МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

С.В. Казмірчук

«_____»_____ 2020 р.

На правах рукопису
УДК 004.056.53

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Система розблокування електронного пристрою з дактилоскопічним захистом

Автор: О. С. Барсукова

Науковий керівник: к.т.н., доц. А.Б. Єлізаров

Нормоконтролер: к.т.н., доц. А.Б. Єлізаров

ВСТУП

Безпека завжди була надзвичайно важливою для людей у всьому світі. Завдяки сучасним технологіям змінився звичний спосіб зберігання та охорони речей, цінностей, цілих будинків. В даний час безпека включає широкий спектр програмного забезпечення, який включає веб-послуги безпеки, біометрію та персональні пристрої з рівнями безпеки.

Впровадження біометрії в безпеку стало одним із найбільших успіхів цифрово-технічної ери, оскільки певні унікальні характеристики людини можуть бути використані для ідентифікації цієї людини. Наприклад, жодна людиа не має абсолютно однакового голосу, ДНК або відбитків пальців. Коли принципи біометрії застосовуються до електронних пристроїв, результатом буде підвищена безпека. Однією з переваг розблокування електронних пристроїв біометричних пристроїв полягає в тому, що на відміну від традиційного розблокування електронного пристрою – він менш схильний до підбору ключа або копіювання. Другою основною перевагою є те, що при даному варіанту користувачу легше експлуатувати даний електронний пристрій, оскільки не треба запам’ятовувати дані для ідентифікації та автентифікації, усі необхідні «паролі» вже «під рукою».

Актуальним є дослідження стану захисту речей, які знаходяться під захистом електронного пристрою з дактилоскопічним захистом.

Постановка завдання Для розблокування електронного пристрою з дактилоскопічним захистом необхідно пройти ідентифікацію та автентифікацію через збіг відбитків пальців. Необхідно створити програмну реалізацію збігу відбитків пальців шаблону, який міститься у пам’яті сенсору відбитків пальців, та ймовірно правдивого відбитка пальця, що сканується сканером відбитків у поточний момент.

Мета – розробка системи розблокування електронного пристрою з дактилоскопічним захистом.

Для досягнення поставленої мети вирішуються такі **задачі:**

− дослідження відомих методів розблокування електронного пристрою з дактилоскопічним захистом;

− розробка алгоритму для систем розблокування електронного пристрою з дактилоскопічним захистом;

− розробка програмного забезпечення для систем розблокування електронного пристрою з дактилоскопічним захистом.

Галузь застосування. Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності електронних систем з дактилоскопічним захистом.

Об’єктом дослідження є система розблокування електронного пристрою з дактилоскопічним захистом.

Предметом дослідження є моделі систем розблокування електронних пристроїв з дактилоскопічним захистом.

Метод дослідження – це аналіз системи розблокування електронних пристроїв з дактилоскопічним захистом.

Наукова новизна одержаних результатів – дістали подальший розвиток системи розблокування електронних пристроїв з дактилоскопічним захистом, які відрізняються від існуючих застосуванням нової елементної бази, що спрямоване на зростання рівня захисту в електронних системах.

Практичне значення отриманих результатів - розроблено систему розблокування електронного пристрою з дактилоскопічним захистом.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

− Засіб захисту персональних даних від несанкціонованого доступу/ Барсукова О. С.//МАТЕРИАЛИ ЗА XVI МЕЖДУНАРОДНА НАУЧНА ПРАКТИЧНА КОНФЕРЕНЦИЯ ДИНАМИКАТА НА СЪВРЕМЕННАТА НАУКА – 2020, 15 – 22 ЮЛИ 2020. С. 72-74

− СИСТЕМА РОЗБЛОКУВАННЯ ЕЛЕКТРОННОГО ПРИСТРОЮ З ДАКТИЛОСКОПІЧНИМ ЗАХИСТОМ/ Барсукова О. С., канд. техн. наук

Єлізаров А. Б.// MATERIŁY XVI MIĘDZYNARODOWEJ NAUKOWIPRAKTYCZNEJ KONFERENCJI NAUKA I INOWACJA – 2020, 07 - 15 października 2020 roku, Przemyśl Nauka i studia 2020. c. 64-68

Розділ 1. Аналітичний розділ

1.1 Історія відбитків пальців

Сучасний світ кінематографу захоплює нашу уяву безліччю швидких та абсолютно надійних способів виявити усі сліди порушника на місці злочину та також швидко за цими слідами найти злочинця. Найменша краплинка поту, що впала з чола зловмисника, дрібніша волосинка або епітелій з-під нігтів жертви – усе це допомагає професіоналам на екранах встановлювати справедливість. Та існують більш прості та реальні технології, які допомагають розгадувати таємниці слідства. Однією із найдавнішою та досі актуальною технологією є порівняння відбитків пальців.

Та хоча ємності, які наповнені парами суперклею, допомагають надати практичний вигляд розслідуванню у фільмах, та що середній глядач кримінальних серіалів знає про відбитки пальців? Більш уважний розгляд технології відбитків пальців показує, що у даному випадку цікава не тільки сама технологія, а ще й історія створення. Крім того, розуміння історії відбитків пальців допомагає розібратися в концепції, яка в даний час керує появою нових біометричних технологій.

Історія відбитків пальців розпочалася задовго до його використання у кримінальному провадженні. На думку істориків , вавилоняни втискали пальці у мокру глину, щоб реєструвати ділові операції. Китайці адаптували цю систему, але дотримувались її переваг як унікального ідентифікатора, використовуючи чорнило на папері для ведення ділових операцій та ідентифікації своїх дітей. Навіть сотні років по тому ця практика все ще застосовувалася, коли в 1858 році англієць на ім'я сер Вільям Гершель, тоді головний магістрат округу Хуглі в Чунгіпурі, Індія, вимагав від мешканців реєструвати свої відбитки пальців при підписанні ділових документів.

Саме на цих засадах перша система відбитків пальців з’явилася в голові шотландського лікаря на ім’я Генрі Фолдс. Під час роботи в Японії лікар виявив відбитки пальців, залишені на старовинних шматках глини. У 1880 році Фолдс написав листа своєму двоюрідному братові Чарльзу Дарвіну з проханням про допомогу в розробці системи класифікації. У той час Дарвін відмовився, але переслав запит серу Френсісу Гальтону. Галтон на той час збирав велику кількість даних про фізичні характеристики людей, щоб визначити механіку успадкування генетичних ознак. Зібравши 8000 зразків відбитків пальців, Гальтон опублікував першу в історії систему класифікації відбитків пальців у своїй книзі “Відбитки пальців” протягом 1982 року. Система не побачила загальнонародного прийняття в той час, але її спадщина полягає в її дивовижному довголітті.

У той же час подібні ідеї мали й інші люди у всьому світі. На момент публікації "Відбитків пальців" француз на ім'я Альфонс Бертільон працював над власною системою, включаючи вимірювання рук, ніг та інших відмінних частин тіла. Ця практика, названа антропометрією, була прийнята британською поліцією Індії у 1890-х роках. В Аргентині поліцейський на ім'я Хуан Вучетіч розробив власну систему. Коли його запросили допомогти у розслідуванні вбивства двох хлопчиків у селі поблизу Буенос-Айреса, його система відіграла ключову роль. Порівнявши зразки з місця злочину, він ідентифікував вбивцю Франциску Рохас, матір хлопців. Вона зізналася у скоєному і народилася порівняльна дактилоскопія.

Лише в 1896 році з’явилася сучасна система ідентифікації відбитків пальців. Сер Едвард Генрі, комісар Лондонської столичної поліції, створив власну систему класифікації, використовуючи новаторські роботи Гальтона. Його система використовувала звичні звиви, петлі та арки фрикційних хребтів на кінчику пальця для ідентифікації осіб. Його система, система класифікації Генрі, замінила систему Bertillonage, і почалася сучасна дактилоскопія. Техніка була настільки успішною, що Скотланд-Ярд створив власне бюро відбитків пальців у 1901 р., вперше представивши докази відбитків пальців у суді в 1902 р.

У 1903 р. Система поширилася в тюрмах штату Нью-Йорк, ще більше закріпивши її використання як інструменту розслідування.

На жаль, система була громіздкою. Записи потрібно було порівнювати вручну, вимагаючи годин або днів, щоб отримати збіг, якщо він навіть був успішним. Японське національне поліцейське агентство відповіло на цю проблему появою комп'ютерів у 1980-х. Їхня система, що отримала назву Автоматизована система ідентифікації відбитків пальців (AFIS), дозволяла проводити перехресну перевірку мільйонів відбитків одночасно. Цифрова дактилоскопія наразі використовує ті самі ідентифікаційні характеристики системи Галтона та Генрі кінця XIX століття при визначенні відповідності.

Однак до 1999 року системи ідентифікації відбитків пальців могли «розмовляти» лише з іншими комп’ютерами в приватній мережі. Наприклад, якщо злочинця заарештували в штаті Юта, поліція Солт-Лейк мала можливість перехресно перевірити його записи з базами даних у Нью-Йорку. У відповідь на це Відділ інформаційних служб кримінального правосуддя ФБР представив інтегрований AFIS, що дозволяє здійснювати категоризацію, пошук та пошук відбитків пальців з будь-якої точки США всього за 30 хвилин. Крім того, система відображає історії кримінальних злочинів для осіб, що входять до системи. Приблизно 70 мільйонів записів знаходиться в IAFIS, в тому числі 34 мільйони цивільних відбитків. Ця сама система використовувалась для перевірки працевлаштування, видачі ліцензії та зарахування до програм соціальних служб, що робить її одним із найбільш використовуваних та найцінніших інструментів у світі.

Ця сама концепція використання справді унікальних ідентифікаторів у кримінальному розслідуванні викликала хвилю інших "відбитків пальців", які називаються біометрією. Ці технології дозволяють більш ретельно ідентифікувати потенційних підозрюваних з ще більшою точністю. У Квантіко, штат Вірджинія, Аудіолабораторія ФБР допомагає ідентифікувати відбитки пальців основних міжнародних злочинців. Вшановуючи систему Альфонса Бертільйона, сканування вух, яке вивчає чіткий розмір, форму та структуру вух,

також бачить застосування. Але найглибшим, звичайно, є відбиток ДНК, який розглядає хімічний код, який створює нас, щоб відрізнити одну людину від іншої.

Але відбитки пальців не зникають. З підвищенням рівня хакерів у зломі паролів на основі символів, відбитки пальців, серед інших біометричних даних, спостерігають все більше використання в споживчих продуктах. Зокрема, новий багато смартфоні було випущено з можливістю сканування відбитків пальців , намагаючись запропонувати більш безпечну альтернативу звичайним методам автентифікації.

І хоча дактилоскопія - це не ракетна наука, її послідовність, повсюдність та розвиток не залишають сумнівів щодо її важливості для цілей розслідування. Від скромного початку древньовавилонянської ділової практики до сканерів, вбудованих у наші мобільні пристрої, очевидно, що відбитки пальців наклали свій відбиток на наше суспільство.

1.2 Переваги та недоліки біометричної ідентифікації

Біометричні технології набувають все більшої популярності з кожним днем у всьому світі. Біометричні дані широко використовуються багатьма державними установами, транснаціональними організаціями, установами, банками та лікарнями. Біометричні технології зростають у кожному секторі, включаючи фінанси, банківську діяльність, робочі професії, кордони та для національної ідентичності. Дослідження свідчать, що люди більше вірять у сучасні біометричні технології, а не в традиційні системи безпеки. Отже, які особливі переваги та недоліки біометрії?

1.2.1 Переваги біометричної ідентифікації

Безпечність. Раніше у нас були паролі з цифрами, алфавітами, символами тощо, які з кожним днем стає легко зламати. Щороку трапляються мільйони випадків хакерства, і люди постійно втрачають свої гроші. Біометрична технологія пропонує різні типи рішень, які практично неможливо зламати, на відміну від паролів. Це велика допомога для нас, особливо для власників підприємств, які тривалий час борються з проблемами безпеки.

Точність. Традиційні системи безпеки регулярно виходять з ладу, що коштує нам великої кількості часу, грошей та ресурсів. Найпоширенішими системами безпеки є паролі, персональні ідентифікаційні номери (PIN-коди) та смарт-картки, які не завжди є точними. Однак біометричний метод працює з вашими фізичними рисами, такими як відбитки пальців, долоні, сітківка та інші, які завжди допоможуть вам точно в будь-якому місці та в будь-який час.

