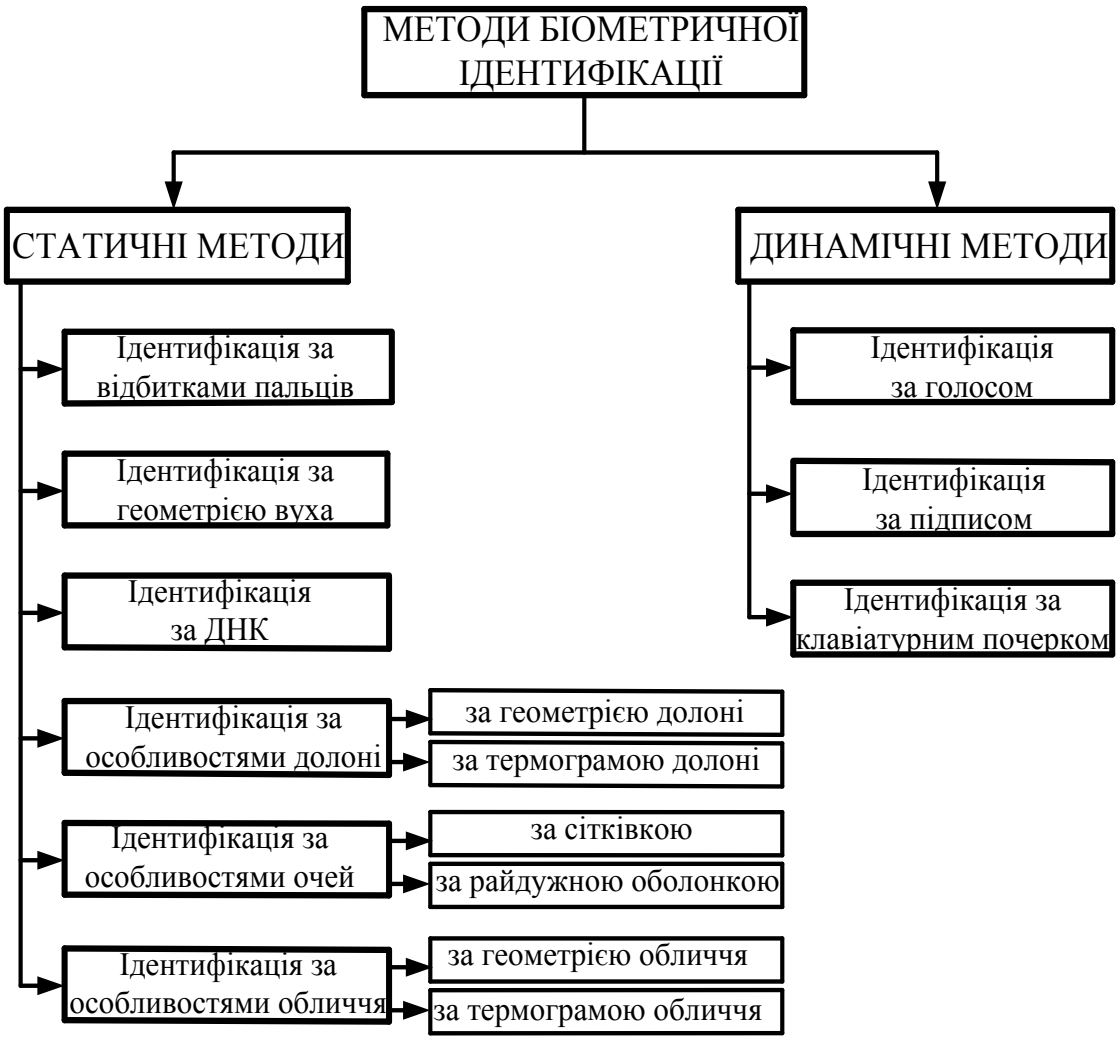


Рис. 1.2. Класифікація методів біометричної ідентифікації.

Проте, незважаючи на вказані вище недоліки, біометрична ідентифікація є досить надійною, крім того, її можливо використовувати у комплексній ідентифікації (двофакторіальній ідентифікації), одночасно з іншим методом ідентифікації (найбільш частіше використовується додатково парольна ідентифікація) або можливість проведення ідентифікації з використанням декількох біометричних ідентифікаторів одночасно, що значно підвищує надійність ідентифікації. Крім того, прийнято поділяти біометричні ознаки на

статичні або їх ще називають фізіологічними та динамічні, які іноді називають психологічними.

1.2.1. Ідентифікація за аналізом ДНК людини

До високоефективних методів ідентифікації, з точки зору вірогідності, можна віднести ідентифікацію за аналізом дезоксирибонуклеїнової кислоти (ДНК) людини, що є статичним методом ідентифікації [1-3]. ДНК – це молекула, яка одночасно розділяє і об'єднує нас. За допомогою ДНК спадкові ознаки однієї людини передаються наступним поколінням, схожість ДНК характерна для родинних сімей та кланів. При цьому, саме процеси відмінності у ДНК дають можливість бути кожній людині унікальною. Подібність ДНК пов'язує людину з її батьками, але її унікальність робить людину відмінною від них.

Ідентифікація за зразком ДНК базується на аналізі ланцюжків генів і є майже ідеальною. Для ДНК-ідентифікації використовують біологічні матеріали організмів. Важливо тільки, щоб ДНК не була пошкоджена чи зруйнована. На практиці часто при проведенні генетичного аналізу з метою ідентифікації особи або ступеня її генетичного споріднення (близькості чи віддаленості) порівнюють певні профілі ДНК з декількох біологічних зразків і оцінюють отриманий результат використовуючи імовірнісний і статистичний аналіз. Досі не існувало таких технологічних рішень, які б уможливили її ширше використання. Апаратура для ДНК-тесту надто дороговартісна, яку мають спеціалізовані хімічні лабораторії в результаті чого і зробити певний тест схожості є дороговартісним.

Отже, на сьогоднішній день ідентифікація за зразком ДНК є дуже точним методом визначення особи, але висока ціна апаратури та необхідний час, що потрібний для проведення аналізу, обробки отриманих результатів та підготовки висновку робить даний метод автентифікації непридатним для створення мікропроцесорних систем, які б широко застосовувались у повсякденному житті людини.

1.2.2. Ідентифікація за допомогою особистого підпису

Для реалізації даного методу використовується особистий підпис людини [4] (іноді це може бути написання кодового слова). Цифровий код формується за динамічними характеристиками написання, тобто будується відповідна згортка, яка включає в себе всю характеристичну інформацію. Це динамічний метод ідентифікації.

Ідентифікація документів і особистостей по рукописному підпису знайшла широке застосовання в діловій практиці і актуальним постало питання автоматизації даного процесу. Автоматичні пристрої аутентифікації особистостей по динаміці особистого підпису з'явилися давніше. В даний час такі пристрої випускаються багатьма зарубіжними фірмами.

Дані пристрої використовують для автентифікації геометричних або динамічних ознак рукописного відтворення особистого підпису в режимі реального часу. Користувачеві пропонується застосовувати для підпису спеціальне перо, яке пов'язане з пристроєм, або звичайне перо, подібне перу олівця або кулькової ручки.

Дані методи мають меншу точність, і використовуються в дещо обмежених масштабах (при ідентифікації підписів використовується характеристики максимальної правдоподібності). Користувач з використанням спеціальної ручки записує своє прізвище на спеціальній пластині, відбувається перетворювання інформації в цифрову форму, та вимір таких характеристик написання, як інтенсивність кожного зусилля і швидкість його завершення. Використовуються також низькі звуки, що виникають в процесі написання слів. Відомими є певні біометричні пристрої, в яких використовується не тільки кінцевий образ підпису, а й сам характер динаміки виконання цього підпису. В таких випадках ймовірність визначення достовірним шаблону з невідповідністю до аналога становить десяту частину і сам процес ідентифікації займає великий проміжок часу, що зменшує достовірність використання такого методу. Ціни на такі пристрої коливаються в діапазоні від 600 до 1200 доларів США.

Більш актуальним на сьогоднішній день є електронно-цифровий підпис (ЕЦП), який використовується для забезпечення автентичності особи (доказ її авторського права) і цілісності документа в системах інтернет-банкінгу. Саме електронний документ з ЕЦП є доказовою базою при вирішенні конфліктних ситуацій. Багато банківських установ рекомендують застосовувати механізм групового підпису. У таких випадках опрацьовуються лише такі платіжні документи, які містять повну групу підписів та співпадають з вказаними підписами у картці зі шаблонами підписів. Така процедура зводить до мінімуму ризики шахрайських дій з рахунками клієнтів третіми особами у разі втрати або компрометації одного з ключів ЕЦП.

Даний метод широко застосовується у науковій сфері та в галузях промисловості. Даний метод стрімко розвивається, але на даний момент його широке застосування для створення систем захисту особистих чи секретних даних не передбачається.

1.2.3. Ідентифікація за голосом людини

Одним із найпоширеніших засобів спілкування людей між собою є усне мовлення, розмовляючи по телефону, користувачі часто не усвідомлюють, що даний пристрій може бути використано для ідентифікації їх голосу [1,4,5]. Широке поширення мереж телефонного зв'язку викликало стимул до розробки пристроїв розпізнавання по голосу людини.

Це динамічний метод ідентифікації. Принцип роботи таких пристроїв аналізує динаміку спектра мови людини, а в деяких випадках і окремі слова. Науковою основою ідентифікації людини за її голосом є криміналістична фоноскопія, яка вивчає звукову та мовну інформацію, в основному у вигляді аудіо записів зроблених за допомогою диктофонів або відео та аудіо апаратури. Принцип роботи базується на наступному: ділянка стиску голосового сигналу відповідає деякому фрагменту мовлення. Це може бути комбінація однієї літери, декількох літер чи коротких речень. Після процесу фрагментації відбувається оцифрування виділених частин сигналів до їх частотних характеристик, як це показано на рис. 1.3.

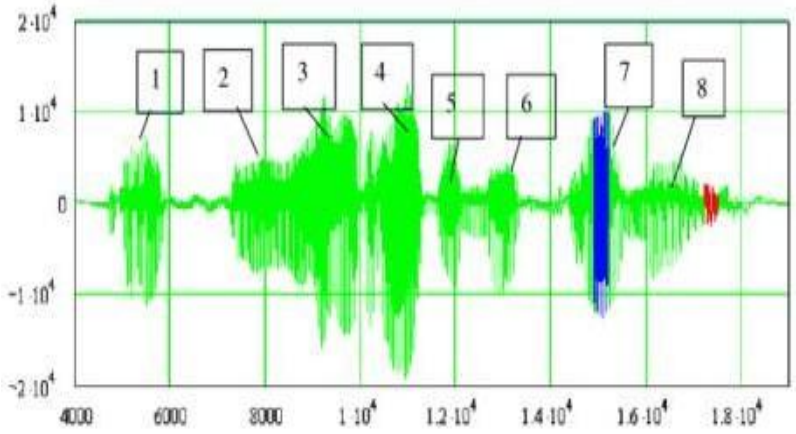


Рис. 1.3. Процес розпізнавання особи за голосом.

Існує багато способів побудови коду ідентифікації людини за голосом, що включає в себе поєднання різних характеристик голосу.

В основу методики фоноскопічних досліджень покладені акустичний і лінгвістичний аналізи усного мовлення. Лінгвістичний аналіз по своїй суті спрямований на дослідження усного мовлення, що відбиває соціальні, інтелектуальні, психофізіологічні та інші особистісні характеристики людини; акустичний має спрямування на вивчення характеристик, які визначаються анатомічними, фізіологічними та психофізіологічними особливостями кожної людини.

В основу акустичного аналізу закладені багатомірні обчислення спектрально-часових і частотних характеристик вхідного мовного сигналу та їх наступній статистичній обробці для виявлення індивідуального комплексу ознак. Розвиток комп'ютерної технології фоноскопічних досліджень не тільки забезпечив реалізацію всіх можливостей аналогових електроакустичних приладів, але й виконав процес вимірювання необхідних характеристичних параметрів.

Комплексний лінгво-акустичний аналіз мови дозволяє виконувати ідентифікацію людини навіть по фонограмах низької якості і малої тривалості. Фоноскопічні дослідження проводяться за допомогою вимірювально-обчислювальних комплексів, що включають високоякісну звукозаписну і відтворюючу апаратуру, з'єднану з комп'ютером, оснащеним спеціальним

пристроєм введення-виведення акустичної інформації і пакетом прикладних програм для обробки мовних сигналів для подальшого їх дослідження.

Записані фрагменти зразків голосу людини чутливі до вибраних способів їх розпізнавання та вимагають від 2 до 20 Кбайт.

Описані системи характеризуються великими допусками і відносно низьким рівнем безпеки, що становить високу оцінку ймовірності не розпізнати ідентичність особи, яку перевіряють (враховуючи те, що голос людини може частково змінюватись під впливом різних зовнішніх чи внутрішніх факторів). Позитивним аспектом голосової ідентифікації є відносна простота реалізації пристрою та його відносна дешевизна, але наявність суттєвих недолік не дає можливості глобальному поширенню та використанню таких систем для захисту інформації.

1.2.4. Ідентифікація за допомогою аналізу роботи за клавіатурою

Характер роботи за клавіатурою є динамічним методом ідентифікації. Проблемними ознаками з використанням даного способу є насамперед відсутність характерних особливостей у людей, які мало користуються або й зовсім не користуються клавіатурою [1,5].

Проведені дослідження показують, що клавіатурний почерк користувача має деяку стабільність, що дозволяє досить однозначно ідентифікувати користувача. Застосовуються статистичні методи обробки вихідних даних і формування вихідного вектора інформації, що є ідентифікатором даного користувача.

У якості вихідних даних використовують вибрані інтервали між процесом натисканням кнопок на клавіатурі й обчислений час їхнього утримання. Тимчасові інтервали між двома послідовними натисканнями по кнопаках в процесі надрукованих знаків істотно відрізняються у різних операторів (користувачів). Ці інтервали характеризують темп роботи та час утримання клавіш.

Ідентифікація користувача по «клавіатурному почерку» можлива такими способами:

- по набору ключових фраз;
- по набору заданого довільного тексту.

Принципова новизна цих двох способів у тому, що у першому випадку використовується ключова фраза, що задається користувачем в останній момент входження у систему (пароль), тоді як у при другому спосібі використовуються ключові фрази, які генеруються системою щоразу в останній момент ідентифікації користувача. Запропоновані користувачеві фрази необхідно підбирати в такий спосіб, щоб використовувані у них символи цілком і рівномірно покривали робоче поле клавіатури.