Підзвітність. В інших методах перевірки будь-хто може використовувати ваш пароль або номер безпеки для зламу вашої особистої інформації, що є дуже ризикованим, і люди постійно страждають від цієї проблеми. Але у випадку біометричної безпеки зловмиснику потрібна пряма взаємодія з жертвою, щоб увійти в систему або пройти систему безпеки, яка дозволяє на 100% підзвітувати за всю вашу діяльність.

Зручність. Уявіть собі усі ті моменти, коли ви забували свої паролі, досить нервово, так? Всі пройшли цей процес, коли важко запам’ятати або записати кожен пароль, і ми, швидше за все, забудемо його в деяких неприємних ситуаціях. Існує кілька зручних інструментів, які можуть виконати цю роботу за вас, але жоден з них не може перевершити біометричні данф, що є найзручнішим рішенням. Ваші дані залишаються з вами назавжди, тому вам не потрібно нічого запам’ятовувати чи записувати.

Масштабованість. На відміну від інших рішень, біометрія є масштабованим рішенням для всіх типів проектів. Біометричні технології використовуються в багатьох державних проектах, системах банківської безпеки, управлінні робочою силою тощо. Це можливо завдяки масштабованості її рішень.

Рентабельність інвестицій. Біометричні рішення забезпечать вам найкращу рентабельність інвестицій порівняно з іншими системами безпеки. Ви можете відстежувати тисячі працівників великої компанії лише за допомогою одного біометричного пристрою та програмного забезпечення. З іншого боку, вам потрібно було б керувати величезним ресурсом, щоб виконати ту саму роботу, яка коштувала б вам більше часу та грошей, ніж відповідне біометричне рішення.

Гнучкість. Безумовно, біометричні системи є найбільш гнучким рішенням безпеки. У вас є власні дані безпеки, тому вам не потрібно турбуватись запам’ятовувати незграбні алфавіти, цифри та символи, необхідні для створення складного пароля.

Довірливість. Звіти стверджують, що молоді покоління більше довіряють біометричним рішенням, ніж іншим рішенням. Банки вже почали використовувати біометричні системи безпеки для підвищення безпеки та надійності своїх клієнтів.

Економія часу. Біометричні технології економлять час. У більшості випадків вам просто потрібно покласти палець на пристрій або подивитися на пристрій оком, щоб пройти систему. З іншого боку, традиційні методи дістають більше клопоту, що стає надокучливим та нестерпним.

Економія грошей. Уряди вкладають гроші на створення національної біометричної бази даних, щоб урядові послуги могли надаватися населенню з більшою точністю та меншими витратами. Корпорації застосовують біометричну систему для отримання точної інформації, яка економить і час, і гроші. За невеликі гроші будь-яка компанія може відстежувати своїх співробітників і зменшувати додаткові витрати, які вони платять роками.

Це вік інформаційних технологій. Наші традиційні системи безпеки з кожним днем будуть застарілими. Ми маємо застосувати новітні технології, щоб підвищити нашу безпеку та розпочати крадіжок. Розвинені країни, включаючи США, Великобританію, Австралію, Канаду тощо, знають переваги біометрії і вже впровадили цю технологію на багатьох етапах надання державних послуг і

продовжують адаптуватися для створення більш біометрично безпечного майбутнього.

1.2.2 Недоліки біометричної ідентифікації

Технології побудовані для покращення якості нашого життя. Це приносить поліпшення у житті в усіх аспектах. Біометрична технологія також є чудовим винаходом, яка вносить суттєві зміни в наш спосіб життя. Як вже говорилося, з великими можливостями приходить ще більша відповідальність, біометричні технології є гарним прикладом цієї цитати. З усіма привілеями біометрії, у неї також є своя темна сторона. Ми дуже мало знаємо про недоліки біометрії порівняно з її загальновідомими перевагами.

Хоча впровадження біометрії приносить багато переваг, на жаль, воно також має свої проблеми.

Фізичні риси не змінюються. Більшість біометричних методів працюють з такими фізичними рисами, як відбитки пальців, райдужна оболонка, вени долоні тощо. У всіх нас є лише пара очей; певна кількість відбитків пальців та інші незмінні частини тіла. Ми можемо скинути пароль, але ніколи не можемо змінити свої відбитки пальців або сітківки ока. Наші біометричні дані зберігаються у відповідних державних базах даних або компаніях, які надають такі послуги.

Чи можуть вони гарантувати, що ці дані ніколи не будуть зламані або викрадені з сервера? На жаль, це вже відбувається навколо нас. Є новини про порушення даних мільярдів приватних даних індіанців з бази даних Aadhaar. Масштабне порушення відбулося у Федеральному урядовому управлінні особистого управління в США, де в 2015 році було викрадено 5,6 мільйона відбитків пальців працівників. Ви можете змінити свій пароль, якщо його вкрадуть, але у вас немає можливості змінити свій відбиток пальця.

Частота помилок. Біометричні машини менш досконалі, і тут можуть траплятися помилки. Зазвичай біометричні пристрої допускають два типи

помилок: коефіцієнт помилкового прийняття (FAR) та коефіцієнт помилкового відхилення (FRR). Коли пристрій приймає несанкціоновану особу, це називається FAR, а коли відхиляє уповноважену особу - FRR.

Рівень помилок у деяких випадках настільки високий, що створює великий хаос для всієї системи безпеки. Це може статися через погоду, фізичний стан, вік та інші проблеми.

Вартість. Вартість біометричних пристроїв порівняно вище, ніж у інших традиційних пристроїв безпеки. Витрати на біометричне програмне забезпечення, пристрої, програмісти, сервер та інше відносне обладнання в сукупності становлять великі гроші.

Затримка. Деякі біометричні прилади займають більше часу, ніж прийнято, і довга черга робітників чекає на реєстрацію у великих компаніях. У цих випадках люди втрачає свій дорогоцінний час при скануванні біометричним пристроєм щодня. Людині важко, коли їй щодня доводиться проходити систему біометричної перевірки перед входом до школи, офісу чи інших місць.

Складність. Одним з найбільших недоліків біометрії є надзвичайно технічна та складна система, що становить весь процес. Для розробки системи компанії наймають досвідчених та кваліфікованих програмістів, тому для її роботи потрібні програмісти.

Негігієнічність. Існують різні типи біометричних методів. Деякі з них засновані на контактах, такі як сканер відбитків пальців і долоні; деякі з них є безконтактними, як райдужна оболонка, розпізнавання обличчя і т. д. У контактних засадах біометричний прилад використовується мільйони разів величезною кількістю людей.

Усі фактично діляться своїми мікробами між собою за допомогою пристрою. Ви ніколи не знаєте, що берете з собою, поклавши палець на пристрій.

Складність сканування. Деякі біометричні методи, такі як сканування райдужної оболонки, можуть зазнати труднощів при скануванні. Це відбувається з кількох причин, включаючи вії, повіки, кришталик та відбиття на рогівці. З цих

причин сканування райдужної оболонки ока може бути не таким надійним для використання.

Фізична вада. Деякі люди могли втратити або пошкодити частини тіла, такі як пальці чи очі у різних життєвих обставинах. У цьому випадку пристрій для розпізнавання відбитків пальців/райдужної оболонки ока буде незручним і просто образливим

Середовище використання. Навколишнє середовище та використання можуть вплинути на загальні вимірювання. Особливо в дуже холодних районах рівень помилок вищий, що створює непотрібний хаос і розчарування у всій системі.

Додаткова інтеграція обладнання. Деякі біометричні методи потребують додаткової інтеграції обладнання, яка є дорогою, незручною та складною.

1.3 Правове регулювання біометричної верифікації та ідентифікації в Україні

Правове регулювання національної системи біометричної верифікації та ідентифікації забезпечуються за допомогою Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Дане *«…Положення регулює порядок впровадження та функціонування національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства (далі - національна система), а також визначає її структуру та призначення.»* [1].

Цим Положенням також визначаються правила та алгоритми обробки персональних даних у національній системі біометричної верифікації та ідентифікації, визначаються суб’єкти національної системи біометричної верифікації та ідентифікації , порядок розміщення програмно-технічних комплексів даної системи, функціонування системи.

Центр обробки даних національної системи забезпечує:

1. Обробку наборів даних з відомчих інформаційних систем суб'єктів національної системи через прикладні програмні інтерфейси електронної взаємодії;
2. Управління біометричною верифікацією та ідентифікацією осіб;
3. Верифікацію та ідентифікацію особи за біометричними даними (параметрами) особи шляхом використання баз даних біометричних шаблонів;
4. Запобігання дуплікації біометричних даних (параметрів);
5. Інформаційну взаємодію суб'єктів національної системи із зовнішніми інформаційними системами за допомогою прикладного програмного інтерфейсу.

Взаємодія суб'єктів національної системи здійснюється Для біометричної ідентифікації особи у формі запитів та відповідей у вигляді наборів даних, які можуть містити інформацію про:

1. Прізвище, ім’я, по батькові (за наявності);
2. Дату народження;
3. Стать;
4. Місце народження;
5. Паспортний документ та його електронний вигляд;
6. Біометричні дані (параметри);
7. Перетин державного кордону;
8. Інші відомості;

Законодавчі документи, які допомагають у функціонуванні національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства:

- Конституція України;
- Закон України «Про захист персональних даних»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про електронний цифровий підпис»;

- Закон України «Про правовий статус іноземців та осіб без громадянства»;
- Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
- Проект Закону України «Про ідентифікацію людини шляхом дактилоскопії»

Функціонування національної системи забезпечує ДМС, яка є розпорядником. Адміністратором національної системи є адміністратор Єдиного державного демографічного реєстру.

Розглянемо більш детально проект Закону України «Про ідентифікацію людини шляхом дактилоскопії»

1.3.1 Проект Закону України «Про ідентифікацію людини шляхом дактилоскопії»

Закон України "Про ідентифікацію людини шляхом дактилоскопії"[2] міг визначати *«…порядок ідентифікації особи шляхом отримання інформації про особливості візерунків її шкіри на окремих частинах тіла. Особливості використання дактилоскопічної інформації та збереження її конфіденційності.»*. Даний Проект Закону України був одержаний Верховною Радою України18.01.2012 та на сьогоднішній момент не був прийнятий.

Проект цього Закону визначає такі ключові статті: *«…Стаття 6. Особи, по відношенню до яких обов'язково застосовується дактилоскопія*

Дактилоскопія є обов'язковою для таких категорій осіб:

1) іноземців, які звернулися за наданням притулку або статусу біженців в Україні;

2) іноземців, які незаконно перетнули державний кордон та (або) незаконно перебувають на території України;

3) осіб, які через стан здоров'я або за віком не в змозі повідомити особисті дані;

4) осіб, для яких встановити зазначені дані іншим чином неможливо;

5) осіб, які виявили бажання обіймати посади в органах державної влади та/або місцевого самоврядування;

6) осіб, які підозрюються в скоєнні злочину, звинувачені за скоєння злочину або засуджені за скоєння злочину;

7) бездомних громадян, безпритульних дітей, дітей-сиріт та дітей, позбавлених батьківського піклування; осіб, підозрюваних в бродяжництві;

8) підданих адміністративному арешту та інших осіб, якщо це прямо передбачено Законом.

Стаття 8. Порядок проведення дактилоскопії

Дактилоскопія проводиться шляхом збирання відбитків усіх пальців рук. Якщо отримати інформацію про особливості візерунків пальців рук неможливо, проводиться дактилоскопія долонь рук, губ, ступень ніг або пальців ніг за вибором особи, щодо якої проводиться дактилоскопія.

Стаття 13. Використання дактилоскопічної інформації

Використання дактилоскопічної інформації здійснюється за умови збереження її конфіденційності для сторонніх осіб та у випадках, прямо передбачених законом, зокрема:

1) ідентифікації людини, яка через стан свого здоров'я чи за віком не в змозі повідомити дані про свою особу;

2) з метою розкриття, розслідування, попередження злочинів;

3) підтвердження особи;

4) розшуку людей, які зникли безвісти;

5) дактилоскопічної перевірки та в інших випадках, передбачених законом…»

1.4 Міжнародні спільноти

1.4.1 Європейський Союз

Найбільш відомим стандартом в Європі є Директива 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних» від 24.10.1995, яка використовувалась до GDPR (The General Data Protection Regulation, 2016/Загальний регламент щодо захисту даних для європейських держав-членів), який вступив в силу з 25.05.2018. Організації, що не входять в Європейський Союз, підпадають під дію GDPR при обробці персональних даних суб'єктів даних ЄС. Фактично, це робить GDPR глобальним законом.