У поставлених задачах ідентифікації користувача по «клавіатурному почерку» основним елементом є оброблення початкових даних. У результаті даної обробки досліджуваний потік даних ділиться на ряд важливих ознак, які характеризують ті чи інші риси характеру особи, яку потрібно ідентифікувати. На наступному етапі ці ознаки, піддаються статистичній обробці, дозволяючи отримати ряд еталонних характеристик користувача.

На початковому етапі обробки даних виконується процес фільтрації. На даному етапі відбувається аналіз вхідного потоку даних. З цього потоку видаляють інформацію про «службові» клавіші – клавіші управління курсором, функціональні клавіші тощо та залишають інформацію про натискання клавіш літер, цифр, математичних та розділових знаків.

Потім виділяється інформація, яка може характеризувати безпосередньо особу, яку потрібно ідентифікувати:

- кількість помилок при наборі тексту;
- інтервали між натисканнями кнопок;
- час утримання кнопок;
- число перекриттів між кнопками;
- ступінь аритмічності при наборі тексту;
- швидкість набору тексту.

Збільшуючи число шаблонних характеристик, можна збільшити надійність системи виконавши поділ вхідного потоку на дані, які стосуються

обох (лівої і правої) рук відповідно. У випадку виявлення певних змін у клавіатурному почерку користувача йому автоматично забороняється робота на ПК.

Проте є низка обмежень щодо практичного застосування даного способу. Застосування способу ідентифікації по «клавіатурному почерку» доцільно лише для користувачів з досить тривалим досвідом роботи за персональни комп'ютером і сформованим почерком роботи з клавіатурою (що властиво програмістам, секретарям, тощо). Інакше, ймовірність неправильного розпізнавання «істинного» користувача істотно зростає і робить непридатним цей спосіб ідентифікації на практиці. Застосовуючи відомої теорії діловодства можна визначити час відповідного “клавіатурного почерку”, у якому досягається велика ймовірність ідентифікації користувача.

Навіть при простій реалізації даного методу та надійності алгоритму розпізнавання окремого користувача за допомогою аналізу його роботи за клавіатурою, є певні суттєві недоліки: обмежена сфера застосування, тривалий час для ідентифікації особи, орієнтація на відносно невелику кількість можливих користувачів та незначна кількість практичних реалізацій, що зумовлено новизною даного методу.

1.2.5. Ідентифікація особи за ознаками її зовнішності

Ідентифікація особи за ознаками її зовнішності – це статичний метод ідентифікації [1-4]. Систему розпізнавання обличчя людини вважають більш надійнішою ніж паролі. Але іноді буває, що часто машин не може відрізнити фотографію або маску від справжнього обличчя. Цей недолік системи стає у нагоді зловмисникам. Комп’ютери не "бачать" фотографії та відео, як цією властивістю володіє людина. Людина має можливість дивитися на фотографії, та описувати саме зображення фотографії, що там відбувається. З точки зору обчислювального пристрою таке зображення – це набір даних, які сприймаються як форми й інформація про значення кольорів. Хоча під час перегляду фотографій комп’ютер не реагує, як людина, його можна «навчити» розпізнавати певні шаблони кольорів і форм. Наприклад, комп’ютер можна

алгоритмічно навчити розпізнавати поширені шаблони форм і кольорів, які формують цифрове зображення обличчя. Цей процес відомий як виявлення розпізнаваних обличчів людей. Дана технологія допомагає захищати конфіденційність даних користувачів Інтернету.

У даному методі ідентифікації будується двох або трьохмірний образ обличчя людини. За допомогою вибраної спеціалазованої камери і відповідного програмного забезпечення на картинці виділяються контури очей, брів, носа, губ та інших важливих едлементів та вираховується відстань між ними. За цими даними будується образ, що перетворюється в цифрову форму для порівняння з аналогом.

На даний час технологія розпізнавання шаблонів, яка лежить в основі виявлення облич, допомагає комп'ютерним системам визначати характеристики виявленого обличчя. Загалом дана технологія розпізнавання облич допомагає комп'ютеру порівнювати відомі обличчя з новими та виявляти ймовірні збіги чи схожість.

Отже, такі системи хоча і є надійнішими за такі способи захисту (паролі, коди доступу) та поки не є можливим її застосування для їх широкомасштабного використання. Попри складні та надійні алгоритми ідентифікації користувачів та потребу в незначній кількості обладнання, все ж у таких системах повинні бути передбачені інтегровані відеокамери та потужні мікропроцесори для обробки отриманої інформації. Цей метод вже знайшов своє використання у певних сферах та у комп'ютерній техніці проте потребує певного вдосконалення.

1.3. Методи біометричної ідентифікації

У найпоширеніших відомих пристроях біометричної ідентифікації успішно використовуються [1,3,5]:

- візерунки сітківки очей;
- геометрія руки;
- відбитки пальців.

Всі ці методи ідентифікації є статичними.

В електронних системах ідентифікації по візерунках сітківки очей використовується оптична система для сканування сітківки очей (одного або двох) і обчислюється кутовий розподіл кровоносних судин по поверхні сітківки ока відповідно до сліпої плями. Даний метод полягає в унікальності малюнка райдужної оболонки ока. Для реалізації цього методу необхідні спеціалізована камера і відповідне програмне забезпечення, що дозволяє виділити з отриманого зображення рисунок райдужної оболонки ока, за яким буде побудований цифровий код. Отриманий образ може бути перенесений на персональну картку користувача або записаний у спеціалізовану базу даних. Зазвичай такі пристрої застосовуються при забезпеченні високого рівня безпеки. Ідентифікація по візерунках сітківки очей ефективна при виявленні спроб зловмисників видати себе за законних власників чи користувачів. Рівень невизнання законних користувачів знаходиться в межах декількох відсотків при практично повній відсутності помилкової ідентифікації.

Система ідентифікації по силуету руки, запропонована фірмою Idenmat (США), була першою комерційною системою цього типу. Такі системи почали випускати і інші американські фірми (Biometrics і PIDEAC). Систему HandKey, що використовує як силует, так і вертикальний профіль руки, пропонує фірма Recognition Systems. За допомогою інфрачервоної камери зчитується малюнок вен на тильній стороні долоні або кисті руки, отримана картинка обробляється, і за схемою розташування вен формується цифрова згортка. Для запису «образу» користувача в цих системах потрібно від 9 до 1000 байт. Проведені в США випробування (Sandia National Laborates) показали, що система HandKey є найбільш точною з усіх біометричних пристроїв ідентифікації. Крім того, проведене по закінченню випробувань опитування користувачів показало, що переважна більшість хоче користуватись системами саме цього типу в порівнянні з пристроями ідентифікації по візерунках сітківки ока, що є менш зручними.

У системах такого типу, в результаті сканування отримують кілька силуетів руки за допомогою підсвічуваних діодів, а після цього будується 3D зображення.

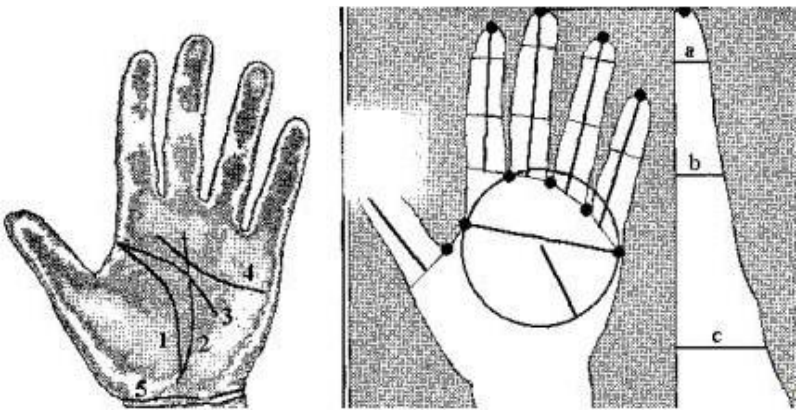


Рис. 1.3. Відбиток руки (ліворуч) та 3D-геометрія руки (праворуч).

Ціна системи: від 2000 до 5000 доларів США.

Ідентифікація за відбитками пальців є найпоширенішим методом біометричної ідентифікації, в основі якого лежить унікальність для кожної людини рисунка папілярних візерунків на пальцях. Зображення відбитка пальця, отримане за допомогою спеціального сканера перетворюється в цифровий код (згортку) і порівнюється з раніше введеним шаблоном або набором шаблонів (у випадку ідентифікації). Ряд фірм США (Fingermatrix, Identix, Thumbscon та інші) випускають недорогі пристрої ідентифікації за відбитками пальців. Дія цих пристроїв заснована на вимірюванні відстаней між основними дактилоскопічними ознаками.

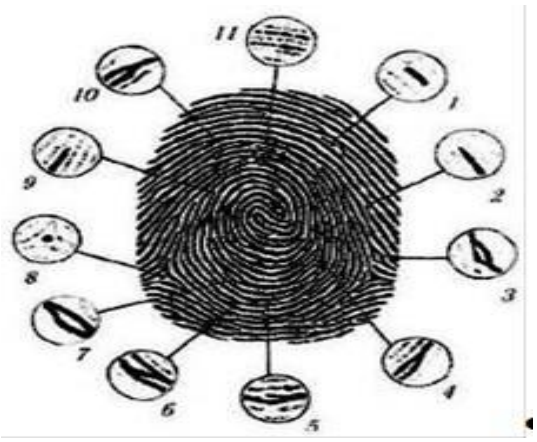


Рис. 1.4. Типи мінуцій, які використовують при дактилоскопічних дослідженнях.

Деталізуємо фрагменти, які підписані цифрами на рис. 1.4: 1 - фрагмент папілярної лінії; 2 - початок папілярної лінії; 3 – вічко; 4 - біфуркація-розгалуження; 5 – гачок; 6 – місток; 7 – острівець; 8 – крапка; 9 - закінчення папілярної лінії; 10 - біфуркація-злиття; 11 – включення.

Для запису кінцевого образу потрібно 400 – 1000 байт. Ціна пристроїв: від 200 до 4000 доларів США (хоча відомі й дешеві пристрої, але вони є менш точними і повільнішими). Ці пристрої визнані найкращими пристроями ідентифікації для споживачів, основними з яких є установи правопорядку та банки.

Розпізнавання за відбитками пальців є найбільш популярним серед біометричних методів, заснованих на фізичних характеристиках. На ці системи припадає близько 30% обсягу продажів біометричних систем. Однак у деяких людей процедура зняття відбитків пальців асоціюється з реєстрацією кримінальних елементів, що перешкоджає широкому впровадженню пристроїв цього типу.

Швидкість операції розпізнавання або ідентифікації в сучасних біометричних системах навіть за наявності тисяч користувачів (доступ персоналу до великих підприємств, аеропортів, атомних станцій) вимірюється секундами, тобто відповідає запитам виробничого режиму. Відомо, що найпершими користувачами систем біометричної ідентифікації були організації з високим рівнем безпеки: банки, ядерні реактори, арсенали. Багато банківських закладів у Європі, особливо в Швейцарії для доступу клієнтів до депозитних сейфів встановили біометричні системи на відбитках пальців, або розпізнавання по обличчю. Це дає змогу клієнтам користуватись депозитними сейфами без присутності співробітників банку. Можливості використання біометричних систем в службах прикордонного контролю, паспортах, ідентифікаційних картках, посвідченнях водіїв прискорюється із введенням єдиних міжнародних стандартів.

На українському ринку з'явилася пропозиція біометричних пристроїв для унеможливлення доступу до комп'ютерних систем і мережних ресурсів.

Основані на методах ідентифікації за відбитками пальців, невеликих розмірів, зручні і прості в користуванні, ці системи унеможливлюють неавторизований доступ до комп'ютерних і мережних ресурсів. Це може стати ефективним інструментом для інформаційних систем типу "клієнт-банк". Біометрія, в комплексі із криптографічними засобами, може бути встановлена в системах голосування, в тому числі для забезпечення посвідчення персони і на різних рівнях передачі результатів голосування для подальшої обробки. При цьому база даних шаблонів біометричної системи знаходиться на різних рівнях в архітектурі мережі.

Отже, біометрія й основані на її принципах системи стали ефективним засобом забезпечення безпеки всіх видів власності, захисту від шахрайства, фальсифікації та криміналу. Їх подальше впровадження в різні галузі є актуальним завданням, адже забезпечить створення зручних і надійних інструментів як для державного сектора, індустріальних і комерційних структур, так і для окремих громадян. Біометрія, може стати надійним захистом певного різноманітної інформації користувачів.

2. ВИБІР ЕЛЕМЕНТНОЇ БАЗИ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

2.1. Огляд відомих сканерів відбитків пальців

З усього розмаїття біометричних технологій, для вирішення задач інформаційної безпеки широке використання знайшли системи, які базуються на скануванні і розпізнаванні відбитку пальця. Порівняльні переваги даного виду біометричної ідентифікації є наступними [1,4]:

- у порівнянні з технологіями розпізнання за сітківкою і райдужною оболонкою ока – сканування відбитка пальця є дешевшим і зручнішим, тому що для входу в різні програмні системи і виконання в них критичних операцій, що вимагають строгої ідентифікації користувача, простіше кілька разів прикласти палець до вікна сканера, ніж кілька разів правильно приставляти око до камери;
- у порівнянні з технологіями розпізнання за формою і розташуванням вен на лицьовій стороні долоні – сканери відбитків пальців на порядок менш громіздкі і процес безпосереднього зчитування ідентифікуючих ознак є зручнішим;
- у порівнянні з технологіями розпізнання за формою і термограмою обличчя – усе що перелічено вище, тобто незручність використання в повсякденних діях і громіздкість устаткування;
- у порівнянні з технологіями розпізнання по рукописному і клавіатурному почерку – у технології ідентифікації за відбитком пальця на кілька порядків кращі статистичні показники помилок першого і другого роду.

Переходячи до огляду застосувань систем біометричної ідентифікації за відбитком пальця, статистика показує, що на сьогоднішній день, в розвинутих країнах, найпоширенішим є саме цей метод. Досвід розвинутих країн показує, що метод біометричної ідентифікації за відбитком пальця є і найбільш точним.

Нижче наведено характеристики та порівняння кількох готових пристроїв, які зараз широко застосовуються на ринку:

- Genuine CROSS MATCH ID500 Portable Ten-Print Scanner Finger Print Scanner.