GDPR (параграф 1 стаття 9) визначає біометричні дані як «конфіденційну» категорію особистої інформації, забезпечуючи надійний захист. GDPR визначає біометричні дані досить широко, у багатьох випадках вимагаючи оцінки впливу на конфіденційність для обробки і дозволяючи державам-членам реалізовувати різні варіанти захисту біометричних даних.

На відміну від Директиви, GDPR спеціально визнає біометричні дані як підмножину конфіденційних особистих даних, які вважаються «конфіденційної категорією особистих даних». Зокрема, GDPR визначає біометричні дані як «особисті дані, отримані в результаті конкретної технічної обробки, що відноситься до фізичних, фізіологічних або поведінкових характеристик людини, які підтверджують унікальну ідентифікацію цієї людини, наприклад зображення обличчя, зображення сітківки ока особи або відбитки пальців».

В цілому GDPR встановив дві категорії біометричних даних. По-перше, інформація про фізичні характеристики (фізичні або фізіологічні характеристики людини: обличчя, відбитки пальців, сітківка ока і т. і.). По-друге, інформація, що відноситься до поведінки людини (будь-які унікальні характеристики людської

поведінки, що дозволяють ідентифікувати особу). На жаль, в правилах немає уточнення.

Важливим здобутком GDPR є те, що суб'єкт даних має право відкликати свою згоду в будь-який час, тобто має право бути забутим. Швидкий розвиток біометричних технологій, неузгодженість, пов'язана з обробкою біометричних даних GDPR, а також можливе розбіжність підходів держав-членів Європейського Союзу до біометричних даних зажадають більшої уваги і обережності з боку контролерів даних.

Варто зазначити, що у 2019 році Європарламент схвалив створення однієї з найбільших біометричних баз даних в світі. Нова база даних буде називатися Common Identity Repository (CIR) та буде призначена для об'єднання записів більше 350 мільйонів чоловік.

1.4.2 Сполучені Штати Америки

У США немає єдиного загальнонаціонального федерального закону, що регулює біометричні дані. Однак, окрім Директив Президента існує досить велика кількість законів, які регулюють правові норми в США:

- Закон «Про захист конфіденційності відеоматеріалів» (The Video Privacy Protection Act, 1980);
- Закон «Про конфіденційність» (The Privacy Act, 1974);
- Закон «Про надання кредитної інформації про покупця» (The Fair Credit Reporting Act, 1970);
- Закон «Про право на фінансову приватність» (The Rightto Financial Privacy Act, 1978);
- Закон «Про свободу інформації» (The Freedom of Information Act, 1996);

- BIPA (Biometric Information Privacy Act, passed by Illinoys (2008), Texas, Washington, Michigan, New Hampshire, Alaska, Montana) — найсуворіший у США закон, який вимагає, щоб люди та організації обробляли біометричні дані, як і всі персональні дані, із заходами безпеки, відповідними шкоді, яку може заподіяти втрата цих даних;
- CCPA (California Consumer Privacy Act, 2018/Каліфорнійський закон про конфіденційність споживачів) набуває чинності 01.01.2020 р.

Станом на червень 2019 року в 47 штатах (за винятком штатів BIPA, де комерційне використання заборонено) законно використовувати програмне забезпечення для ідентифікації осіб з використанням зображень, зроблених без її згоди в громадських місцях.

CCPA часто є потенційною моделлю закону США про конфіденційність даних. Фактично, з точки зору впливу CCPA може стати другим GDPR. Однак цей закон розширює права жителів Каліфорнії на недоторканність приватного життя і захист споживачів. Можна сказати, що інтерпретація біометричних даних CCPA ширше, ніж GDPR. Це «фізіологічні, біологічні та поведінкові характеристики людини, включаючи його ДНК, які можуть використовуватися окремо або в поєднанні один з одним або з іншими ідентифікаційними даними для ідентифікації людини».

Коротше кажучи, права, надані CCPA споживачам в Каліфорнії для захисту їх особистої інформації і біометричних даних, пов'язані з можливістю видалення отриманих даних (право на забуття); доступ до даних (право на розкриття або доступ); збір даних (можливість передачі даних, т. е. дані повинні бути отримані в зручному форматі); вимоги до компанії не продавати свою особисту інформацію; відмова від участі («Угода» - це основний стандарт згоди, дозволений європейським GDPR); застосування позову (застосування штрафних санкцій).

Варто відзначити ряд нормативних актів в Сан-Франциско (Каліфорнія, травень 2019 г.), Сомервіллі (Массачусетс, червень 2019 г.), Окленді

(Каліфорнія, 2019 г.), згідно з якими міста вирішили заборонити використання технологій розпізнавання особами, в тому числі поліцією.

Треба ще згадати, що найбільша біометрична база даних в світі - в Індії (найбільша в світі біометрична база даних включає більше 90% населення, а біометрія використовується повсюдно) - UIDAI (Unique Identification Authority of India). Унікальний особистий номер, присвоєний системою, називається AADHHAAR.

1.5 Методи біометричної ідентифікації

Біометрична перевірка - це будь-який засіб, за допомогою якого особа може бути однозначно ідентифікована шляхом оцінки однієї або кількох відмінних біологічних ознак. Унікальні ідентифікатори включають відбитки пальців, геометрію рук, геометрію мочки вуха, візерунки сітківки та райдужки, голосові хвилі, ДНК та підписи[3].

Найдавнішою формою біометричної перевірки є дактилоскопія. Історики знайшли приклади відбитків великих пальців, які використовувались як засіб унікальної ідентифікації на глиняних печатках у Стародавньому Китаї. Біометрична перевірка значно просунулася з появою комп’ютеризованих баз даних та оцифрування аналогових даних, що дозволяє проводити майже миттєву особисту ідентифікацію.

Методи автентифікації за шаблоном ірису та за допомогою сітківки вже застосовуються в деяких банківських автоматичних касах. Розпізнавання форми голосової хвилі, метод верифікації, який використовується протягом багатьох років із записом магнітофонних стрічок у телефонних підслуховуваннях, зараз використовується для доступу до власних банків даних у науково-дослідних установах. Технологія розпізнавання обличчя була використана правоохоронними органами, щоб зі значною надійністю вибирати людей у великих натовпах. Геометрія рук використовується в промисловості для забезпечення фізичного доступу до будівель. Геометрія мочки вуха була

використана для спростування особистості людей, які заявляють, що є кимось, ким вони не є (крадіжка особистості). Порівняння підписів не настільки надійне, саме по собі, як інші біометричні методи перевірки, але пропонує додатковий рівень перевірки, коли використовується разом з одним або кількома іншими методами.

Незалежно від того, яка біометрична методологія використовується, процес перевірки ідентифікації залишається незмінним. Запис унікальної характеристики людини фіксується та зберігається у базі даних. Пізніше, коли потрібна перевірка ідентифікації, новий запис фіксується та порівнюється з попереднім записом у базі даних. Якщо дані в новому записі збігаються з даними у записі бази даних, особа підтверджується.

Розрізняють фізіологічні та поведінкові методи ідентифікації особистості. Фізіологічна біометрія в основному включає розпізнавання обличчя, відбитків пальців, геометрію рук, розпізнавання райдужки та ДНК. Тоді як поведінкова біометрія включає натискання клавіш, підпис та розпізнавання голосу[4].

Біометрична ідентифікація особистості найбільш розповсюджена у варіантах, представлених нижче:

1. Розпізнавання відбитків пальців
2. Розпізнавання обличчя
3. Розпізнавання райдужки ока
4. Розпізнавання голосу
5. Розпізнавання підписів

1.5.1 Розпізнавання відбитків пальців

Розпізнавання відбитків пальців включає зйомку відбитків пальців людини та записує такі її особливості, як дуги, звивини та петлі (Основні типи відбитків пальців представлені на рис. 1.1), а також контури країв, дрібниць та борозд. Відповідність відбитків пальців можна досягти трьома способами, такими як дрібниці, кореляція та хребет.

Збіг відбитків пальців на основі Minutiae зберігає площину, що включає набір точок, і набір точок відповідає шаблону та деталям в / п.

Відповідність відбитків пальців на основі кореляції накладає два зображення відбитків пальців і обчислюється зв'язок між еквівалентними пікселями.

Зіставлення відбитків пальців на основі риджів - це інноваційний метод, який фіксує хребти, оскільки зйомка відбитків пальців на основі дрібниць є важкою за низької якості.

Для збору відбитків пальців у сучасних методах використовуються оптичні датчики, які використовують CMOS-датчик зображення або CCD; твердотільні датчики працюють за принципом технології перетворювачів, використовуючи теплові, ємнісні, п'єзоелектричні датчики або електричне поле; або ультразвукові датчики працюють на ехографії, в якій датчик передає акустичні сигнали через передавач біля пальця і фіксує сигнали в приймачі. Сканування відбитків пальців є дуже стабільним і надійним. Це захищає вхідні пристрої для побудови дверних замків та доступу до комп'ютерної мережі стають все більш взаємними. В даний час невелика кількість банків ініціювала використання зчитувачів відбитків пальців для затвердження в банкоматах.

Рис. 1.1. Основні типи відбитків пальців

1.5.2 Розпізнавання обличчя

Система розпізнавання обличчя[5] - це один із типів біометричних комп'ютерних додатків, який може ідентифікувати або перевірити людину за цифровим зображенням шляхом порівняння та аналізу шаблонів. Ці біометричні системи використовуються в системах безпеки . Сучасні системи розпізнавання обличчя працюють із відбитками обличчя, і ці системи можуть розпізнавати 80 вузлових точок на обличчі людини. Вузлові точки - це не що інше, як кінцеві точки, що використовуються для вимірювання змінних на обличчі людини, що включає довжину та ширину носа, форму вилиць та глибину очниці. Вузлові точки обличчя представлені на рис. 1.2.

Системи розпізнавання обличчя працюють шляхом збору даних для вузлових точок на цифровому зображенні обличчя людини, і отримані дані можуть зберігатися як відбиток обличчя. Коли умови сприятливі, ці системи використовують відбитки обличчя для точної ідентифікації. В даний час ці системи орієнтовані на програми для смартфонів, які включають особистий маркетинг, соціальні мережі та теги зображень. Соціальні сайти, такі як FB, використовують програмне забезпечення для розпізнавання облич для позначення користувачів на фотографіях. Це програмне забезпечення також збільшує персоналізацію маркетингу. Наприклад, білборди розроблені з інтегрованим програмним забезпеченням, яке розпізнає етнічну приналежність, стать та передбачуваний вік тих, хто спостерігає, для забезпечення цільового маркетингу.

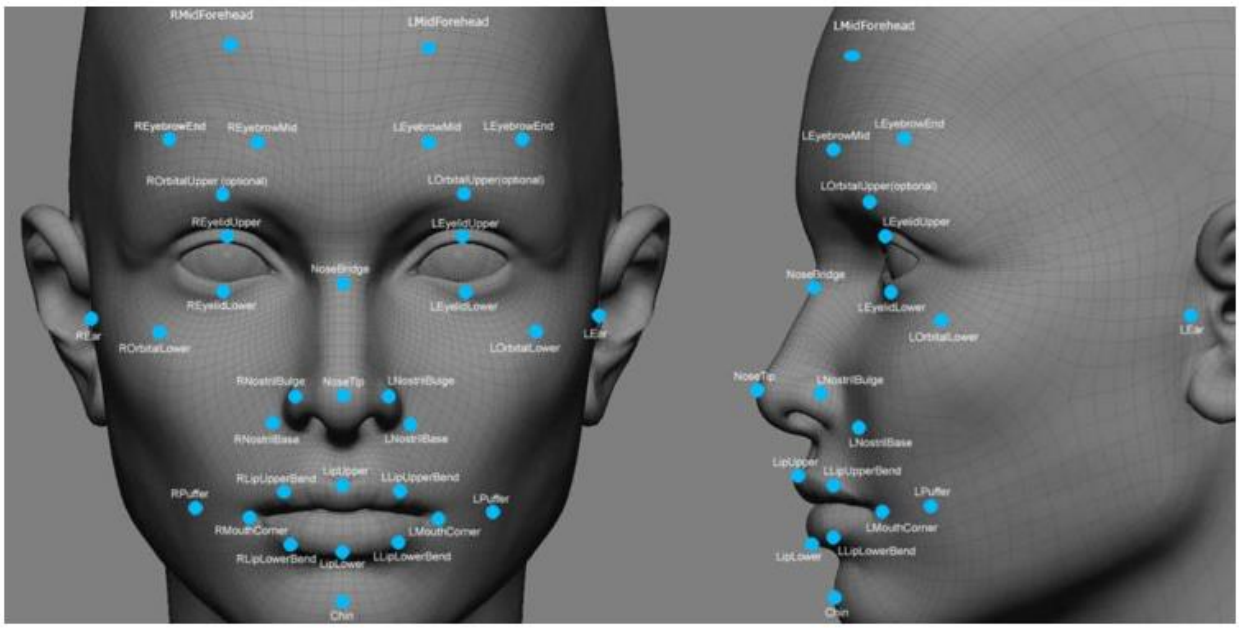

Рис. 1.2. Вузлові точки на обличчі

1.5.3 Розпізнавання райдужки ока

Розпізнавання райдужки - це один із видів біометричних методів, що використовується для ідентифікації людей на основі одинарних візерунків в області кільцеподібної оточеної зіниці ока. Як правило, райдужка має синій, коричневий, сірий або зелений колір зі складними візерунками, які помітні при уважному огляді. Принцип розпізнавання райдужки ока представлений на рис. 1.4.

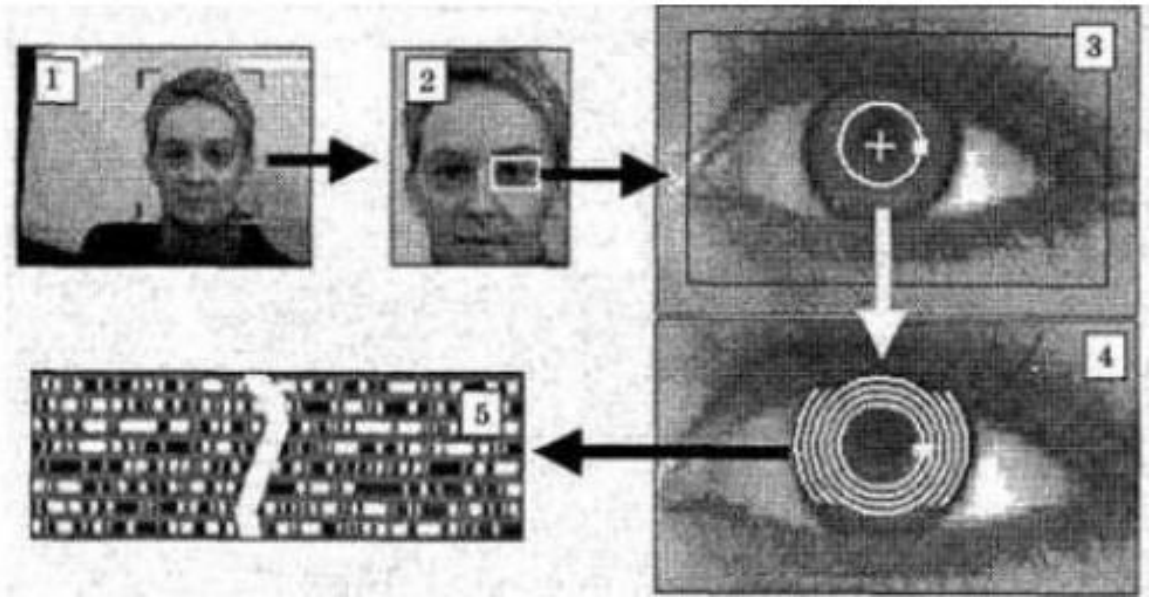

Рис. 1.3. Принцип розпізнавання райдужки ока

1.5.4 Розпізнавання голосу

Технологія розпізнавання голосу використовується для створення мовленнєвих зразків шляхом поєднання поведінкових та фізіологічних факторів, які можна вловити за допомогою обробки мовної технології. Найважливішими властивостями, що використовуються для аутентифікації мови, є носовий тонус, основна частота, перегин, каденція. Розпізнавання голосу можна розділити на різні категорії залежно від типу домену автентифікації, наприклад методу фіксованого тексту, методу, залежного від тексту, методу, незалежного від тексту, та техніки розмови. Алгоритм розпізнавання голосу представлений на рис. 1.4.

Рис. 1.4. Алгоритм розпізнавання голосу

1.5.5 Розпізнавання підписів

Розпізнавання підпису - це один із видів біометричного методу, який використовується для аналізу та вимірювання фізичної активності підпису, як тиск, що застосовується, порядок удару та швидкість, нахил, орієнтація відносно поверхні. Дані принципи представлені на рис. 1.5. Деякі біометричні дані використовуються для порівняння візуальних зображень підписів. Розпізнавання

підписів може виконуватися двома різними способами, наприклад, статичним та динамічним.

У статичному режимі споживачі пишуть свій підпис на папері, оцифровують його за допомогою камери або оптичного сканера. Ця система визначає підпис, що перевіряє його форму.

У динамічному режимі споживачі пишуть свій підпис на планшеті, який отримує підпис у режимі реального часу. Інший варіант – зробити підпис за допомогою стилусових КПК. Деякі біометричні дані також працюють зі смартфонами з ємнісним екраном, де споживачі можуть підписуватись за допомогою пера або пальця. Цей тип розпізнавання також відомий як "он-лайн".

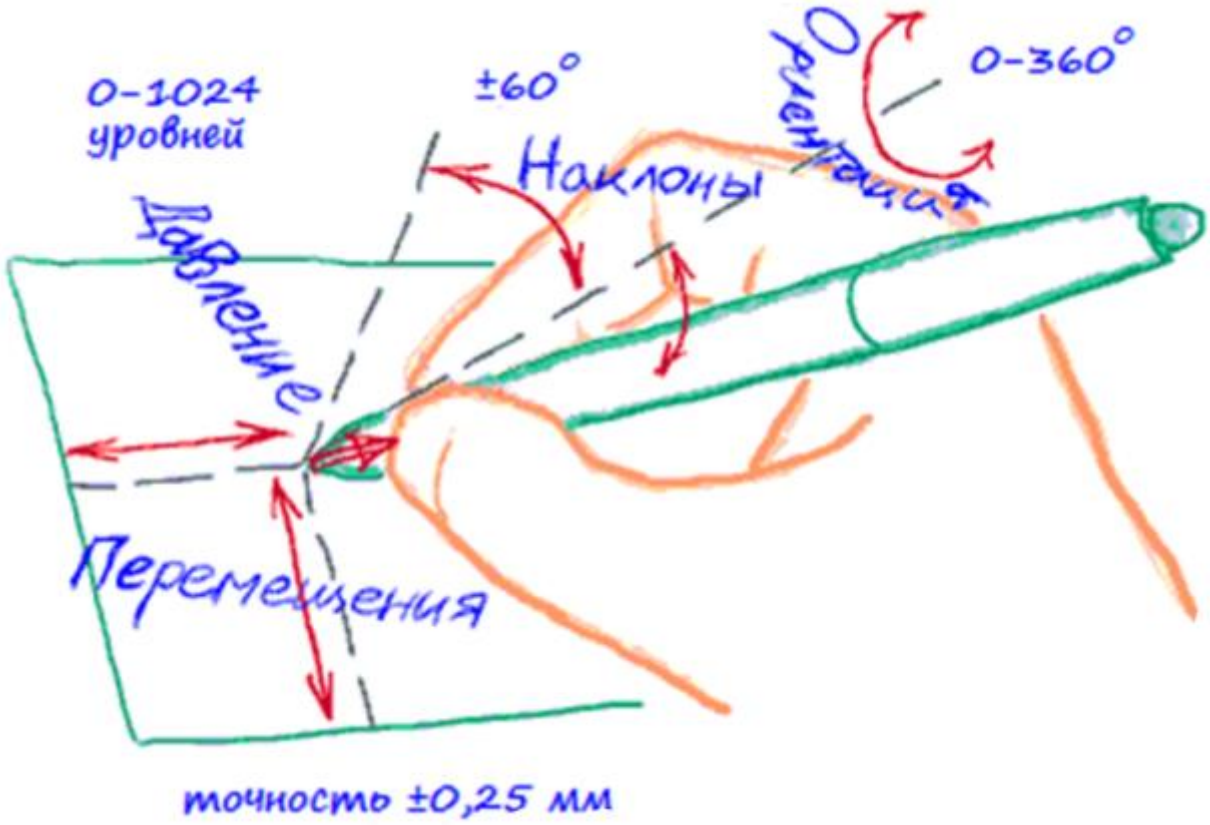

Рис. 1.5. Принципи фізичної активності підпису

1.5.6 Обрання методу біометричної ідентифікації

При обранні методу біометричної ідентифікації слід зважати не тільки на те, які суттєві відмінності між методами біометричної ідентифікації, а на

загальне розпосюдження методу зчитування, дороговартість процесу пошуку збігу, кількість даних у базі перевірки. За даними критеріями було обрано метод зчитування відбитків пальців, оскільки даний метод дешевше, порівняно з іншими методами та доступніший для встановлення перевірок на збіг відбитків пальців в побутових ситуаціях.

1.6 Види сканерів відбитків пальців

Сканер відбитків пальців є типом електронної системи безпеки , яка використовує відбитки пальців для біометричної автентифікації для надавання користувачу доступ до інформації[6].

Раніше сканери відбитків пальців переважно бачили у фільмах та телешоу або читали про них у науково-фантастичних романах[7]. Але такі часи давно минули - сканери відбитків пальців використовувались десятки років. Сканери відбитків пальців не тільки стають більш звичним явищем для новітніх мобільних пристроїв, але вони поступово просуваються у повсякденне життя[8]. Сканери відбитків пальців працюють, фіксуючи малюнок хребтів і долин на пальці. Потім інформація обробляється програмним забезпеченням для аналізу шаблонів пристрою , яке порівнює її зі списком зареєстрованих відбитків пальців у файлі. Успішне збіг означає, що особу підтверджено, тим самим надаючи доступ. Спосіб збору даних відбитків пальців залежить від типу використовуваного сканера[9].

1.6.1 Ємнісні сканери відбитків пальців

Ємнісні сканери відбитків пальців[10] - це тип, який в основному використовується в смартфонах. Вони працюють за принципом, що якщо відстань досить мала, можна передавати електроенергію від конденсатора і шкіри.

У масштабі таких конденсаторів гребені відбитків пальців схожі на пагорби та долини. Хребти будуть здаватися ближчими до конденсатора, і більше електроенергії буде стікати. Якщо у вас є масив або сітка конденсаторів (чим більше, тим вище роздільна здатність), вони можуть діяти як пікселі з різною інтенсивністю рівня сірого (більший потік електроенергії, темніший піксель), утворюючи таким чином 2D-зображення відбитка пальця.

Це просто, дуже міцно і працює лише зі шкірою. Це не можна обдурити аркушем паперу, і якщо ви намагаєтеся виготовити форму справжнього відбитка пальця, вам потрібно знайти матеріал, який має таку ж провідність, як шкіра. Не неможливо, але досить незручно, щоб відсіяти більшість зловмисників.

Недоліком ємнісних зчитувачів відбитків пальців є те, що вони не можуть працювати, якщо палець не чистий або на ньому є вода / піт, оскільки це змінює провідність, на якій побудована система. Крім того, вони не працюють з металом. Тому даний сканер неможливо сховати, він завжди є окремим елементом на пристрої. Принцип роботи ємнісного сканера відбитків пальців представлений на рис. 1.6.

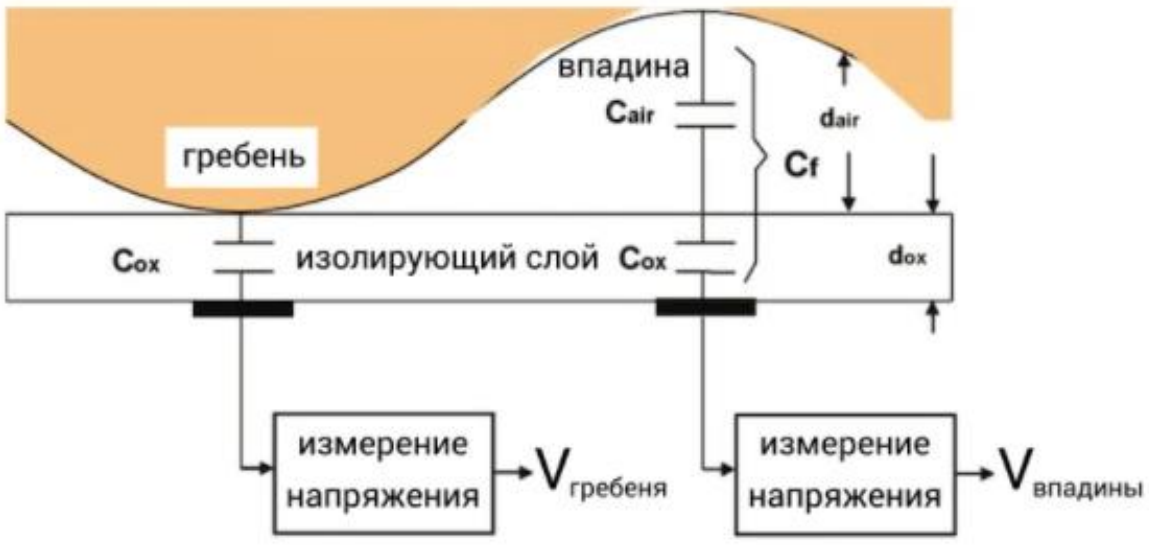

Рис 1.6. Принцип роботи ємнісного сканера відбитків пальців

1.6.2 Ультразвукові сканери відбитків пальців

Ультразвукові сканери відбитків пальців є новими та мають майбутнє, якщо вони будуть працювати за призначенням. Принцип - 3D замість 2D. За допомогою ультразвуку датчик може нанести на карту 3D-хребти і долину, що утворюють відбиток пальця.