Рис. 2.1. Зовнішній вигляд сканера відбитків пальців Genuine CROSS MATCH ID500.

Виробник пристрою (фірма Cross Match Technologies inc.) запевняє, що Cross Match ID 500 – це точна, міцна, мобільна система та найменший, найлегший, простий у використанні пристрій із всіх їхніх наявних зразків.

Його розміри: 170 х 440 х 262 міліметрів та вага: 5,2 кілограми. Область сканування має 200 точок на сантиметр, активна область зображення становить 52,1 х 91,4 мм. Динамічний діапазон 8 біт, 256 відтінків сірого. Потужність 12 В постійного струму при 1 А (12 Вт). Діапазон робочих температур: 2° С до 38° С (35°F до 100°F), вологість 10% – 90% без конденсації. Наявний внутрішній зчитувач магнітних карт AAMVA /ANSI 7811-5 та вбудований сенсорний екран розміром 121,2 х 93,5 мм (320 х 240 пікселів). Пам'ять: 256 Мб оперативної пам'яті, жорсткий диск: 30 Гбайт. Процесор Celeron 2,0 ГГц.

Система швидкого захоплення зображення, Rapid Auto Image Capture, автоматично визначає розміщення пальця та захоплює зображення без ручного втручання і додаткових кроків або натискань клавіш. Це забезпечує швидкий процес зняття відбитків пальців. Захоплює зображення високої якості незалежно від наявності плям на пальцях від чорнила, барвників, жиру і бруду, працює із сухими та жорсткими пальцями.

Вбудований зчитувач магнітних карт призначений для автоматичного зняття демографічних даних з водійських прав користувача, що скорочує час бронювання (при використанні пристрою авіакомпаніями чи деінде при потребі купити квиток, оплатити номер в готелі, тощо) і підвищує точність.

Real Time User Feedback – це система зворотного зв'язку з користувачем, що працює у режимі реального часу. Вона оснащена сенсорним екраном на сканері з підказками, що швидко проводить користувача через процес зняття відбитків пальців, забезпечуючи візуальний та звуковий зворотний зв'язок.

Наявне зручне програмне забезпечення з «випадними» меню, що також працює в режимі реального часу. У зв'язку з тим, що пристрій портативний, на його надійному корпусі є ручка для зручного транспортування.

Ціна: від 800 до 1200 доларів США.

2) digitalPersona U.are.U 516.

Рис. 2.2. Зовнішній вигляд сканера відбитків пальців digitalPersona U.are.U 5160.

Сенсорний пристрій U.are.U 5160 – це зчитувач відбитків пальців, що відповідає всім сертифікатам та стандартам якості. Оптичний сканер відбитків пальців призначений для використання в якості периферійного пристрою USB з сучасним дизайном і компактними розмірами: 72 мм (довжина) х 39 мм (ширина) х 21,7 мм (висота); мала вага.

Синя підсвітка покращує процес роботи з пристроєм та допомагає системі покращити точність сканування. Програмне забезпечення має змогу змінити колір підсвітки на зелений чи червоний у зв'язку з тим, чи коректно пройшов

користувач процес ідентифікації, чи ні. Це виключає потребу в додатковому моніторі.

Міцність корпусу та скла надає можливість використання пристрою в суворих умовах. Виробництво ведеться великими обсягами, що говорить про широке коло споживачів.

Ціна таких пристроїв: 200 – 400 доларів США.

3) Realand ZD2F20 Fingerprint Access Control and T&A.

Рис. 2.3. Зовнішній вигляд сканера відбитків пальців Realand ZD2F20.

Пристрій переважно використовується, як дверний замок для вхідних дверей квартири, багатоквартирних будинків, офісу, фабрик, готелів, шкіл і т.д.

Технічні характеристики пристрою:

- розширення екрану: 128 x 64 пікселі;
- екран працює в режимі реального часу;
- область сканування: 200 точок на сантиметр;
- коефіцієнт відмови в доступі при виникненні помилок (забороняється доступ користувачеві, зареєстрованому в систем – FRR) $\leq 0{,}1\%$;
- коефіцієнт допуску при виникненні помилки (враховуються випадки надати системою доступу користувачу який неавторизувався - процентний поріг, що визначає ймовірність того, що один користувач може бути прийнятий за іншого – FAR) $\leq 0{,}0001\%$;

- час ідентифікації ≤ 0,1 секунда;
- робочий режим: Off-line/On-line;
- режими ідентифікації: відбиток пальця, ID-картка, код доступу;
- порти вводу/виводу: TCP/IP, RS485;
- мова інтерфейсу: Англійська, Китайська, Корейська;
- потужність 12 В постійного струму, 1 А;
- діапазон робочих температур: 0°С – 80°С при відносній вологості повітря 80%.

Також, особливістю пристрою є сигналізація при спробі несанкціонованого демонтажу.

Ціна: від 200 до 500 доларів США.

Аналізуючи дані аналоги можна зробити висновок, що крім подібних загальних характеристик, дані пристрої відрізняються один від одного. Це зумовлено тим, що кожен з них має своє визначене застосування у певній сфері, що й підтверджує факт про широке розповсюдження цих пристроїв у побуті та їхню надійність.

Сфера застосування пристроїв біометричної ідентифікації, як бачимо є різноманітною. Одні пристрої застосовуються великими корпораціями для контролю персоналу та захисту важливої особистої інформації, інші застосовуються готелями чи іншими великими фірмами у якості перепустки до офісу чи особистого номеру, а деякі з них використовуються, як додатковий периферійний пристрій для персонального комп'ютера, тощо.

Від сфери застосування залежить і потужність пристрой його швидкодія пристрою та споживана потужність. У деяких наявних аналогах потужність досить висока, як і швидкодія, а для деяких дані характеристики не є суттєвими. Проте, у будь-якому випадку, швидкодія пристрою знаходиться на прийнятному рівні, бо це зумовлено швидкістю розвитку комп'ютерних технологій та відповідними вимогами користувачів. Споживана потужність є невеликою (від 5 до 25 В), а наявність у пристроях Off-Line та On-Line режимів

зменшує шанс виходу з ладу чи відмови у роботі та робить їх енергозберігаючими.

Наявність додаткової периферії хоч і є хорошим та корисним фактором, проте не завжди актуальним, так як це позначається на габаритах пристрою, його масі та споживаній потужності.

Так, як база даних фінальних контрольних зразків відбитків пальців може бути віддаленою та знаходитись на сервері, то його внутрішня пам'ять не обов'язково повинна мати великий об'єм, тим не менше, зважаючи на широкий спектр таких пристроїв, при апаратній реалізації системи такого типу потрібно пам'ятати, що після обробки зображення відбитка пальця, один кінцевий шаблон («темплейт») може сягати об'єму більше 1Кб пам'яті.

Ціни таких пристроїв, коливаються в рамках від 150 до 1200 доларів США (приблизно).

Отже, для побудови пристрою для біометричної іденнтифікації за відбитком пальця потрібно врахувати наступне:

- відповідність міжнародним стандартам;
- проходження процесу ідентифікації не повинен бути надто складним та забезпечувати точність ідентифікації при високій швидкодії;
- споживана потужність не повинна перевищувати 12 В при 1 А;
- відносно невеликі габарити та вагу;
- невисоку ціну реалізації готового пристрою.

2.2. Вибір мікроконтролера

В якості центрального контролера системи використано платформу Arduino UNO [6].

Arduino UNO – пристрій побудований на основі мікроконтролера ATmega328. Платформа має 14 цифрових входів/виходів (6 з яких можуть використовуватися як виходи широтно-імпульсного модулятора), 6 аналогових входів, кварцовий генератор 16 МГц, порт USB, порт для живлення, порт для внутрішньосхемного програмування ICSP і кнопку перезавантаження (рис. 2.4).

Для початку роботи необхідно під'єднати макетну плату до ПК чи ноутбука за допомогою кабелю USB, або подати живлення за допомогою адаптера AC/DC або батареї.

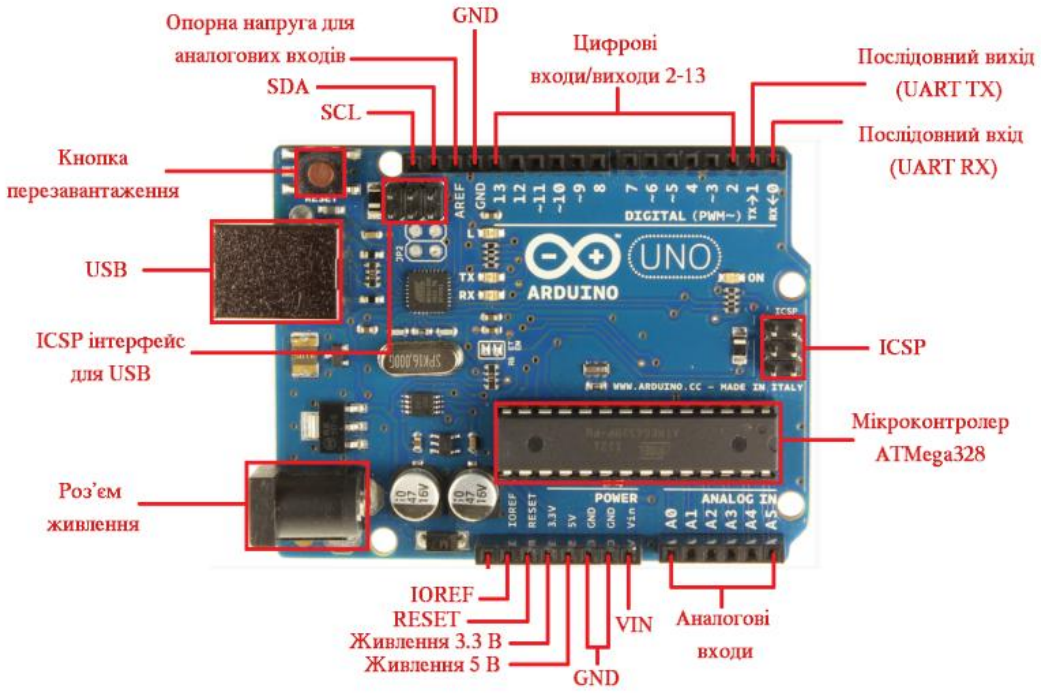


Рис. 2.4. Призначення виводів Arduino UNO.

На відміну від всіх попередніх плат, які використовували FTDI USB мікроконтролер для з'єднання з USB, новий Arduino UNO використовує мікроконтролер ATmega8U2.

Основні технічні характеристики Arduino UNO:

- робоча напруга – 5 В;
- напруга живлення (рекомендована) – 7-12 В;
- напруга живлення (гранична) – 6-20 В;
- цифрові входи/виходи – 14 (з них 6 можуть використовуватися в якості ШІМ-виходів);
- аналогові входи – 6;
- максимальний струм одного виводу – 40 мА;
- максимальний вихідний струм виводу 3,3V – 50 мА;

- Flash-пам’ять – 32 КБ (ATmega328) з яких 0,5 КБ використовуються завантажувачем;
- SRAM – 2 КБ (ATmega328);
- EEPROM – 1 КБ (ATmega328);
- тактова частота – 16 МГц.

2.3. Вибір модуля розпізнавання відбитків пальця

У якості модуля розпізнавання відбитків пальця вибрано оптичний давач FPM10A (рис. 2.5). Вибраний оптичний давач для відбитків пальців FPM10A зазвичай використовуються в системах безпеки [7]. Ці сенсори включають в себе DSP чіп, який обробляє зображення, робить необхідні розрахунки для виявлення відповідності між записаними і поточними даними. Дешевші модулі відбитків пальців дозволяють записувати до 162 різних відбитків пальців.

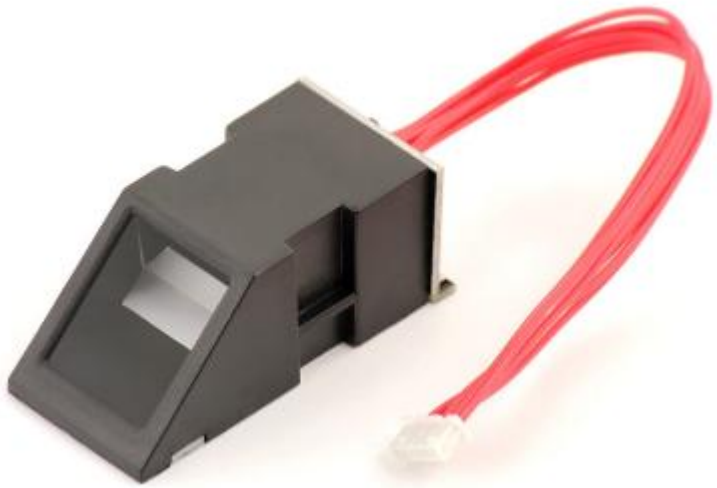


Рис. 2.5. Модуль розпізнавання відбитків пальця FPM10A.

Нижче наведено технічні характеристики модуля розпізнавання відбитків пальця FPM10A.

Технічні характеристики:

- Напруга живлення: DC 3.6 ~ 6.0 В/3.3 В;
- Струм живлення: 120 мА;
- Піковий струм: 150 мА;

- Час обробки зображення відбитка: <1.0 секунди;
- Розмір вікна: 14 мм х 18 мм;
- Кількість одночасно записаних файлів: 162;
- Режим відповідності: 1: 1;
- Режим пошуку: (1: N);
- Файл ПЗ: 256 байт;
- Файли шаблону: 5;12 байт;
- Ємність: 300;
- Кількість рівнів безпеки: 5;
- Коефіцієнт відхилень, при помилкових значеннях (FRR): <1.0% (при рівні безпеки 3);
- Час пошуку: <1.0 секунд (1: 500, середнє);
- Інтерфейс ПК: UART (TTL Logic Level) або usb2.0 / USB1.1;
- Швидкість передачі (UART): (9600 x N) BPS де N = 1 ~ 12 (значення за замовчуванням N = 6, 57600bps);
- Робоча температура: -20 °C - + 50 °C;
- Відносна вологість: 40% - 85%;
- Температура зберігання: 40 °C - + 85 °C.

На рис. 2.6 показано вигляд та розміри мікросхеми, яка кріпиться до модуля відбитків пальців FPM10A.