Перевага полягає в тому, що це потенційно набагато точніше (у роздільній здатності), ніж ємнісний зчитувач відбитків пальців, відстань між відбитками пальців і датчиком може бути більшим, і він працює за металом / склом. Це означає, що датчик відбитків пальців не повинен бути видимим, і його можна заховати за корпусом телефону або, можливо, під дисплеєм. Принцип роботи ультразвуковогоо сканера відбитків пальців представлений на рис. 1.7.

Рис 1.7. Принцип роботи ультразвукового сканера відбитків пальців

1.6.3 Оптичні сканери відбитків пальців

Оптичні зчитувачі відбитків пальців старіші і вони використовують найпростіші технології. Світло світить відбитком пальців збоку, щоб відкрити хребти та долини відбитка пальця для зчитування оптичного датчика.

Недоліком є те, що для розміщення світла потрібен більший обсяг, і це не надто надійно, оскільки надруковане зображення, протез або відформований відбиток пальця можуть призвести до збігу: їх найпростіше обдурити, оскільки вони по суті схожі на копіювальні машини. Принцип роботи оптичного сканера відбитків пальців представлений на рис. 1.8.

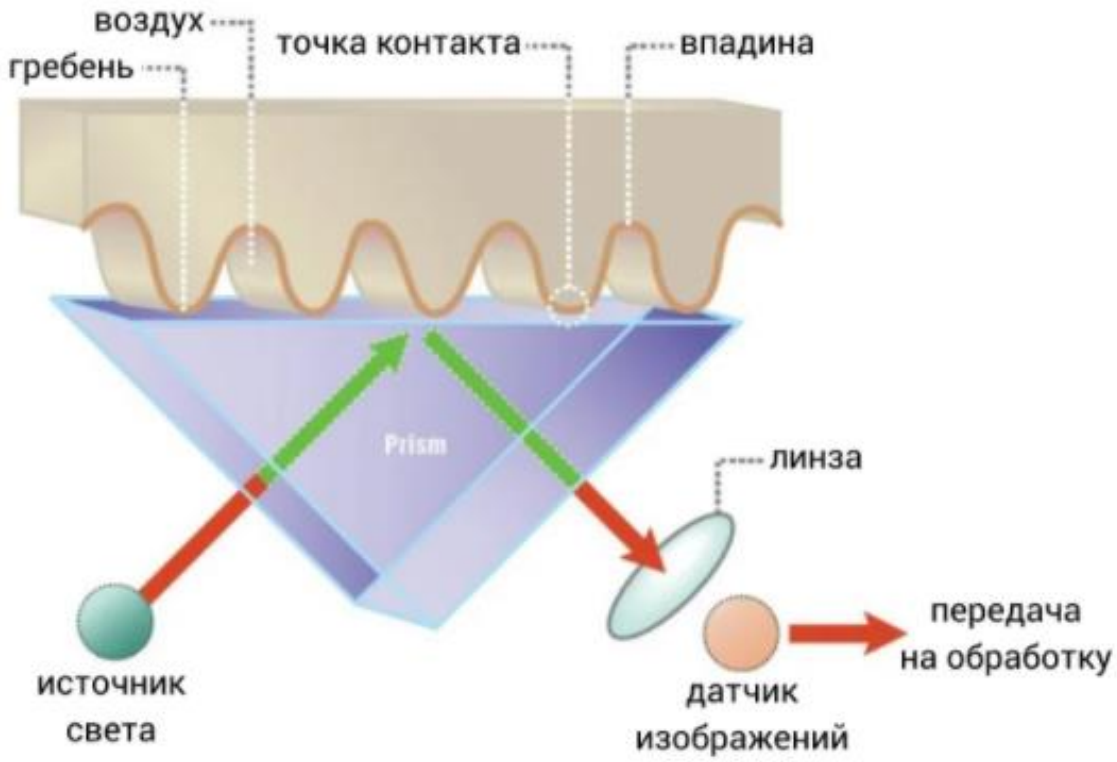

Рис 1.8. Принцип роботи оптичного сканера відбитків пальців

1.6.4 Інші сканери відбитків пальців, що не використовуються для побутової електроніки

1.6.4.1 Теплові сканери відбитків пальців

Теплові сканери відбитків пальців працюють подібно до ємнісного зчитувача відбитків пальців, за винятком того, що замість вимірювання електричного потоку вони вимірюють коливання температури. Хребти відбитка створюють більше тепла, ніж долини, і саме вони можуть створити 2D-зображення для аналізу. Одним з недоліків данного методу є те, що існує необхідність теплих погодніх умов для використання данного методу.

1.6.4.2 Сканери відбитків пальців під тиском

Сканери відбитків пальців під тиском фіксують різницю в тиску, спричинену хребтами та долинами відбитка. Знову ж таки, ми говоримо про хвилинні різниці, тому це надзвичайно чутливо. Недоліком є те, що будь-який шар, який ви покладете поверх датчика (скло ...), впливатиме на чутливість. Але якщо ви нічого не покладете, датчик може бути більш схильний до ударів та подряпин.

1.6.4.3 Радіочастотні сканери відбитків пальців

Датчики відбитків пальців мають крихітні антени для кожного пікселя остаточного 2D-зображення. Вони можуть виходити за межі глибини шкіри і злегка читати під шкірою (як обмежена ехографія), що надає більше даних і може обійти невеликі пошкодження шкіри.

1.6.5 Обрання сканера відбитків пальців

При обранні сканера відбитків пальців требазважати на співідношення якості зчитуваних даних та можливості підробки відбитків пальців та

дороговартості даного сканеру. За даними критеріями було обрано емнісним сканер відбитків пальців, оскільки в категорію недороговартісних сканерів відбитків пальців входять оптичні та емнісні сканери відбитків пальців, але слід зазначити, що оптичні сканери є найбільш уразливими. Оптичні сканери використовують найпростіші технології, тому даний сканер можливо обдурити, навіть, фотокарткою з необхідним відбитком пальців, тому було обрано саме ємнісний сканер відбитків пальців.

1.7 Arduino – створення електронного пристрою

Arduino - це електронна платформа з відкритим кодом, заснована на простому у використанні апаратному та програмному забезпеченні. Плати Arduino здатні читати входи - світло на датчику, палець на кнопці або повідомлення в Twitter - і перетворювати його на вихід - активуючи двигун, включаючи світлодіод, публікуючи щось в Інтернеті. Ви можете сказати своїй платі, що робити, надіславши набір інструкцій мікроконтролеру на платі. Для цього ви використовуєте мову програмування Arduino (на основі підключення) та програмне забезпечення Arduino (IDE) на основі обробки .

Протягом багатьох років Arduino був мозком тисяч проектів, від повсякденних об'єктів до складних наукових інструментів. Всесвітнє співтовариство виробників - студенти, любителі, художники, програмісти та професіонали - зібралося навколо цієї платформи з відкритим кодом, їх внески додали неймовірний обсяг доступних знань, які можуть бути корисними як для новачків, так і для експертів.

Ардуїно народився в Інституті дизайну взаємодії Ivrea як простий інструмент для швидкого створення прототипів, орієнтований на студентів, які не мають досвіду в галузі електроніки та програмування. Як тільки платформа Arduino дійшла до ширшої спільноти, вона почала змінюватися, щоб адаптуватися до нових потреб і викликів, диференціюючи свою пропозицію від простих 8-бітних плат до продуктів для додатків IoT , носимих пристроїв, 3D-

друку та вбудованих середовищ. Усі плати Arduino повністю відкриті, що дозволяє користувачам створювати їх самостійно та врешті-решт адаптувати їх до їхніх конкретних потреб. Програмне забезпечення теж є відкритим, і воно зростає завдяки внеску користувачів по всьому світу.

1.7.1 Переваги Arduino

Завдяки простому та доступному користувачеві досвіду Arduino використовується в тисячах різних проектів та додатків. Програма Arduino проста у використанні для початківців, але досить гнучка для досвідчених користувачів. Він працює на Mac, Windows і Linux. Викладачі та студенти використовують його для побудови недорогих наукових інструментів, для доведення принципів хімії та фізики або для початку роботи з програмуванням та робототехнікою. Дизайнери та архітектори створюють інтерактивні прототипи, музиканти та художники використовують його для інсталяцій та експериментів з новими музичними інструментами. Виробники, звичайно, використовують його для побудови багатьох проектів, виставлених на Maker Faire, наприклад. Arduino - ключовий інструмент для вивчення нових речей. Будь-хто - діти, любителі, художники, програмісти - може розпочати майструвати, просто дотримуючись покрокових інструкцій набору,

Є багато інших мікроконтролерів та платформ мікроконтролерів, доступних для фізичних обчислень. Parallax Basic Stamp, Netmedia BX-24, Phidgets, MIT's Handyboard та багато інших пропонують подібну функціональність. Усі ці інструменти беруть безладні деталі програмування мікроконтролера та обертають їх у простий у використанні пакет. Arduino також спрощує процес роботи з мікроконтролерами, але це пропонує певну перевагу для вчителів, студентів та зацікавлених аматорів перед іншими системами:

- Недорого - плати Arduino відносно недорогі в порівнянні з іншими платформами мікроконтролера. Найдешевшу версію модуля Arduino можна зібрати вручну, і навіть попередньо зібрані модулі Arduino коштують менше 50 доларів

- Кроссплатформенність - програмне забезпечення Arduino (IDE) працює на операційних системах Windows, Macintosh OSX та Linux. Більшість систем мікроконтролера обмежені Windows.

- Просте, зрозуміле середовище програмування - Програмне забезпечення Arduino (IDE) є простим у користуванні для початківців, але при цьому досить гнучким для просунутих користувачів. Для вчителів це зручно на основі середовища програмування Processing, тому студенти, які навчаються програмуванню в цьому середовищі, будуть знайомі з тим, як працює Arduino IDE.

- Програмне забезпечення з відкритим кодом та розширення - Програмне забезпечення Arduino публікується як інструменти з відкритим кодом, доступні для розширення досвідченими програмістами. Мову можна розширити за допомогою бібліотек C ++, і люди, які хочуть зрозуміти технічні деталі, можуть зробити перехід від Arduino до мови програмування AVR C, на якій вона базується. Подібним чином, ви можете додати код AVR-C безпосередньо у свої програми Arduino, якщо хочете.

- Відкрите вихідне та розширюване обладнання - Плани плат Arduino публікуються під ліцензією Creative Commons, тому досвідчені дизайнери схем можуть зробити власну версію модуля, розширивши його та вдосконаливши. Навіть відносно недосвідчені користувачі можуть створити макетну версію модуля , щоб зрозуміти, як він працює, і заощадити гроші.

1.7.2 Uno 3

Arduino UNO R3 часто використовуваний мікроконтролер плати в родині Arduino. Це третя версія плати Arduino UNO випущена в 2011 році. Головна перевага цієї плати полягає в тому, що якщо сталась помилка, то є можливість зміни мікроконтролера на платі. Основні особливості цієї плати в основному

включають те, вона доступна в DIP (подвійний вбудований пакет), знімний та мікроконтролер ATmega328. Програмування цієї плати можна легко завантажити за допомогою комп'ютерної програми Arduino[12].

Arduino Uno R3 - це один із видів мікроконтролерів на базі ATmega328P. Він включає все, що потрібно для утримання мікроконтролера; необхідно просто підключити його до ПК за допомогою USB-кабелю і для початку необхідно подати живлення за допомогою адаптера змінного струму або батареї. Термін Uno означає "один" мовою "італійської" і був обраний для позначення випуску програмного забезпечення IDE 1.0 від Arduino. R3 Arduino Uno - це третя, а також остання модифікація Arduino Uno. Плата Arduino та програмне забезпечення IDE є еталонними версіями Arduino і наразі перейшли до нових версій. Плата Uno є основною в послідовності плат USB- Arduino та еталонною моделлю, розробленою для платформи Arduino. Загальний вигляд плати Arduino Uno R3 зображений на рис. 1.9.

Рис. 1.9. Загальний вигляд плати Arduino Uno R3

1.7.2.1 Технічні характеристики

Плата Arduino Uno R3 включає наступні характеристики.

- Це мікроконтролер на базі ATmega328P
- Робоча напруга Arduino становить 5В
- Рекомендована вхідна напруга коливається від 7 В до 12 В
- Напруга в / п (гранична) становить від 6 В до 20 В
- Цифрові входи та виходи - 14
- Цифрові вхідні та вихідні штифти (ШІМ) -6
- Аналогові штифти вводу / виводу - 6
- Струм постійного струму для кожного виводу вводу-виводу становить 20 мА
- Струм постійного струму, який використовується для виводу 3,3 В, становить 50 мА
- Флеш-пам’ять -32 КБ та 0,5 КБ пам’яті використовується завантажувачем
- SRAM становить 2 КБ
- EEPROM - 1 Кб
- Швидкість CLK становить 16 МГц
- Вбудований світлодіод
- Довжина і ширина Arduino складають 68,6 мм X 53,4 мм
- Вага дошки Arduino становить 25 г.

Схема виводів Arduino Uno R3 показана на рис. 1.10. складається з 14-значних штифтів вводу-виводу. З цих штифтів можна використовувати 6-штиркові, як Pin-виходи. Ця плата включає 14 цифрових вхідних/вихідних штифтів, аналогові входи-6, USB-з'єднання, кварцовий кристал-16 МГц, гніздо живлення, USB-з'єднання , резонатор- 16 МГц, гніздо живлення, заголовок ICSP і кнопку RST.

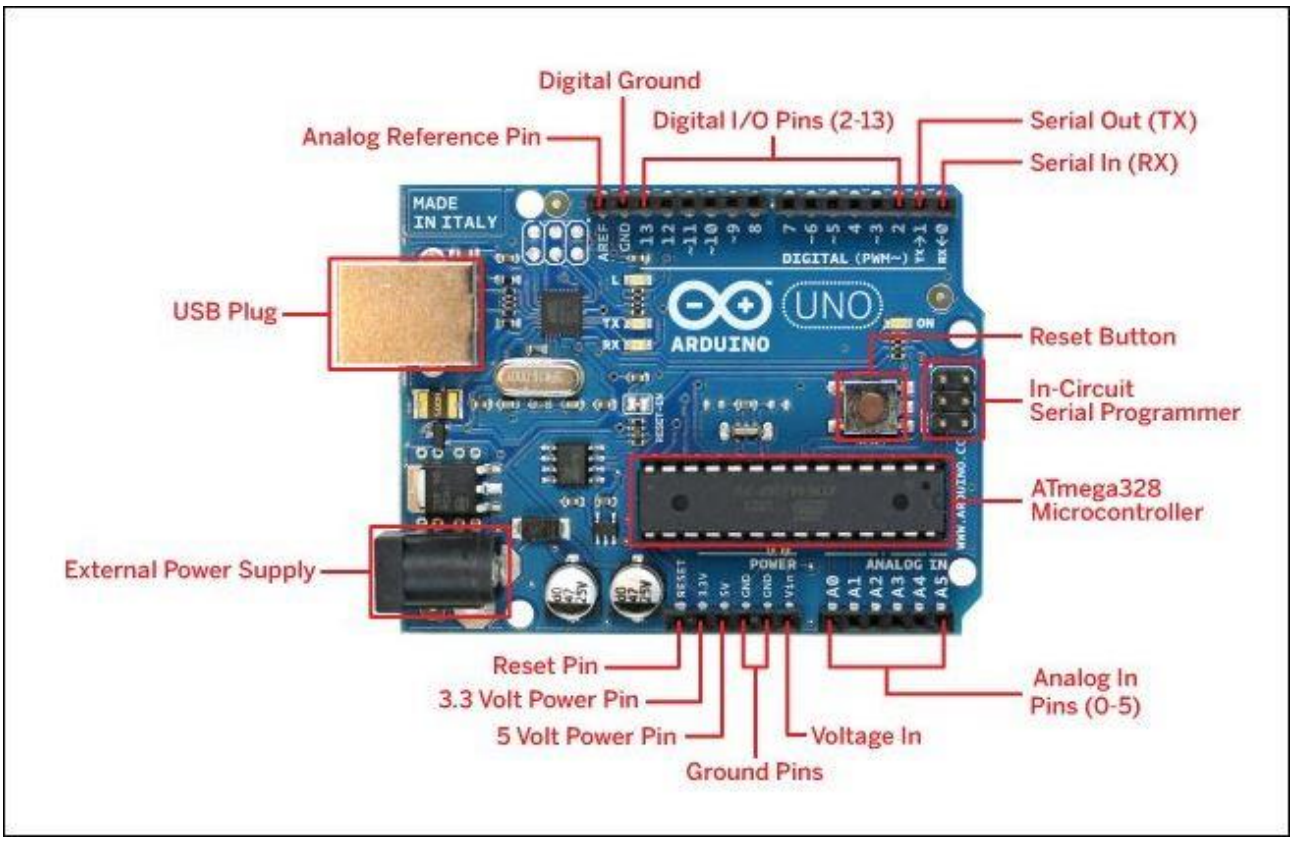

Рис. 1.10. Схема виводів Arduino Uno R3

1.7.3 Програмне середовище Arduino.ide

Інтегроване середовище розробки Arduino - або Arduino Software (IDE) - містить текстовий редактор для написання коду, область повідомлень, текстову консоль, панель інструментів з кнопками для загальних функцій та ряд меню. Він підключається до апаратного забезпечення Arduino для завантаження програм та зв’язку з ними.

Програми, написані за допомогою програмного забезпечення Arduino (IDE), називаються ескізами . Ці ескізи написані в текстовому редакторі та зберігаються із розширенням файлу .ino. Редактор має функції для вирізання / вставки та для пошуку / заміни тексту. Область повідомлення надає зворотній зв'язок під час збереження та експорту, а також відображає помилки. На консолі відображається текст, виведений програмним забезпеченням Arduino (IDE), включаючи повне повідомлення про помилки та іншу інформацію. У нижньому правому куті вікна відображаються налаштовані плата та послідовний порт.

Кнопки на панелі інструментів дозволяють перевіряти та завантажувати програми, створювати, відкривати та зберігати ескізи та відкривати послідовний монітор.

На рис. 1.11 позначена кнопка «Перевірити». Перевіряє код на наявність помилок при його складанні.

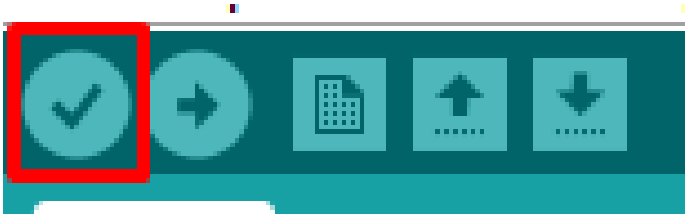

Рис. 1.11. Кнопка «Перевірити»

На рис. 1.12 позначена кнопка «Вивантажити». Компілює код і завантажує його на налаштовану плату.

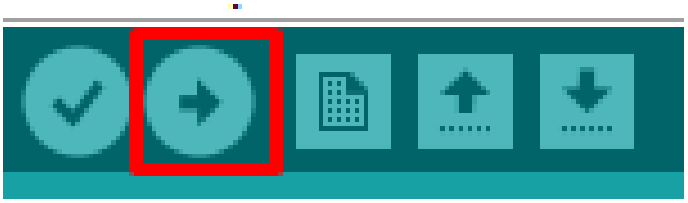

Рис. 1.12. Кнопка «Вивантажити»

На рис. 1.13 позначена кнопка «Створити». Створює новий ескіз.

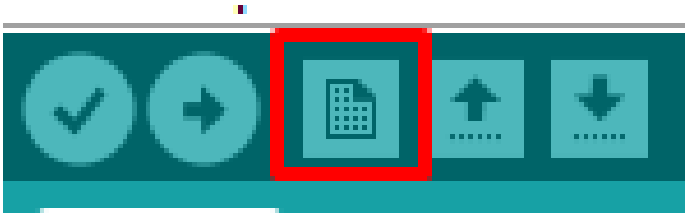

Рис. 1.13. Кнопка «Створити»

На рис. 1.14 позначена кнопка «Відкрити». Представляє меню всіх ескізів у етюднику. Натиснувши один, він відкриється в поточному вікні, перезаписавши його вміст.

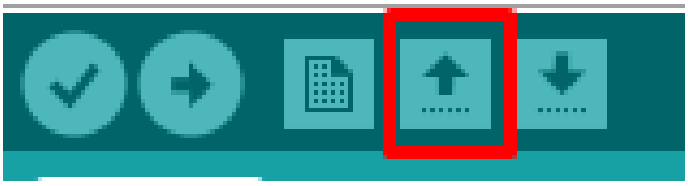

Рис. 1.14. Кнопка «Відкрити»

На рис. 1.15 позначена кнопка «Зберегти». Зберігає ескіз.

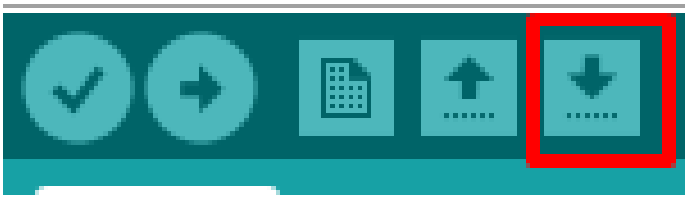

Рис. 1.15. Кнопка «Зберегти»

Додаткові команди знаходяться в п'яти меню: Файл , Редагувати , Ескіз , Інструменти , Довідка . Меню залежить від контексту, що означає, що доступні лише ті пункти, що стосуються роботи, що виконується в даний час.

Меню «Файл». Додаткові параметри.

- Створити. Створює новий екземпляр редактора з мінімальною структурою ескізу, що вже існує.
- Відкрити. Дозволяє завантажувати файл ескізу, переглядаючи диски та папки комп'ютера.
- Відкрити нещодавні. Надає короткий список найсвіжіших ескізів, готових до відкриття.
- Тека зі скетчами. Показує поточні ескізи в структурі папки альбому. натискання будь-якого імені відкриває відповідний ескіз у новому екземплярі редактора.
- Приклади. У цьому пункті меню відображається будь-який приклад, наданий програмним забезпеченням Arduino (IDE) або бібліотекою. Усі приклади структуровані у дереві, що забезпечує легкий доступ за темою чи бібліотекою.
- Закрити. Закриває екземпляр програмного забезпечення Arduino, з якого його натискають.

- Зберегти. Зберігає ескіз із поточною назвою. Якщо файл раніше не називався, ім'я буде вказано у вікні "Зберегти як ..".
- Зберегти як. Дозволяє зберегти поточний ескіз з іншою назвою.
- Параметри сторінки Відображає вікно Налаштування сторінки для друку.
- Друк. Надсилає поточний ескіз на принтер відповідно до налаштувань, визначених у Налаштування сторінки.
- Налаштування. Відкриває вікно Налаштування, де можна налаштувати деякі налаштування IDE як мову інтерфейсу IDE.
- Вихід. Закриває всі вікна IDE. Ті самі ескізи, відкриті при виборі Quit, будуть автоматично відкриті при наступному запуску IDE.

Відображення меню «Файл» показано на рис. 1.16.