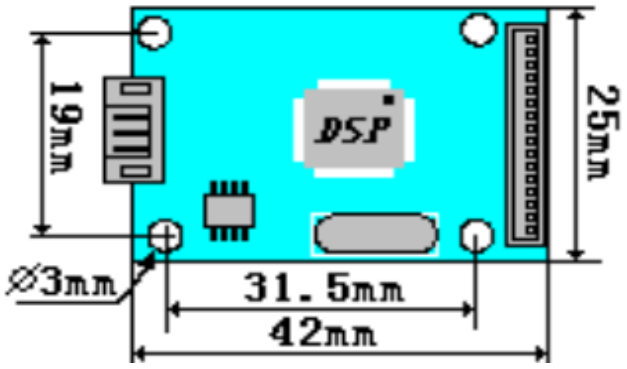


Рис. 2.6. Вигляд та розміри основної мікросхеми модуля FPM10A.

Як бачимо на даній мікросхемі розміщено основні компоненти модуля відбитків пальців DSP-чіп, роз'єми для під'єднання шлейфу та допоміжні SMD-компоненти.

2.4. Вибір зовнішньої пам'яті

У якості зовнішньої пам'яті можна використати Flash-пам'ять об'ємом 2 Гбайт, Transcend MicroSD, TS2GUSD [8]. На рис. 2.7 показано зовнішній вигляд карти пам'яті Transcend MicroSD та нумерація її контактів.

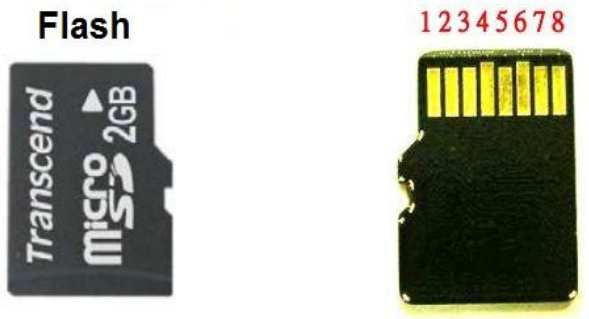


Рис. 2.7. Зовнішній вигляд карти пам'яті та нумерація контактів.

На рис. 2.8 подана внутрішня архітектура вибраного флеш-накопичувача Transcend MicroSD TS2GUSD.

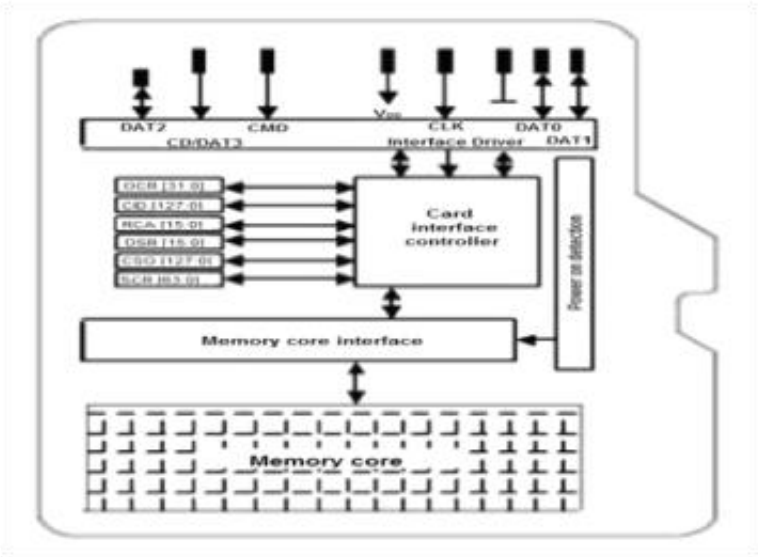


Рис. 2.8. Внутрішня архітектура флеш-накопичувача Transcend MicroSD TS2GUSD.

Даний зразок карти пам'яті серії MicroSD є енергонезалежним (зовнішнє джерело живлення не потрібно, щоб зберегти інформацію). До позитивних

якостей пам’яті такого типу також можна віднести: малі габарити (11мм х 15мм х 1мм), високу швидкість передачі даних та відмінну безпеку даних, що зберігаються. Напруга живлення 2,7 – 3,6 В. Діапазон робочих температур: від −25°C до +85°C.

Таблиця 2.1.

Призначення контактів карти пам’яті TS2GUSD

№ ніжки	Назва	Тип	Опис
1	RSV		Зарезервовано
2	CS	I	Вибір карти пам’яті
3	DI	I	Лінія даних для запису
4	V_{DD}	S	Напруга живлення
5	SCLK	I	Лінія синхроімпульсів (Clock)
6	V_{SS}	S	Логічна земля (Ground)
7	DO	O/PP	Лінія даних для читання
8	RSV		Зарезервовано

(S: Живлення; I: Вхід; O: Вихід; PP: Push-Pull)

2.5. Вибір дисплея LCD 1602A

В роботі вибрано рідкокристалічний дисплей LCD1602A (рис. 2.9), який побудовано на технолгії рідких кристалів [9].

Дисплей LCD1602A міститить плату конвертер для перетворення паралельного 8-бітного інтерфейсу дисплею в шину I2C, за допомогою якої він і підключається до плати Arduino за адресою яка виставляється перемичками. Наявність послідовного інтерфейсу дозволяє забезпечувати зв’язок з контролером Arduino за допомогою 2-х провідного зв’язку, це допоможе зменшити кількість використаних цифрових пінів контролера для підключення додаткової периферії.

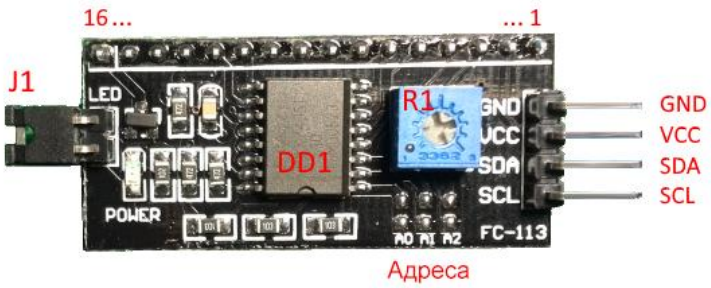
Контактні площадки A1 ... A3 використовуються для зміни адреси I2C пристрою. Встановлюючи відповідні перемички, можна змінювати адресу пристрою. На рис. 2.10 наведено відповідність адрес і перемичок: «0»

відповідає відсутністю контакту, «1» - встановленій перемичці. За замовчуванням всі 3 перемички розімкнені і адреса пристрою 0x27.

Дисплей LCD 1602A I2C може одночасно відображати до 32 символів (16 символів, 2 рядки). Дисплей оснащений світлодіодним підсвічуванням, колір підсвітки може бути різним в залежності від модифікації.

Контролер дисплея HD44780 має ПЗП в якій зберігаються цифри, символи латиниці, для їх відображення на дисплеї. Відсутні символи, в тому числі і символи кирилиці, можна завантажувати в пам'ять ОЗП контролера.

Рис. 2.9. Символьний дисплей LCD 1602A.



A2	A1	A0	Адреса
1	1	1	**0x20**
1	1	0	**0x21**
1	0	1	**0x22**
1	0	0	**0x23**
0	1	1	**0x24**
0	1	0	**0x25**
0	0	1	**0x26**
0	0	0	**0x27**

Рис. 2.10. Відповідність адрес і перемичок модуля PCF8574.

Мікросхема може використовуватися для керування дисплеєм з використанням контролера HD44780, в 4-х бітному режимі. Для цієї мети на платі встановлена мікросхема PCF8574, яка є перетворювачем шини I2C в паралельний 8 бітний порт.

Плата модуля розведена таким чином, щоб її можна було відразу під'єднати до дисплею. На платі одразу встановлені підтягуючі резистори на лініях SCL і SDA, потенціометр для регулювання контрастності дисплея та джампер який вмикає/вимикає підсвічування дисплею.

Схема підключення дисплея до Arduino Uno наведена на рис. 2.11.

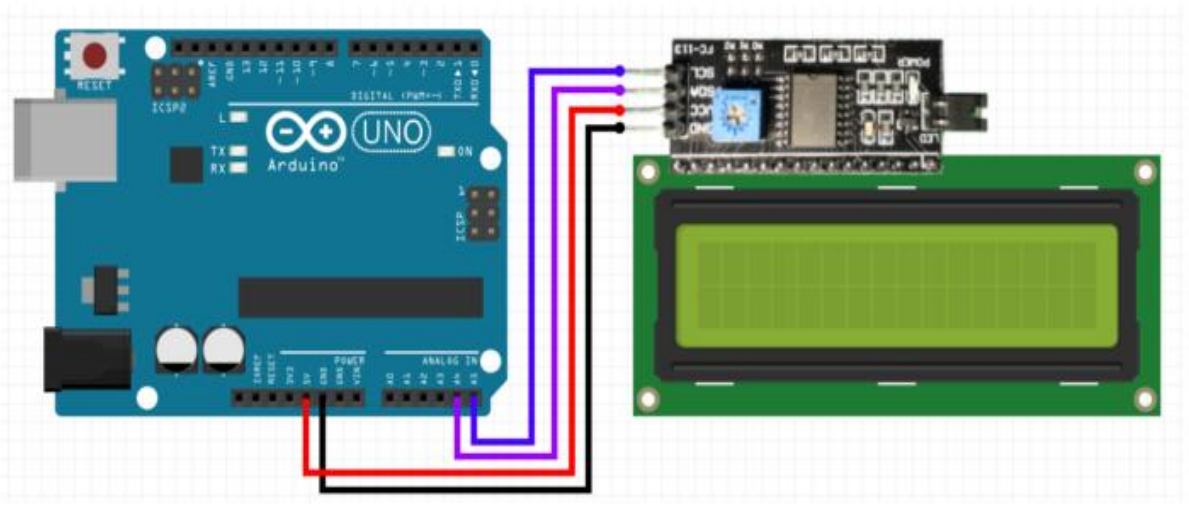


Рис. 2.11. Схема підключення дисплея LCD 1602A I2C до Arduino Uno.

Характеристики LCD 1602 I2C:

- Тип дисплея: рідкокристалічний символьний.
- Кількість символів в рядку: 16.
- Рядків: 2.
- Контролер HD44780.
- Світлодіодна підсвітка.
- Символьний тип відображення, є можливість загрузки символів.
- Кут огляду: 180 °.
- Напруга живлення: 5В.
- Робоча температура: від -20 °С до +70 °С.
- Розміри: 98 х 60 х 12 мм.
- Вага: 80 гр.

2.6. Вибір середовища програмування Arduino IDE

Для написання програми для вибраного мікроконтролерного макету Arduino Uno вибрано середовище розробки – Arduino IDE. Дане програмне

середовище має велику кількість переваг: використовує мало пам'яті, невибаглива до ресурсів комп'ютера, проста і зручна у користуванні, легка у підключенні до плати та багато інші.

На рис. 2.12 зображено головне вікно вибраного програмного середовища Arduino IDE [10].

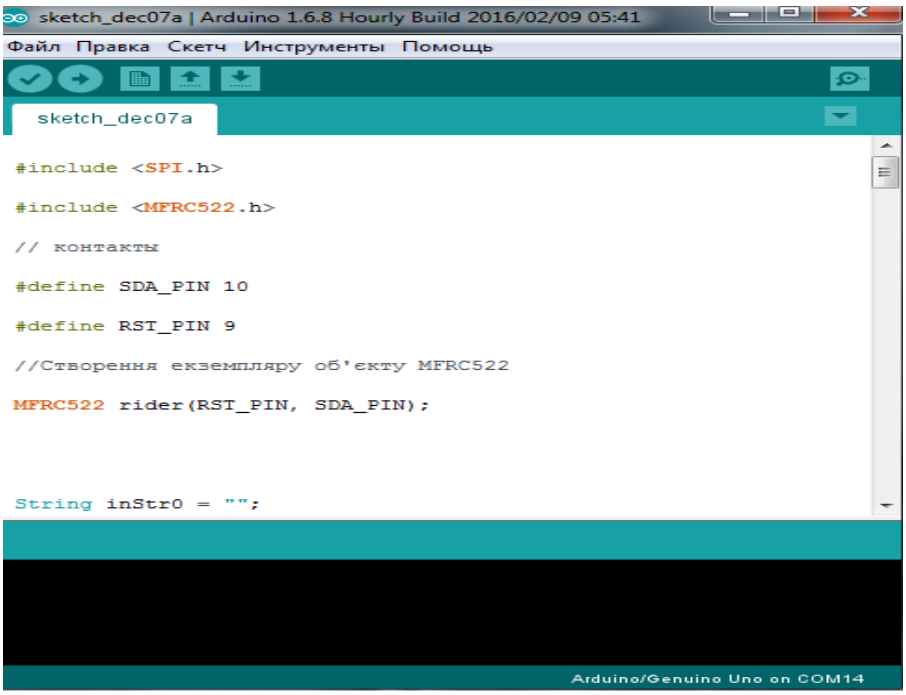


Рис. 2.12. Інтерфейс програми Arduino IDE.

Як видно із рисунку, середовище складається з вбудованого текстового редактора коду, вікна виводу тексту (консоль), панелі інструментів з кнопками команд. Що використовуються найчастіше і декількох меню. Програма, що була написана в Arduino IDE називається скетч. Програма (скетч) пишеться у текстовому редакторі на мові програмування C/C++. Скетч складається з 2 блоків, це блок *setup* та блок вічного циклу - *loop*. У першому блоці приписуються налаштування пінів, ініціалізація певних допоміжних блоків. Другий блок є основним тілом програми. Тут записується основний код програми, тобто певні зчитування з давачів, обробка даних, виведення інформації. Код, який знаходиться у функції *loop* виконується циклічно. Вікно виводу тексту, або ж консоль, відображає повідомлення про хід завантаження повідомлення помилок, що виникли у ході компіляції або завантаження скетчу.

3. ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

3.1. Опис структурної схеми пристрою біометричної ідентифікації

Розроблений пристрій біометричної ідентифікації за відбитком пальця може використовуватись для реалізації різних технічних рішень, включаючи електронні дверні замки, системи запалювання двигунів внутрішнього згорання (ДВЗ), USB флеш-накопичувачі з контролем доступу за відбитком пальця, та багато інших. Цифрові елементи обробки сигналів у сканері відбитків пальців виконують складні функції цифрової обробки сигналів, такі як фільтрування, перетворення, виділення ознак, операції зіставлення (порівняння) та інші алгоритмічні функції.