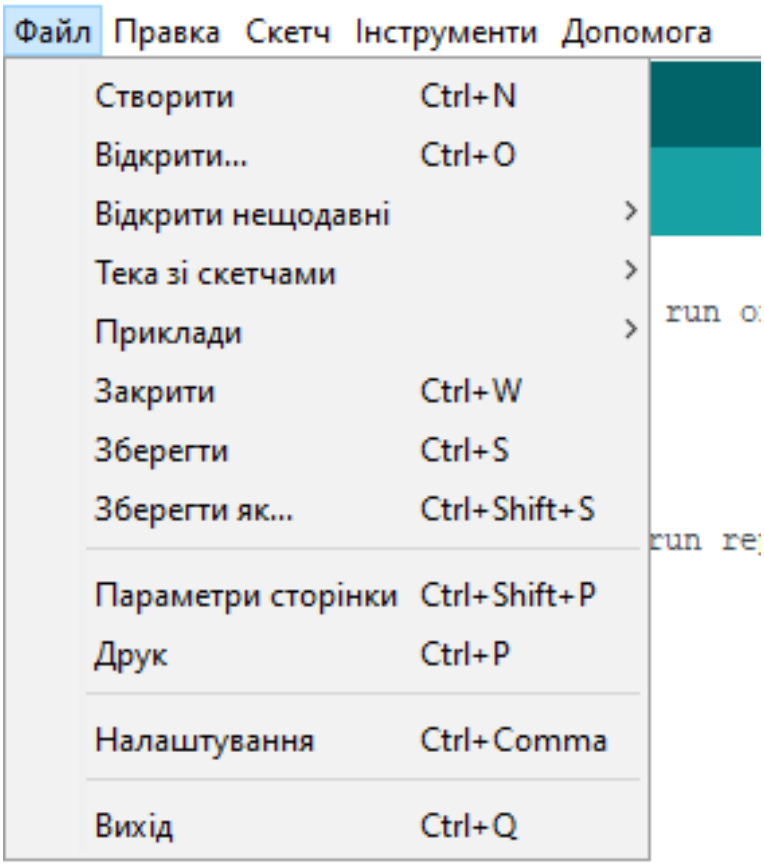

Рис. 1.16. Відображення меню «Файл»

Меню «Правка». Додаткові параметри.

- Повернути/Повернути. Повертається до одного або декількох кроків, зроблених під час редагування; При поверненні назад можливо відмінити крок вперед за допомогою Ctrl+Y.
- Вирізати. Видаляє виділений текст із редактора та розміщує його в буфері обміну.
- Копіювати. Дублює виділений текст у редакторі та розміщує його в буфері обміну.
- Копіювати для форуму. Копіює код ескізу в буфер обміну у формі, придатній для публікації на форумі, разом із забарвленням синтаксису.
- Копіювати як HTML. Копіює код ескізу у буфер обміну як HTML, що підходить для вбудовування у веб-сторінки.
- Вставити. Вміщує вміст буфера обміну в позицію курсора в редакторі.
- Виділити все. Виділяє та виділяє весь вміст редактора.
- Коментувати/Розкоментувати. Проставляє або видаляє маркер // коментаря на початку кожного вибраного рядка.
- Збільшити/зменшити відступ. Додавання або віднімання пробілу на початку кожного виділеного рядка, переміщення тексту на один пробіл праворуч або вилучення пробілу на початку.
- Збільшити/зменшити розмір шрифту. Додавання або віднімання пунктів до поточного значення розміру шрифту.
- Знайти. Відкриває вікно «Знайти та замінити», де можливо вказати текст для пошуку в поточному ескізі відповідно до кількох варіантів.
- Знайти далі. Виділяє наступне входження (якщо воно є), вказаного як елемент пошуку у вікні «Знайти», щодо позиції курсора.
- Знайти попереднє. Виділяє попереднє входження (якщо воно є), вказаного як елемент пошуку у вікні Знайти щодо позиції курсору.

Відображення меню «Правка» показано на рис. 1.17.

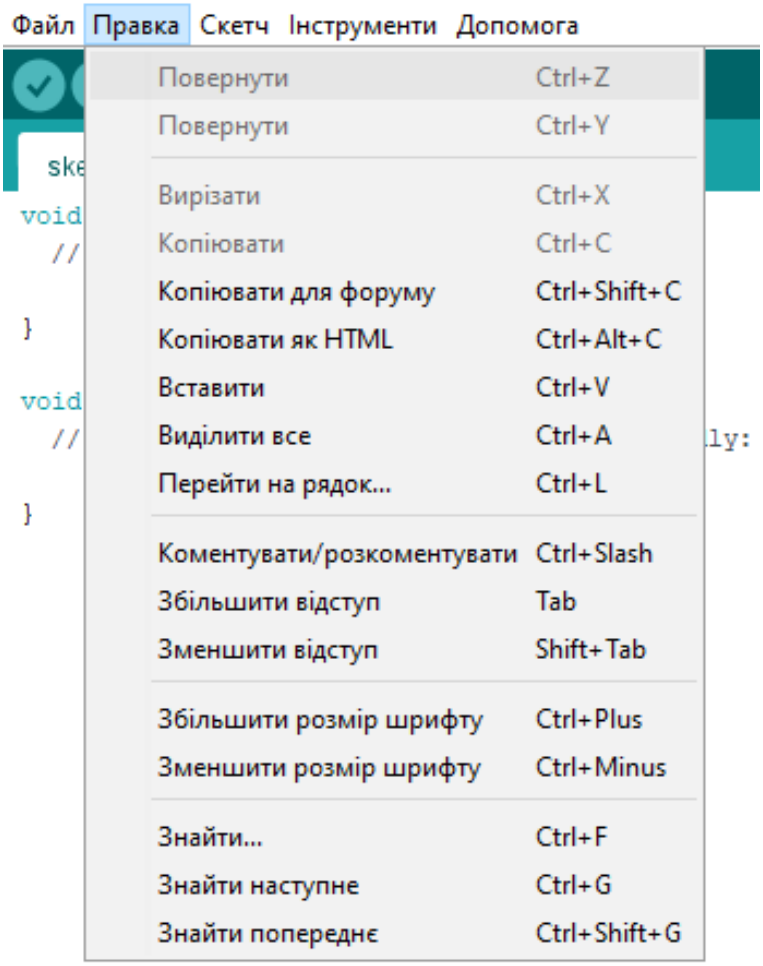

Рис. 1.17. Відображення меню «Файл»

Меню «Скетч». Додаткові параметри.

Перевірити/Зкомпілювати. Перевіряє ескіз на наявність помилок при його складанні; буде повідомляти про використання пам'яті для коду та змінних в області консолі.

Вивантажити. Перевіряє та завантажує двійковий файл на налаштовану плату через налаштований порт.

Вивантажити за допомогою програматора. Буде перезаписаний завантажувач на платі; необхідно скористатися Інструменти > Записати завантажувач, щоб відновити його та мати можливість знову завантажити на послідовний порт USB.

Експорт скомпільованого бінарника. Зберігає файл .hex, який може зберігатися як архів або надсилатися на дошку за допомогою інших інструментів.

Показати папку скетчів. Відкриває поточну папку ескізу.

Додати бібліотеку. Додає бібліотеку до ескізу, вставляючи оператори #include на початку коду.

Додати файл. Додає вихідний файл до ескізу (він буде скопійований із поточного місця розташування). Новий файл з'явиться на новій вкладці у вікні ескізу. Файли можна вилучити з ескізу за допомогою меню вкладок, до якого можна натиснути маленький піктограму трикутника під послідовним монітором праворуч від панелі інструментів.

Відображення меню «Скетч» показано на рис. 1.17.

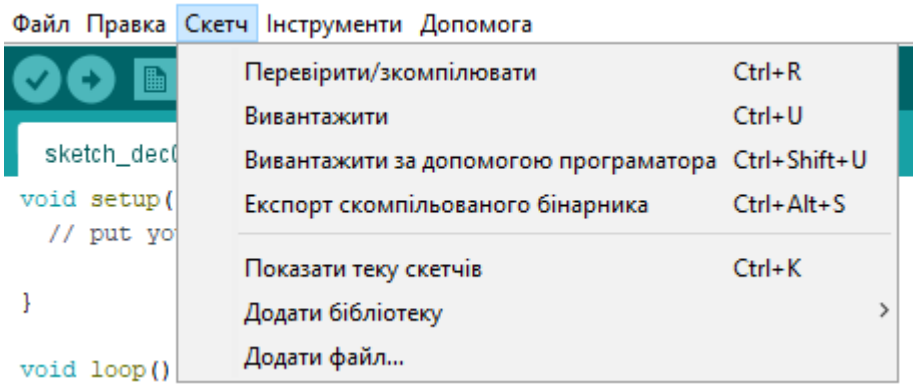

Рис. 1.17. Відображення меню «Скетч»

Меню «Інструменти». Додаткові параметри.

Автоформатування. Візуально форматує код, робить його з відступами, щоб відкриті та закриті фігурні дужки вирівнювались, а оператори всередині фігурних дужок мали більший відступ.

Архівувати скетч. Архівує копію поточного ескізу у форматі .zip. Архів розміщується в тому ж каталозі, що і ескіз.

Виправити кодування та перезавантажити. Виправляє можливі розбіжності між кодуванням карт редактора символів та іншими картами символів операційних систем.

Послідовний плотер. Відкриває вікно послідовного плотера та ініціює обмін даними з будь-якою підключеною платою на поточно обраному порту.

Плата. Вибір плати для використання.

Порт. Це меню містить усі послідовні пристрої (реальні або віртуальні) на вашому комп'ютері. Він повинен автоматично оновлюватися кожного разу, коли відкривається меню інструментів верхнього рівня.

Програматор. Для вибору програмного забезпечення під час програмування плати чи мікросхеми без використання вбудованого послідовного USB-з'єднання.

Записати завантажувач. Елементи цього меню дозволяють записати завантажувач на мікроконтролер на платі Arduino. Це не потрібно для використання плати Arduino або Genuino, але необхідно для нового мікроконтролера ATmega (який зазвичай постачається без завантажувача).

Відображення меню «Інструменти» показано на рис. 1.18.

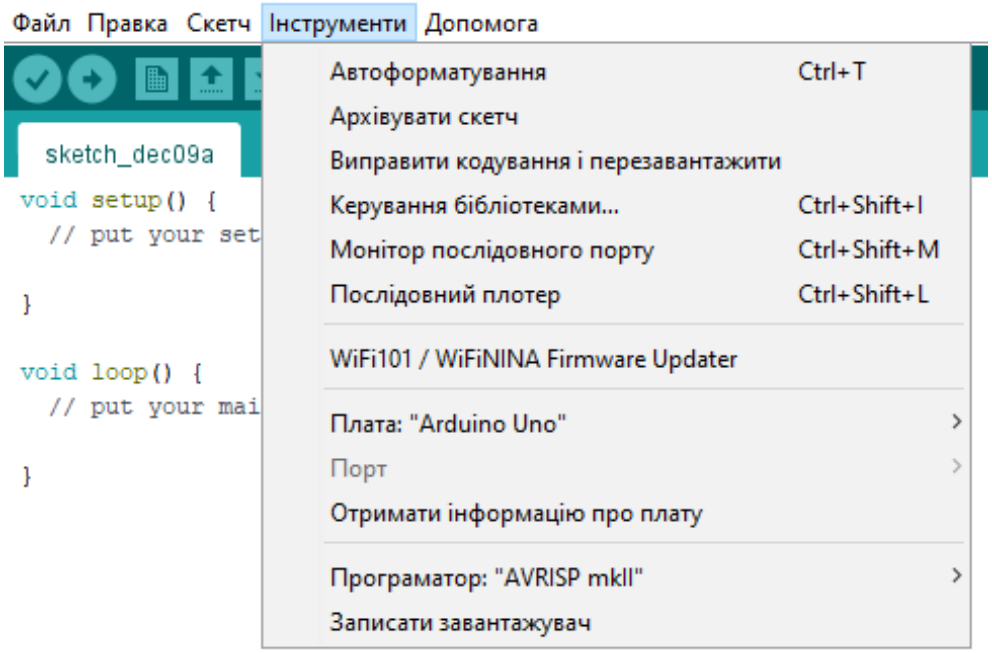

Рис. 1.18. Відображення меню «Інструменти»

Меню «Допомога». Додаткові параметри.

Це меню надає доступ до ряду документів, що постачаються з програмним забезпеченням Arduino (IDE). Доступ до Початок роботи, Довідника, цього посібника з IDE та інших документів надається локально, без з'єднання з Інтернетом. Документи є локальною копією Інтернет-документів і можуть посилатися на веб-сайт Arduino.

Знайти в довідці. Це єдина інтерактивна функція меню Допомога: вона безпосередньо вибирає відповідну сторінку в локальній копії Посилання для функції або команди під курсором.

Відображення меню «Допомога» показано на рис. 1.19.