На рис. 3.1 показано спрощену структурну схему пристрою біометричної системи ідентифікації за відбитком пальця.

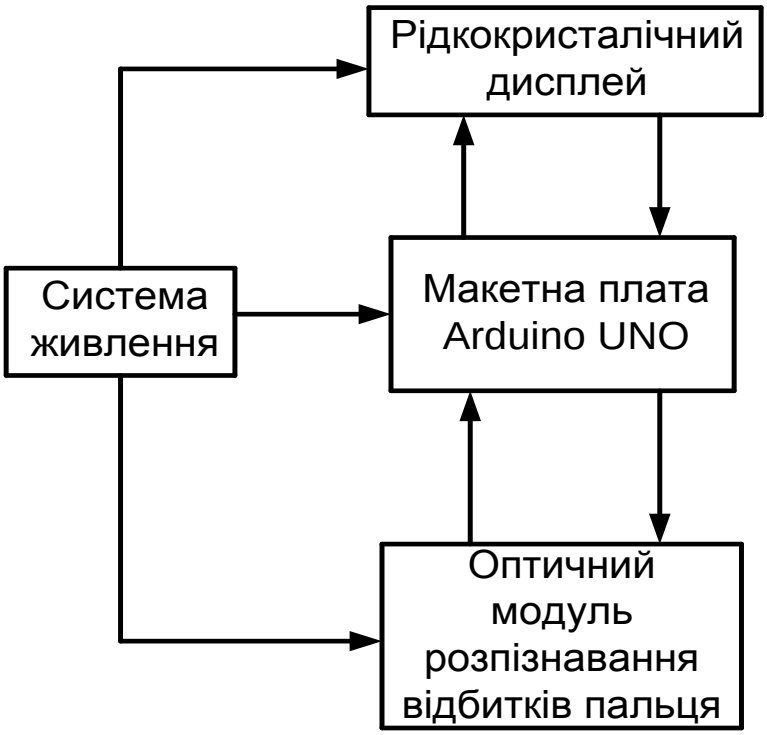


Рис. 3.1. Структурна схема спрощеної системи біометричної ідентифікації за відбитком пальця.

Спрощена система біометричної ідентифікації складається із макетної плати Arduino UNO, оптичного модуля розпізнавання відбитків пальців (FPM10A), рідкокристалічного дисплею (LCD1602A) та системи живлення.

При ідентифікації персони за відбитком пальця створюється бібліотека шаблонів відбитків пальців користувачів в межах невеликої офісної фірми. При запуску процесу ідентифікації користувач підносить палець до оптичного сканера, який сканує папілярний відбиток пальця руки та на основі методу порівняння даного відбитку із наявними у базі відбитками пальців за унікальними елементарними деталями рисунка визначає імовірність подібності відбитків. При низькій імовірності система видасть повідомлення на екран монітору чи дисплею про невідповідність відбитків та заблокує доступ користувача. При високій імовірності більше 85% система надасть доступ користувачу, про що буде повідомлено на моніторі чи дисплеї.

На рис. 3.2 показано розширену структурну схему пристрою біометричної системи ідентифікації за відбитком пальця.

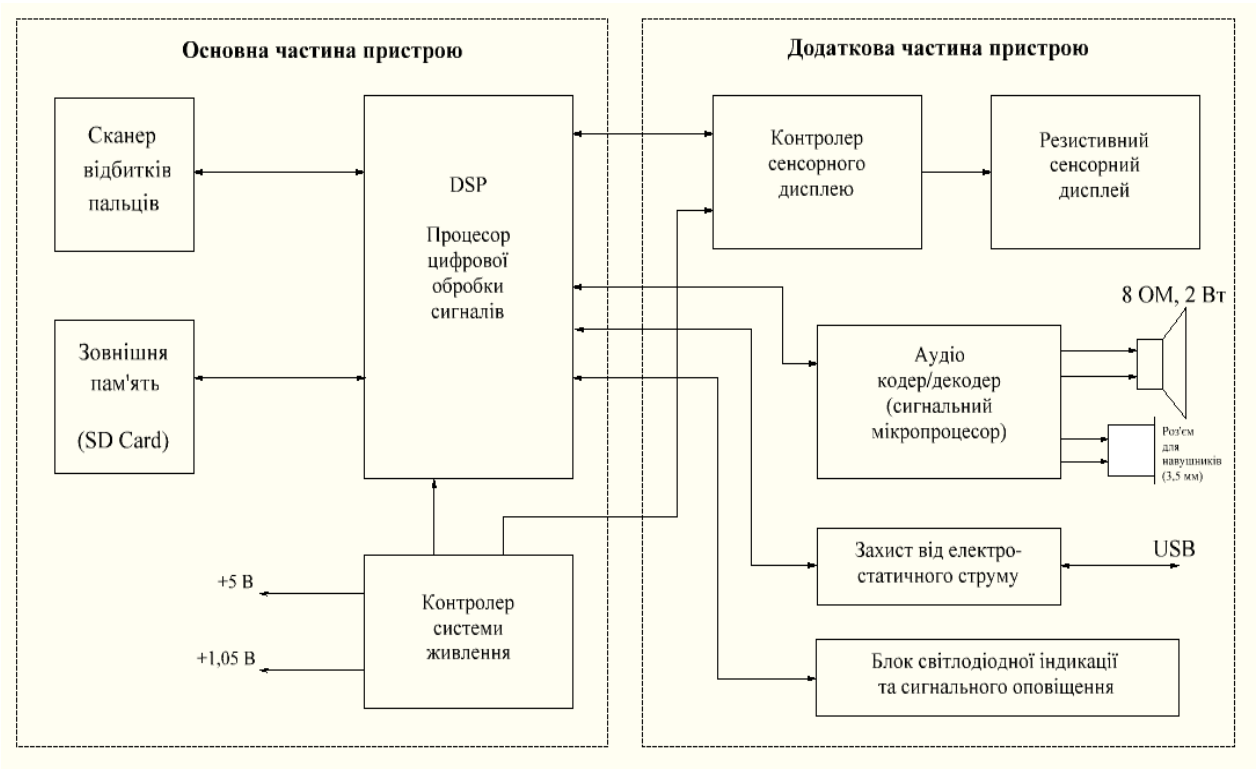


Рис. 3.2. Структурна схема розширеної системи біометричної ідентифікації за відбитком пальця.

Основна частина пристрою складається із сканера відбитків пальця (FPM10A), який підсвічує відбиток за допомогою лазера чи світлодіоду, що випромінює некогерентне світло, якщо крізь нього проходить електричний струм, а потім захоплює зображення за допомогою приладу із зарядовим

зв'язком (ПЗЗ) чи більш дешевим метал-діелектрик-напівпровідниковим (КМОН) сенсором, що являє собою напівпровідниковий сенсор, побудований на основі КМОН-транзисторів. Датчик відбитків пальців є типовим автономним модулем, який включає в себе аналого-цифровий перетворювач, щоб перетворити аналогову інформацію в цифровий потік даних. Роздільна здатність, динамічний діапазон і щільність пікселів є факторами, що сприяють підвищенню якості зображення і впливають на точність датчика. Після того, як зображення захоплено, цифрова інформація передається до процесора цифрової обробки сигналів для генерації збігів (DSP-чіпу). Першим кроком у процесі порівняння є кондиціювання відсканованого відбитку пальця (створення так званого шаблону). Зчитувачі відбитків пальців рідко використовують повний відбиток для ідентифікації. Частіше використовуються алгоритми цифрової обробки сигналів для визначення унікальних особливостей та закономірностей кожного відбитку для створення унікального цифрового коду. У шаблоні зберігаються лише координати розташування багатьох деталей малюнка щодо обраної точки (центра). Другий крок виконується за допомогою проміжного програмного забезпечення де отриманий цифровий код, згенерований із відсканованого зображення порівнюється з кожним із зразків у базі даних потенційних збігів. Цей крок вимагає від системи доступ до інформації з відбитками у мережевій базі даних або на енергонезалежному блоці зовнішньої пам’яті. Контролер системи живлення призначений для живлення системи від блоку живлення змінного струму, або від порту USB 2.0.

Додаткова частина пристрою складається із резистивного сенсорного дисплею, який використовується для відображення повідомлень або варіантів меню, модуля захисту від електростатичного струму, блоку світлодіодної ідентифікації та сигнального оповіщення, аудіо кодера/декодера для забезпечення зворотного зв'язку з користувачем у вигляді оповіщень або попередньо записаних голосових команд.

Після того, як зображення захоплено, цифрова інформація передається до процесора цифрової обробки сигналів для генерації збігів (DSP-чипу). Першим

кроком у процесі порівняння є створення так званого шаблону відсканованого відбитку пальця. Зчитувачі відбитків пальців рідко використовують повний відбиток для ідентифікації. Частіше використовуються алгоритми цифрової обробки сигналів для визначення унікальних особливостей та закономірностей кожного відбитку для створення унікального цифрового коду. У шаблоні зберігаються лише координати розташування багатьох деталей малюнка щодо обраної точки (центра), як це показано на рис 3.3.

Рис. 3.3. Виділення елементарних деталей малюнка папілярних ліній.

Другий крок виконується за допомогою проміжного програмного забезпечення де отриманий цифровий код, згенерований на основі відсканованого зображення порівнюється з кожним із зразків у базі даних потенційних збігів. Цей крок вимагає від системи доступ до інформації з відбитками у мережевій базі даних або на енергонезалежному блоці пам’яті.

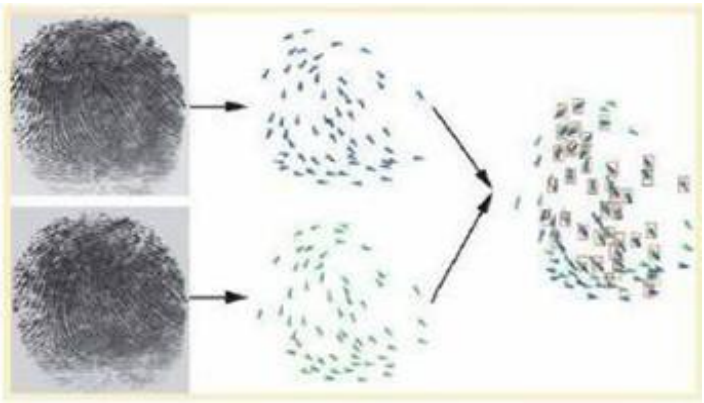


Рис. 3.4. Метод порівняння двох відбитків пальця за унікальними елементарними деталями рисунка.

Рідкокристалічний дисплей може бути використаний для відображення повідомлення або варіантів меню. Інтеграція контролера сенсорного екрану у цей пристрій надає можливість для користувача вибрати певні опції з відображеного меню.

У роботі використано рідкокристалічний дисплей LCD 1602A через його технічні характеристики та простоту під'єднання до мікропроцесора (йому потрібно всього вісім портів введення/виведення). Він використовує стандартний драйвер дисплею Hitachi HD44780 та має всі необхідні процедури для відображення символів, горизонтальних і вертикальних гістограм, стану ОЗУ або ПЗУ, тощо.

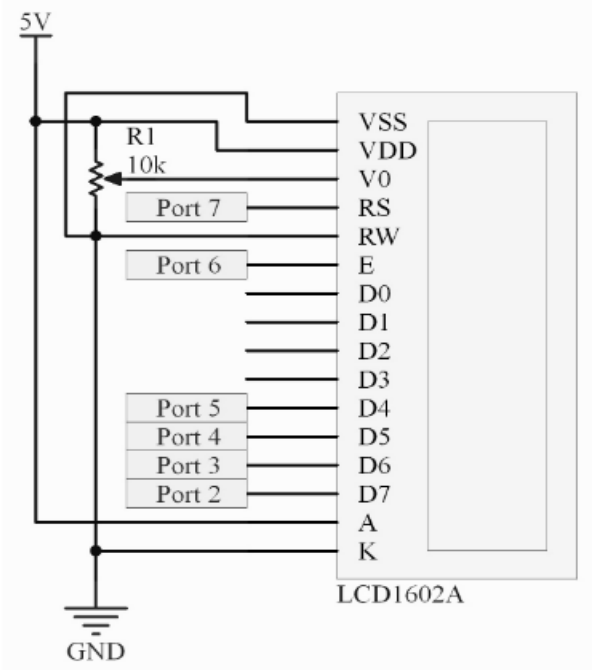


Рис. 3.5. Типова схема виводів дисплею LCD1602A.

Аудіо функціонал також може бути включений у цей пристрій, щоб забезпечити зворотний зв'язок з користувачем у вигляді оповіщень або попередньо записаних голосових команд. Це досягається за допомогою можливості послідовної шини даних I^2C забезпечити цифровий аудіо-потік на аудіо цифро-аналоговий перетворювач (ЦАП). Пристрій, на зразок DAC3120, призначений для перетворення цифрового аудіо-потоку в аналоговий сигнал, а також для збільшення системної інтеграції шляхом включення вбудованого аудіо підсилювача класу АВ (тобто підсилювача, що працює використовуючи

дві лампи або на транзисторах, за тим же принципом, як і підсилювач класу В, де «позитивна» половина півхвилі сигналу підсилюється одним транзистором, а «негативна» половина — іншим, однак тут поле дії обох транзисторів взаємно перекривають одне одного, що дозволяє зменшити кількість нелінійних перекручувань, в той же час у порівнянні з класом А, у яких повний сигнал підсилюється однією лампою або транзистором, підсилювачі класу АВ мають значно кращий коефіцієнт корисної дії – ККД), який може керувати моно-динаміком потужністю до 2,5 Вт.

3.2. Під'єднання модуля відбитків пальців FPM10A

Виконаємо під'єднання модуля розпізнавання відбитків пальця FPM10A до мікропроцесорного комплекту Arduino UNO. На рис. 3.6 подано схему з'єднання. Плата модуля розпізнавання відбитків пальця FPM10A має 6 дротів, з яких для під'єднання використовуються 4 дроти (GND – земля, VCC – живлення 5В, Tx – лінія передачі даних через UART та Rx – лінія прийому даних через UART, дані ліній прийому і передачі під'єднуються до цифрових виводів модуля Arduino UNO).

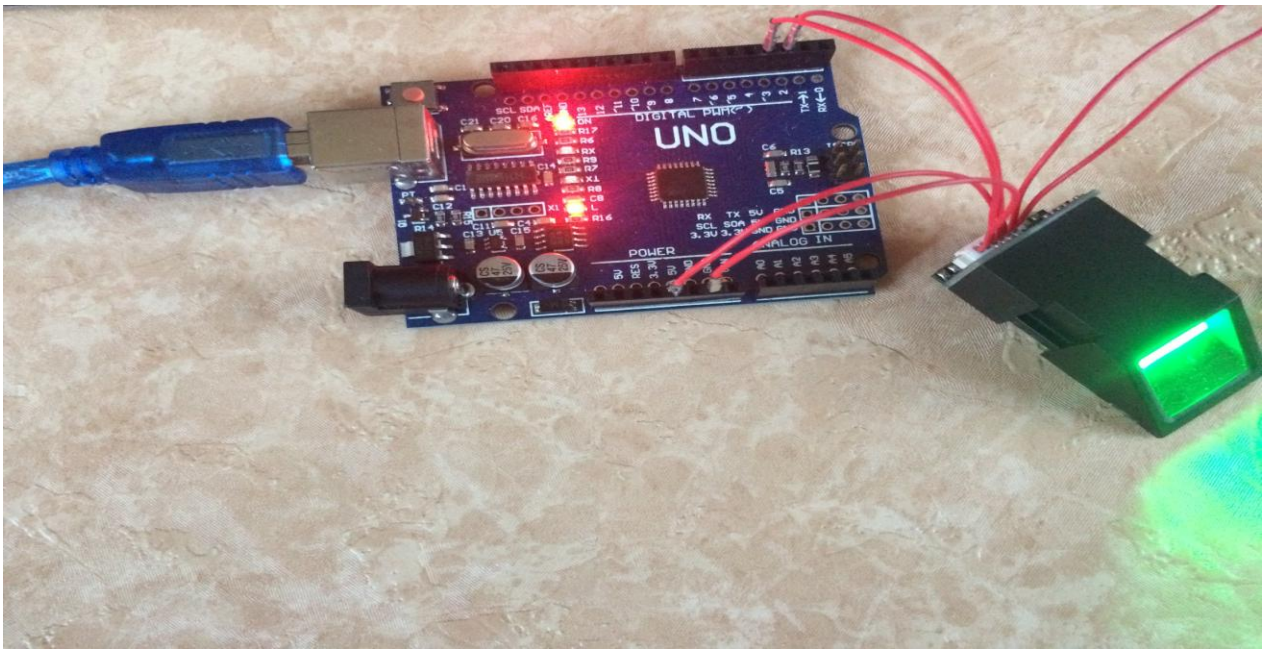


Рис. 3.6. Під'єднання модуля FPM10A до Arduino UNO.

Наступним кроком запускаємо середовище програмування Arduino IDE та встановлюємо бібліотеку для роботи з модулями відбитків пальців (Adafruit

Fingerprint Sensor Library). Коли дана бібліотека встановлена і додана в бібліотеку середовища Arduino IDE, запускамо Приклади -> Adafruit Fingerprint Sensor Library -> enroll. Лістинг програми подано в Додатку А. Відкриється бібліотечний код програми, яка дозволяє записати та зберегти у пам'яті модуля відбитки пальців користувачів даний модуль має певні обмеження, можна записати до 162 різних відбитків).

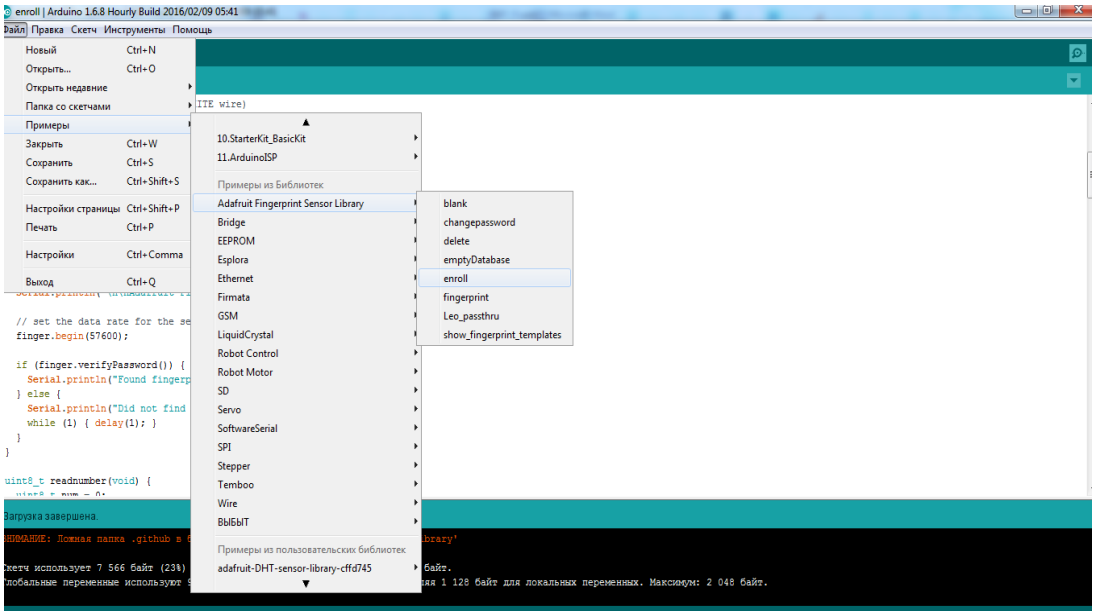


Рис. 3.7. Запуск програмного коду для записування відбитків пальців.

Після перевірки та завантаження даного скетчу в мікроконтролер та запуску монітору порта на швидкості 9600 біт (рис. 3.8), програма видасть повідомлення про те, що модуль відбитків знайдений та готовий до роботи, після цього система просить ввести номер ідентифікатора ID під яким користувач повинен зберегти відбиток пальця у базі даних системи. В даному випадку вводиться 1 (оскільки відскановується перший відбиток пальця) та натискається кнопка Відправити.

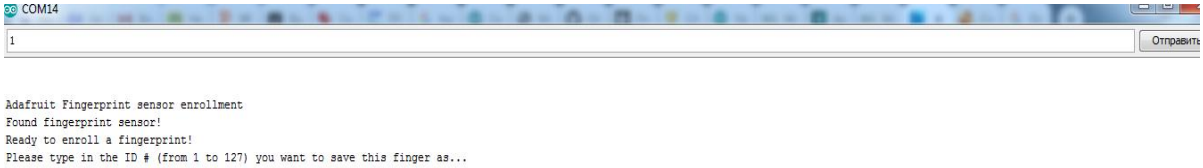


Рис. 3.8. Ввід номера ідентифікатора ID відбитку пальця.

Далі потрібно піднести відбиток пальця до сенсора, система попросить зробити це два рази, та видасть повідомлення про конвертацію відбитку та його збереження Prints matched під вказаним номером в базі даних (рис. 3.9).

```
Image taken
Image converted
Remove finger
ID 1
Place same finger again
.....................................................................................................................
Image converted
Creating model for #1
Prints matched!
ID 1
Stored!
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Рис. 3.9. Конвертація та збереження відбитку пальця за вказаним ID.

Наступним кроком з бібліотеки для роботи з відбитками пальця середовища Arduino IDE, запускамо наступний скетч, заходимо Приклади -> Adafruit Fingerprint Sensor Library -> fingerprint. Лістинг програми подано в додатку Б. Відкриється бібліотечний код програми, який дозволяє провести порівняння відбитків пальців, які вже записані до бази даних з відбитками пальців, які будуть підноситися до сенсора.

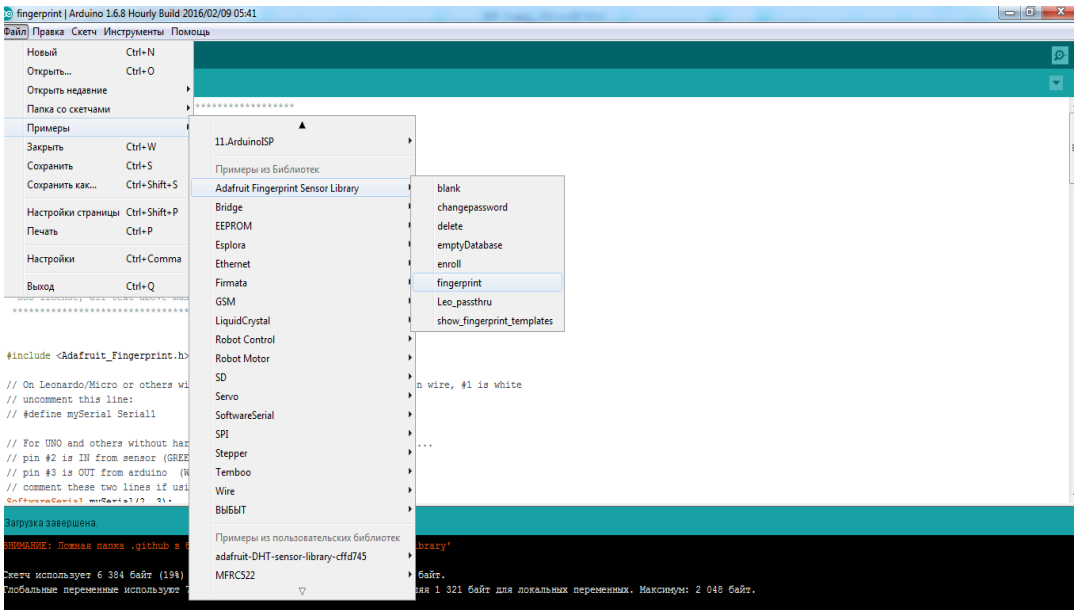


Рис. 3.10. Запуск програмного коду для порівняння відбитків пальців.

Після перевірки та завантаження даного скетчу в мікроконтролер та запуску монітору порта на швидкості 9600 біт (рис. 3.11), програма видасть повідомлення про те, що в базі даних вже є записано 3 відбитки чи шаблони. Після піднесення відбитку пальця до сенсора та його сканування програма

видасть номер ідентифікатора, який співпадає з даним відбитком а також виводиться довіра (confidence) і чим вона вища, тим більша імовірність співпадання піднесеного відбитку пальця із наявним вже записаним відбитком в базі даних.

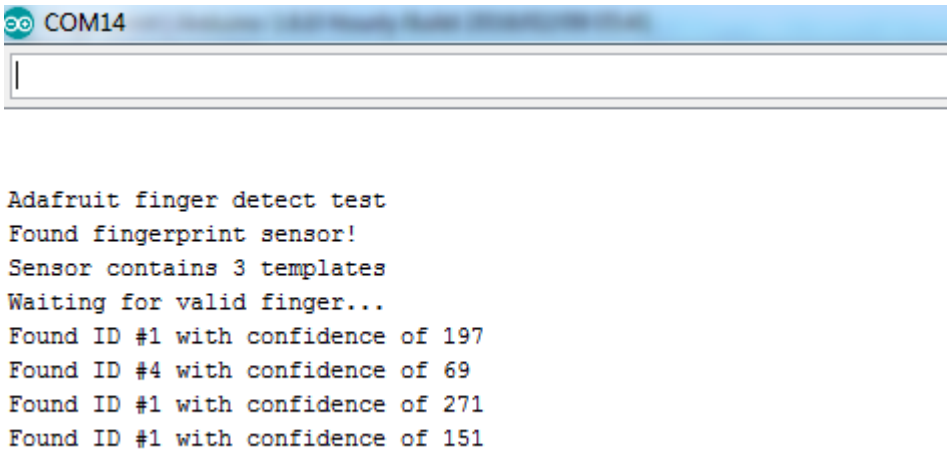


Рис. 3.11. Порівняння піднесених відбитків пальців із наявними у базі даних за їх номерами ID.

При роботі із модулем відбитків пальців були використані такі основні функції:

1. Функція fingerprint_setup () – дозволяє конфігурувати послідовний порт для швидкості обміну 9600 бод і підключається до модуля;
2. readFingerprint () – функція опитування, яка повертає -1, якщо щось відбулося не так, або повертає інформацію про те, що знайдено відповідний відбиток;
3. enrollFingerprint (int id) – додає відбиток пальця в систему із присвоенням ідентифікатора ”id”.

3.3. Під’єднання рідкокристалічного дисплею LCD1602A

Для під’єднання рідкокристалічного дисплею LCD1602A до мікропроцесорного комплекту Arduino Uno, потрібно проаналізувати функції виводів дисплею (рис. 3.12).

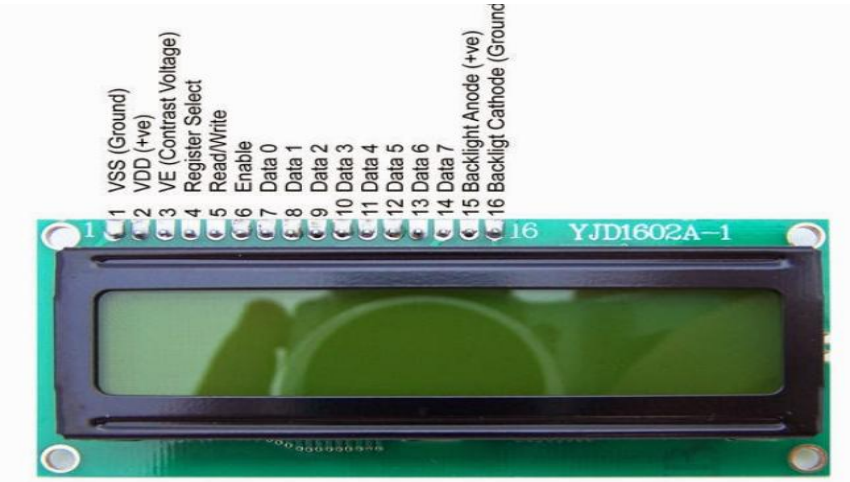


Рис. 3.12. Деталізація виводів рідкокристалічного дисплею LCD1602A.

Виводи дисплея LCD1602A мають такі функції:

1. VSS (Ground) – земля;
2. VDD (+ve) – живлення (+5В);
3. VE (Contrast Voltage) – встановлення контрасту дисплея;
4. Register/Select – вибір регістра;
5. Read/Write – Запис/читання даних;
6. Enable – дозвіл;

7-14. Data0 – Data7 – 8 ліній даних;

15. Backlight Anode – збільшення яскравості підсвітки дисплею;

16. Backlight Cathode – зменшення яскравості підсвітки дисплею.

На рис. 3.13. показано схему електричну принципову на якій підключено рідкокристалічний дисплей LCD1602A до мікропроцесорного плати Arduino Uno. Недоліком даного дисплею є те, що дисплей має 16 виводів і обов'язковими для підключення є 6 виводів а в деяких випадках і більше, тому при використанні додаткових сенсорів його під'єднання до Arduino Nano і Arduino Uno має деякі обмеження через брак виводів. Для уникнення даного недоліку рекомендується використовувати модуль I2C, який можна легко припаяти до екрану LCD1602A, це дасть можливість зекономити на кількості під'єднаних проводів до 4 (2 з них будуть використовуватися для даних і 2 для системи живлення).

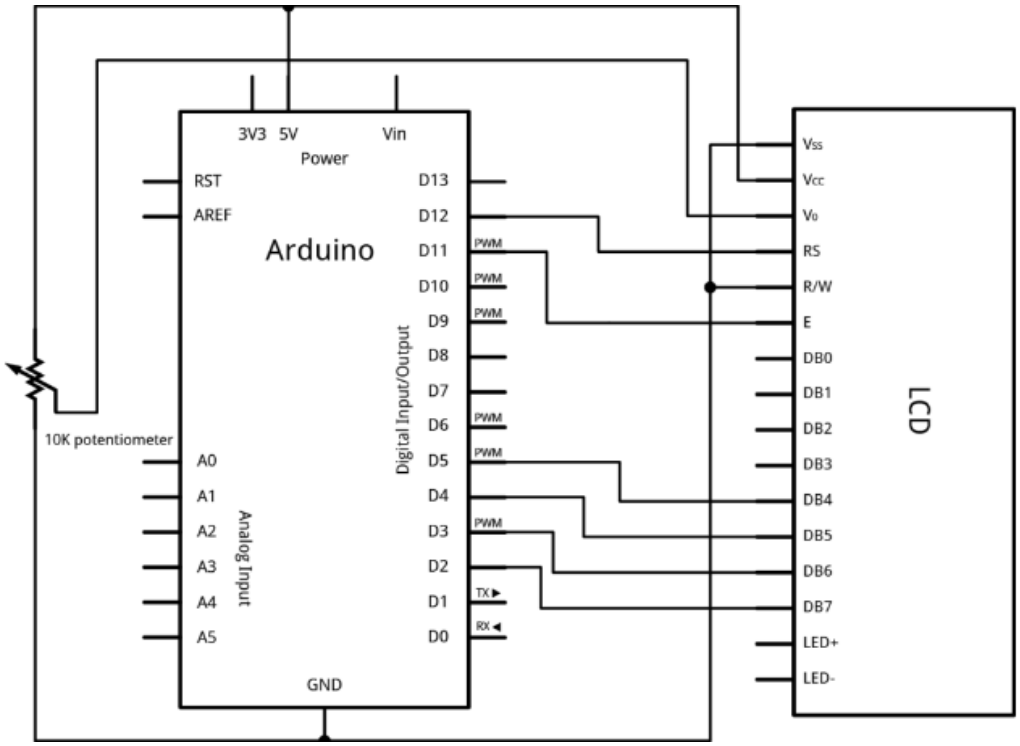


Рис. 3.13. Схема електрична принципова підключення дисплею LCD1602A до плати Arduino Uno.

На рис. 3.14. показано схему під'єднання модуля LCD1602A I2C до мікропроцесорної плати Arduino Uno.

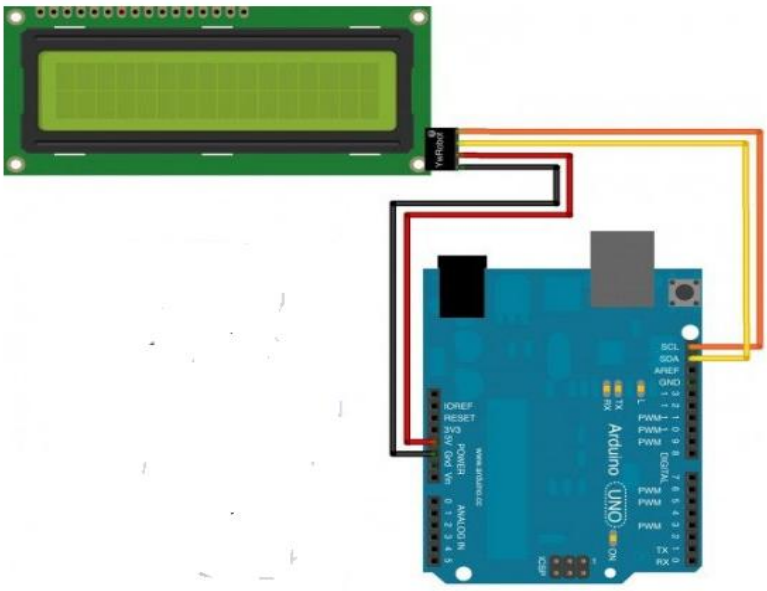


Рис. 3.14. Під'єднання модуля LCD1602A I2C до Arduino UNO.

Для роботи LCD1602A з використанням модуля I2C потрібно лінії SDA (лінія даних), SCL (лінія синхронізації), вивід для підключення живлення VCC - +5В та вивід для підключення землі GND.

Для взаємодії плати Arduino Uno із LCD1602A по шині I2C потрібно підключити, як правило 2 бібліотеки:

1. Бібліотеку Wire.h – для роботи із шиною I2C, яка є вбудованою в середовище Arduino IDE.
2. Бібліотеку LiquidCrystal_I2C, яка включає в себе велике число різноманітних команд для керування роботою рідкокристалічного дисплею по шині I2C.

3.4. Розроблення пристрою ідентифікації та алгоритму його роботи

На рис. 3.15 подано розроблений пристрій ідентифікації персони за відбитком пальця.

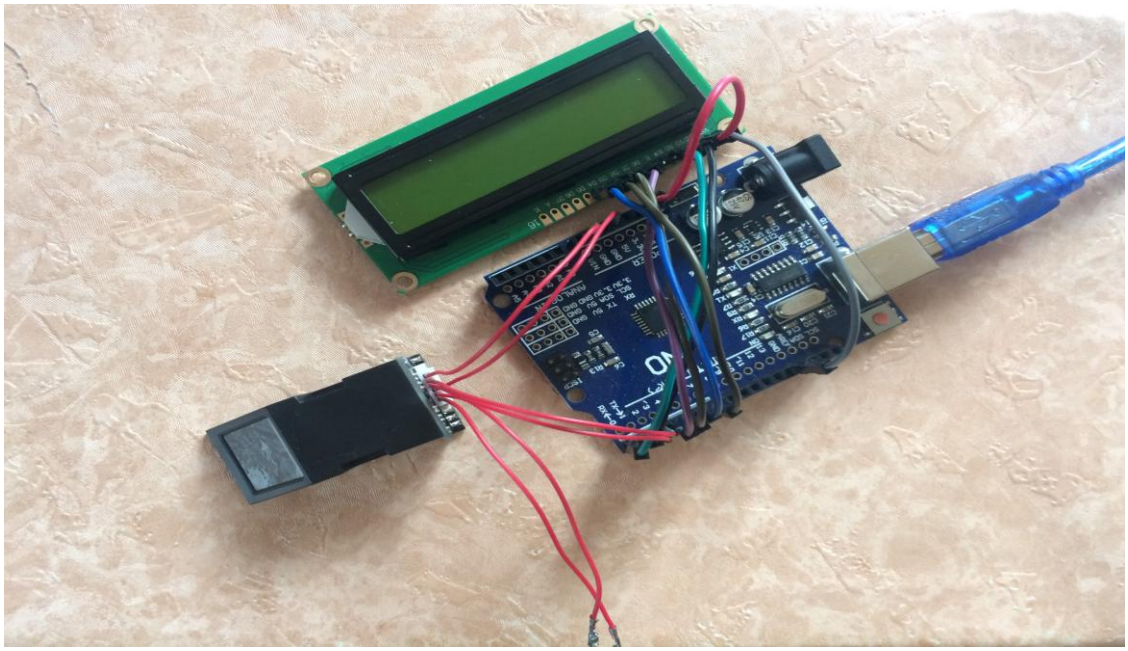


Рис. 3.15. Пристрій ідентифікації персони за відбитком пальця.

Розроблений пристрій складається з оптичного сенсора відбитку пальця FPM10A, який призначений для сканування папілярних відбитків користувачів та їх збереженні у базі даних та виконанні процесу ідентифікації персони за відповідним алгоритмом, рідкокристалічного дисплею LCD1602A за допомогою якого інформація про ідентифікацію особи виводиться візуально виводиться на екран та мікропроцесорного модуля керування Arduino Uno.

При розробленні програмного забезпечення пристрою ідентифікації були використані бібліотеку для роботи з сенсором відбитків пальця (Adafruit_Fingerprint.h), з рідкокристалічним дисплеєм (LiquidCrystal.h) та бібліотека (SoftwareSerial.h) для передачі даних:

#include < LiquidCrystal.h>

#include <Adafruit_Fingerprint.h>

#include <SoftwareSerial.h>

Основний код програми функціонування пристрою ідентифікації подано в Додатку В.

На рис. 3.16 описано запропоновану блок-схему алгоритму роботи системи ідентифікації персони за відбитком пальця.

Пристрій працює в режимі енергозберігання. При його ввімкненні проводиться перевірка цілісності системи. Якщо є якийсь збій відправляється повідомлення на віддалений сервер і вмикається сигналізація про збій системи. Якщо все гаразд, починається опитування сенсора сканування, наступним кроком проводиться процес сканування папілярного відбитку пальця, далі відбувається оцифровування отриманого зображення за допомогою алгоритмів ідентифікації. Далі відбувається порівняння отриманого цифрового коду зображення відбитку пальця із кожним із зразків зображень відбитків пальців, які є збережені у базі даних, далі запускається процес перевірки генерації збігів, якщо відбиток пальця співпав із наявним відбитком пальця у базі даних то відбувається успішна процедура ідентифікації і користувачу надається доступ до ресурсів системи у протилежному випадку система видасть на екран код помилки, про незбіжність відбитку пальця і доступі буде відмовлено.

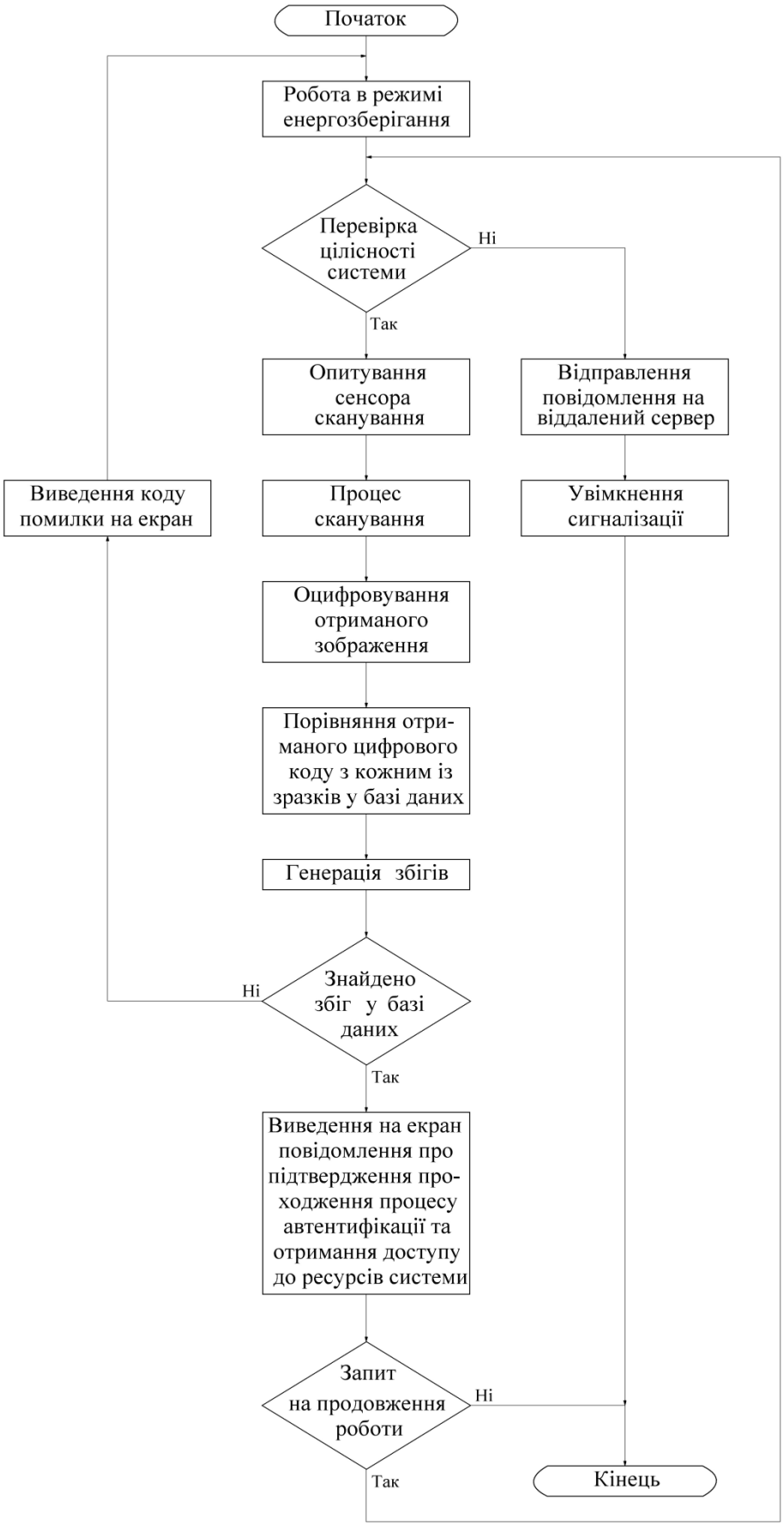


Рис. 3.16. Блок-схема алгоритму роботи пристрою ідентифікації.

4. ЕКОНОМІЧНА ЧАСТИНА

В данному розділі бакалаврської кваліфікаційної роботи обґрунтовується економічна доцільність розробки спеціалізованого мікропроцесорного пристрою біометричної ідентифікації персони за відбитком пальця.

Реалізація цієї системи допоможе покращити захист персональних даних, обмежити доступ до використання певних пристроїв та спростити процес автентифікації персони. Є аналоги такої системи, що виробляються у промислових масштабах, проте можна відзначити, що всі ці аналоги мають або безліч зайвих комплектуючих, без яких можна було б обійтись, які досить дорогі і виконують не всі функції, або мають недостатньо такої периферії. Розроблена система складається з відносно дешевших елементів, за допомогою яких було реалізовано доволі функціонально складну систему, яка виконує свої завдання не гірше за аналоги.

4.1 Визначення собівартості і ціни системи

Визначення виробничої собівартості спроектованого приладу здійснюється за питомою вагою у ньому окремих елементів витрат. У таблиці 4.1 наведені всі основні компоненти розширеної системи біометричної ідентифікації за відбитком пальця.

Таблиця 4.1

Елементи системи та їх вартість

Комплектуючі вироби	Кількість, шт.	Вартість за одиницю, грн.	Сума, грн.
Процесор (Atmega328)	1	74,325	74,325
Аудіо кодер/декодер (TLV320DAC3120)	1	20,125	20,125
Динамік (8 Ом, 2 Вт)	1	24	24
Роз’єм для навушників (3.5 мм)	1	5	5
Контролер сенсорного дисплею (TSC2003)	1	25,875	25,875
Резистивний сенсор (PX 0245)	1	160	160
Дисплей (LCD1602A)	1	63	63

Продовження таблиці 4.1

Контролер системи живлення (LP8900)	1	3,45	3,45
Роз'єм 2 конт.	1	2	2
Картка пам'яті (TS2GUSD)	1	45	45
Мікросхема для захисту від електростатичного струму (TPD3E001)	1	1,725	1,725
Сканер відбитків пальців	1	269	269
Порт USB 2.0	1	5	5
Кнопка	2	1	2
Регулятор напруги (5 В)	1	4	4
Конденсатор полярний (1 мкФ)	2	0,7	1,4
Конденсатор неполярний (1 мкФ)	1	0,4	0,4
Конденсатор неполярний (0,1 мкФ)	15	0,2	3
Продовження табл. 5.2			
Конденсатор неполярний (22 мкФ)	2	0,2	0,4
Конденсатор неполярний (10 мкФ)	6	0,2	1,2
Резистор змінного струму (25 КОм)	1	5,4	5,4
Резистор (34,8 КОм)	1	0,25	0,25
Резистор (9,76 КОм)	1	0,25	0,25
Резистор (1,2 КОм)	2	0,2	0,4
Резистор (50 КОм)	2	0,5	1
Резистор (10 КОм)	6	0,25	1
Резистор (100 Ом)	2	0,1	0,2
Світлодіод	2	0,3	0,6
Текстоліт двосторонній	1	5	5
Разом			525

Отже, $С_{вир2}$ = 100 / 65 * 525 = 807,7 (грн.);

Для визначення економічного ефекту в умовах виробництва знаходимо ціну спроектованого пристрою:

$$Ц_2 = 848,085 * (1 + 30 / 100) = 1102,5105 \text{ (грн.)};$$

Отже, економічний ефект у сфері виробництва становить:

$$Е_в = 2300 – 1102,5105 = 1197,4895 \text{ (грн.)}.$$

4.2 Визначення економічного ефекту в сфері експлуатації

$Ц_1$, $Ц_2$ – оптова ціна аналога та спроектованого приладу, грн.

$Е_а$ = 16,7 * 0,6 * (2300 – 1102,5105) / 100 = 119,9884479 (грн./рік);

Річний економічний ефект на витратах на енергію визначається:

$$E_{ен} = (M_1 – M_2) * T * a \quad (4.1)$$

де, M_1, M_2 – споживані потужності відповідно аналога та спроектованого приладу.

а = 0,9052 грн – тариф за 1 кВт/год;

Т = 264*8 – кількість робочих годин на рік (згідно з прийнятим бюджетом робочого часу на відповідний період);

$E_{ен}$ = (0,03 – 0,02) * 2112 * 0,9052 = 16,8 грн. /рік;

Річний економічний ефект по заробітній платі у нашому випадку :

$E_{зпл.}$ = 0, так як зарплата фахівця з обслуговування залишилася такою самою.

Оскільки конструкцією камери ремонт не передбачений, то Ер=0.

Сумарний річний економічний ефект визначається за формулою:

$E_{ер}$ = 119,9884479 + 16,8 = 136,7884479 (грн/рік);

Термін експлуатації пристрою становить 8 років. Річний $E_{ер}$ = 150,4657479 грн/рік. Тоді сумарний економічний ефект за термін експлуатації становить:

$E_е$ = 136,7884479 * 3,18547390056832 + 136,7884479 * 2,699554153024 + 136,7884479 * 2,2877577568 + 136,7884479 * 1,93877776 + 136,7884479 * 1,643032 + 136,7884479 * 1,3924 + 136,7884479 * 1,18 + 136,7884479 * 1 = 435,736030684699420710528 + 369,26782261415205144 96 + 312,93883272385767072 + 265,202400613438704 + 224,7477971300328 + 190,46423485596 + 161,410368522 + 136,7884479 = 2096,6 грн.

Загальний економічний ефект:

$$E_з = E_в + E_е = 1197,4895 + 2096,6 = 3294,0895 \text{ грн.}$$

За результатами проведених розрахунків було визначено економічні показники системи та доцільність її розробки. При порівнянні з наближеним аналогом проаналізовано різницю величин витрат та технологічні показники.

Згідно проведених обчислень, комплексний показник якості рівний 2,7421; ціна розробленої системи – 1102,5105 грн.; економічний ефект у сфері виробництва 1197,4895 грн.; загальний економічний ефект – 3294,0895 грн.

ВИСНОВКИ

В результаті виконання даної бакалаврської кваліфікаційної роботи виконано наступні завдання:

1. Проведено огляд та аналіз різних методів біометричної ідентифікації персони. Основну увагу зосереджено на біометричному методі відбитків пальців на основі папілярних ліній.

2. Розглянуто відомі аналоги пристроїв біометричної ідентифікації за відбитком пальця на визначено їхні основні переваги та недоліки. На основі цього визначено необхідні технічні характеристики проектованого пристрою.

3. Виконано вибір та обґрунтування апаратних засобів реалізації пристрою, вибрано оптичний сканер відбитків пальців FPM10A, мікропроцесорний комплект Arduino Uno та рідкокристалічний дисплей LCD1602A. А також вибрано середовище програмування мікропроцесорних пристроїв Adruino IDE.

4. Розроблено структурну схему пристрою, яка складається з основної та додаткової частини. Реалізовано готовий пристрій, який забезпечує сканування відбитку пальця людини, збереження його у базі даних та порівняння з існуючими при виконання процедури розпізнавання.

5. Розроблено програмне забезпечення пристрою ідентифікації персони за відбитком пальця та описано основну блок-схему функціонування пристрою.

6. Розроблено економічну оцінку готового пристрою та оцінку його експлуатації, які у порівнянні з аналогами є дешевшими.

Запропонований пристрій біометричної ідентифікації за відбитком пальця може використовуватись для реалізації різних технічних рішень, включаючи електронні дверні замки, системи запалювання двигунів внутрішнього згорання, тощо. Невеликі розміри пристрою та простота його реалізації, надають можливість для його інтеграції в різні системи чи інші прилади.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Царьов Р.Ю, Лемеха Т.М. Біометричні технології: навчальний посібник – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.
2. Кухарев Г.А. Биометрические системы: Методы и средства индентиф и-кации личности человека / Кухарев Г.А. – СПб .: Политехника, 2001.- 123с.
3. Голубев Г.А., Габриелян Б.А. Современное состояние и перспективы развития биометрических технологий. Нейрокомпьютеры. Разработка. Применение. № 10. 2004.- 40с.
4. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Москва: Радиотехника, 2004.-144 с.
5. Ландэ Д.В. О цифровой идентификация личности // Д.В. Ландэ, В.Н. Фурашев. – Харьков: НАКУ, 2007. – Вып. 34. – С. 127 – 135. Радиотехника, 2004.- 134 с.
6. Arduino Uno- Режим доступу: https://uk.wikipedia.org/wiki/Arduino_Uno - Дата доступу: 27.04.2020 р.
7. FPM10A- Режим доступу: https://ardushop.in.ua/arduino/fpm10a-fingerprint-recognition-module - Дата доступу: 29.04.2020 р.
8. Transcend- Режим доступу: https://ua.transcend-info.com/ - Дата доступу: 28.04.2020 р.
9. LCD1602A- Режим доступу: https://robotchip.ru/obzor-lcd-displeya-1602a/ - Дата доступу: 29.04.2020 р.
10. Arduino IDE- Режим доступу: https://www.arduino.cc/en/main/software - Дата доступу: 30.04.2020 р.
11. Економіка підприємства: Підручник / за заг. редакцією Й.М. Петровича.- Львів: “Магнолія плюс”, Видавець В.М. Піча– 2004.– 680 с.
12. О.О. Гетьман, В.М. Шаповал Економіка Підприємства : Навчальний посібник для студентів вищих навчальних закладів. – К: Центр навчальної літератури) 2006. – 488 с.

ДОДАТКИ

Додаток А.

Лістинг програми запису відбитків пальця

```
include <Adafruit_Fingerprint.h>
// On Leonardo/Micro or others with hardware serial, use those! #0 is green wire, #1 is white
// uncomment this line:
// #define mySerial Serial1
// For UNO and others without hardware serial, we must use software serial...
// pin #2 is IN from sensor (GREEN wire)
// pin #3 is OUT from arduino  (WHITE wire)
// comment these two lines if using hardware serial
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
uint8_t id;
void setup()
{
  Serial.begin(9600);
  while (!Serial);  // For Yun/Leo/Micro/Zero/...
  delay(100);
  Serial.println("\n\nAdafruit Fingerprint sensor enrollment");
  // set the data rate for the sensor serial port
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1) { delay(1); }
  }
}
uint8_t readnumber(void) {
  uint8_t num = 0;
  while (num == 0) {
    while (! Serial.available());
    num = Serial.parseInt();
  }
  return num;
}
void loop()                     // run over and over again
{
  Serial.println("Ready to enroll a fingerprint!");
  Serial.println("Please type in the ID # (from 1 to 127) you want to save this finger as...");
  id = readnumber();
  if (id == 0) {// ID #0 not allowed, try again!
     return;
  }
  Serial.print("Enrolling ID #");
  Serial.println(id);

  while (!  getFingerprintEnroll() );
}
```

```
uint8_t getFingerprintEnroll() {
  int p = -1;
  Serial.print("Waiting for valid finger to enroll as #"); Serial.println(id);
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println(".");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      break;
    default:
      Serial.println("Unknown error");
      break;
    }
  }
  // OK success!
  p = finger.image2Tz(1);
  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;
  }
  Serial.println("Remove finger");
  delay(2000);
  p = 0;
  while (p != FINGERPRINT_NOFINGER) {
    p = finger.getImage();
  }
  Serial.print("ID "); Serial.println(id);
```

```
p = -1;
Serial.println("Place same finger again");
while (p != FINGERPRINT_OK) {
  p = finger.getImage();
  switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image taken");
    break;
  case FINGERPRINT_NOFINGER:
    Serial.print(".");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    break;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Imaging error");
    break;
  default:
    Serial.println("Unknown error");
    break;
  }
}
// OK success!
p = finger.image2Tz(2);
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!
Serial.print("Creating model for #");  Serial.println(id);
p = finger.createModel();
if (p == FINGERPRINT_OK) {
  Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return p;
```

```
  } else if (p == FINGERPRINT_ENROLLMISMATCH) {
    Serial.println("Fingerprints did not match");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }
  Serial.print("ID "); Serial.println(id);
  p = finger.storeModel(id);
  if (p == FINGERPRINT_OK) {
    Serial.println("Stored!");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return p;
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not store in that location");
    return p;
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }
}
```

Додаток Б.

Лістинг коду програми, яка порівнює записані відбитки пальців

```
#include <Adafruit_Fingerprint.h>
// On Leonardo/Micro or others with hardware serial, use those! #0 is green wire, #1 is white
// uncomment this line:
// #define mySerial Serial1

// For UNO and others without hardware serial, we must use software serial...
// pin #2 is IN from sensor (GREEN wire)
// pin #3 is OUT from arduino  (WHITE wire)
// comment these two lines if using hardware serial
SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  while (!Serial);  // For Yun/Leo/Micro/Zero/...
  delay(100);
  Serial.println("\n\nAdafruit finger detect test");

  // set the data rate for the sensor serial port
  finger.begin(57600);
  delay(5);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1) { delay(1); }
  }

  finger.getTemplateCount();
  Serial.print("Sensor contains "); Serial.print(finger.templateCount); Serial.println(" templates");
  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);

  return finger.fingerID;
}

// 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!
  Serial.print("Found ID #"); Serial.print(finger.fingerID);
  Serial.print(" with confidence of "); Serial.println(finger.confidence);
  return finger.fingerID;
```

Додаток В.

Лістинг основного коду програми пристрою ідентитфікації

```
#include < LiquidCrystal.h>
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
int fingerprintID = 0;
String IDname;

void setup(){
  Serial.begin(9600);
  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  }
  else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1) { delay(1); }
  }

  Wire.begin();
  display.begin(SSD1306_SWITCHCAPVCC, 0x3C);
  displayMainScreen();
}

void loop(){
  displayMainScreen();
  fingerprintID = getFingerprintIDez();
  delay(50);
  if(fingerprintID == 1 || fingerprintID == 3 || fingerprintID == 4 || fingerprintID == 5){
    IDname = "Roman";
    displayUserGreeting(IDname);
  }
  else if(fingerprintID == 2){
    IDname = "Nazar";
    displayUserGreeting(IDname);
  }
}

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;

  Serial.print("Found ID #");
  Serial.print(finger.fingerID);
  Serial.print(" with confidence of ");
  Serial.println(finger.confidence);
  return finger.fingerID;
}

void displayMainScreen(){
  display.clearDisplay();
  display.setTextSize(1);
  display.setTextColor(WHITE);
  display.setCursor(7,5);
  display.println("Waiting fingerprint");
  display.setTextSize(1);
  display.setTextColor(WHITE);
  display.setCursor(52,20);
  display.println("...");
  display.display();
  delay(2000);
}

void displayUserGreeting(String Name){
  display.clearDisplay();
  display.setTextColor(WHITE);
  display.setTextSize(2);
  display.setCursor(0,0);
  display.print("Hello");
  display.setCursor(0,15);
  display.print(Name);
  display.display();
  delay(5000);
  fingerprintID = 0;
```