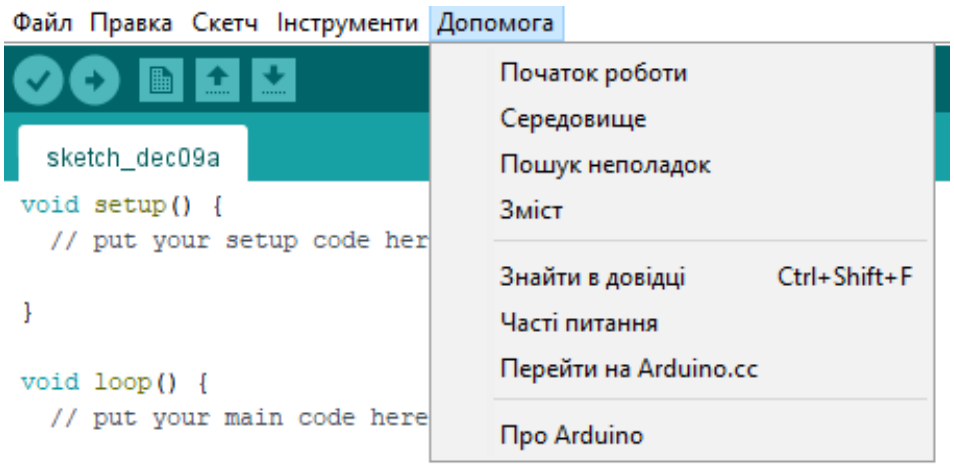

Рис. 1.19. Відображення меню «Допомога»

Висновки до розділу 1

В розділі 1 було проаналізовано діюче Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства та проект Закону України "Про ідентифікацію людини шляхом дактилоскопії". Аналіз показав, що

Були наведені основні методи біометричної ідентифікації, які поділяються на фізіологічні, тобто ті, які були придбані при народженні, а також поведінкові, які, при бажанні, можна змінити. Наразі найбільш поширеною системою для біометричної ідентифікації є сканування відбитків пальців, оскільки, даний метод є низьким за собівартістю для впровадження у різні аспекти життя людини та швидка швидкість автентифікації. Та сканування відбитків пальців – це надійніша система, оскільки є висока ймовірність фальсифікації, що неможлива, наприклад при розпізнаванні райдужки ока.

Також були наведені основні види сканерів відбитків пальців. Виявлено, що найпростішим сканером є оптичний сканер, оскільки його можливо обійти навіть за допомогою листка з надрукований відбитком пальця або фотографії. Найскладнішим для створення системи розблокування є ультразвуковий сканер, оскільки для створення даної моделі необхідний 3D-муляж з «внутрішніми» даними, такими як пульс

Розділ 2. Практичний розділ

Для подальшої роботи використаємо середовище програмування Arduino.ide.

Оскільки плата Uno 3 не підтримує більше однієї програми, то необхідно роз’єднати задачу внесення та перевірки відбитків пальців на дві частини:

- Перша частина. Программа enroll.ino. Реалізує зчитування, завантаження та зберігання відбитків пальців у пам’яті сенсору для можливості подальшої перевірки на збіг нових відсканованих відбитків пальців з моделями, які завантажені до пам’яті сенсору. Дана програма використовується одноразово, після чого встановлюється програма fingerprint.ino.
- Друга частина. Программа fingerprint.ino. Реалізує перевірку на збіг відсканованих відбитків пальців з моделями, які завантажені до пам’яті сенсору. Дана програма завантажується другою та є активною увесь час.

2.1. Створення алгоритмів роботи системи розблокування електронного пристрою з дактилоскопічним захистом

Оскільки дана система розблокування поділяється на дві програми, то необхідно окремо описати два алгоритми функціонування для даних програм:

- Алгоритм функціонування для програми enroll.ino
- Алгоритм функціонування для програми fingerprint.ino

2.1.1. Алгоритм для програми enroll.ino

Покроково розглянемо алгоритм роботи першої програми enroll.ino:

1. Проводиться ініціалізація сенсору. За допомогою цього можна ще перевірити систему на відгук;
2. Скануємо палець та отримуємо відбиток пальця у пам’яті сенсору; Зі сканованого відитку отримуємо малюнок, з характерними рисами для подальшої роботи;
3. Перетоворюмо отриманий малюнюк на модель для подальшого пошуку збігів;
4. Зберігаємо отриману модель відбитків пальців;
5. Для більшої захищеності встановлюємо пароль на систему.

Алгоритм роботи даної програми enroll.ino поданий на рис. 2.1.

Рис. 2.1. Алгоритм програми enroll.ino

2.1.2. Алгоритм для програми fingerprint.ino

Також покроково розглянемо алгоритм роботи програми fingerprint.ino:

1. Користувач вносить програму fingerprint.ino до Arduino;
2. На екран виводяться основні характристики та перевіряє відгук датчиків;

3. Виконується перевірка наявності відбитків пальців у системі. У разі, якщо даних не має, на екран виводиться інформація про відсутість відбитків у базі та прохання внести відбитки до пам’яті. У разі присутності даних виводится інформація про те, що дані є, та запрошення на зчитування відбитків для подальшої перевірки;

4. Сканером скануються відбитки пальців;

5. Виконується перевірка на коректність зчитування. У разі, якщо зчитування првоелось некоректно, на екрані з’явиться інформація та запрошення на повторне зчитування (пункт 4). У разі коректного зчитування дані будуть передані для подальшої роботи;

6. Коректно зчитаний відбиток перетворюється на шаблон для подальшої перевірки на збіг;

7. Виконується перевірка на збіг зчитаного відбитку пальця з існуючими відбитками у пам’яті сенсору. У разі відсутності збігу виведеться інформація про відсутність даних у базі сенсору та прохання внести коректний відбиток (пункт 4). У разі знаходження збігу буде відкритий замок.

Алгоритм роботи даної програми enroll.ino поданий на рис. 2.2.

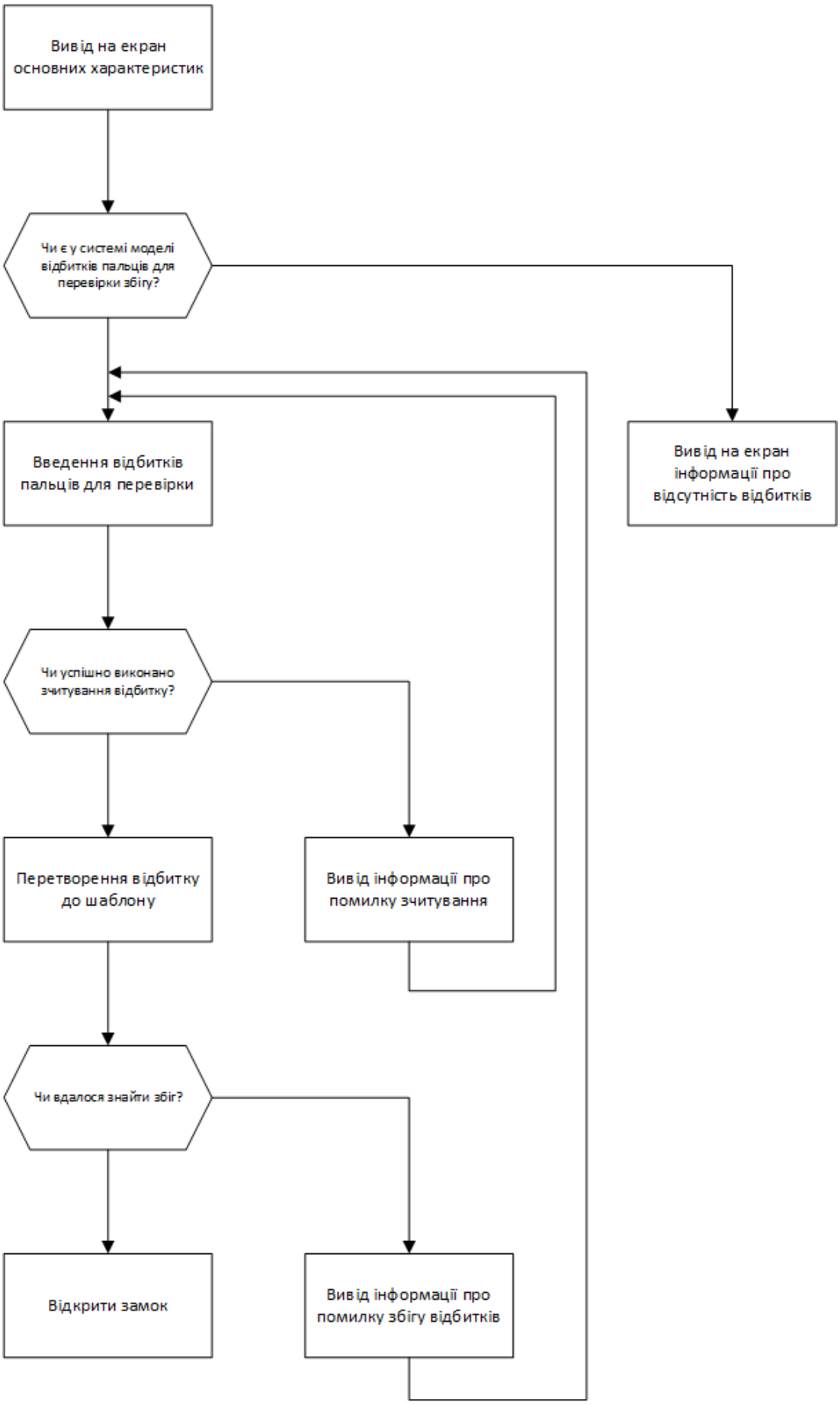

Рис. Алгоритм програми 2.2.

2.2. Програмна реалізація системи розблокування електронного пристрою з дактилоскопічним захистом

4.2.1. Програма 1 - Enroll.ino

Розглянемо програмну реалізацію використаного алгоритму програми enroll.ino[11].

У рамках першої дії за допомогою функції зробимо ініціалізацію сенсору. У даній функції ініціалізується послідовний інтерфейс та швидкість передачі даних. Реалізацію даної ініціалізації можливо побачити на рис. 2.3.

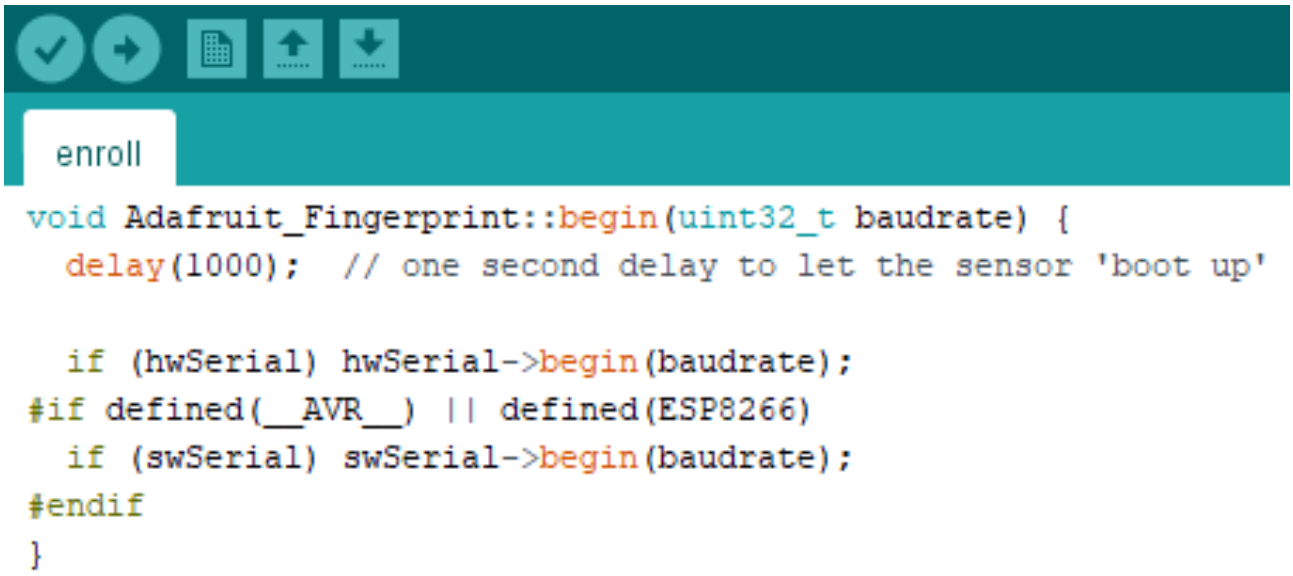

Рис. 2.3. Ініціалізація сенсору

У рамках другої дії перевіряється паролі доступу до датчиків (за замовчуванням 0x0000000). За допомогою даної перевірки можливо також перевірити чи активні датчики та чи відповідають вони. У разі корректності паролі видає True. Дану перевірку можливо побачити на рис. 2.4.

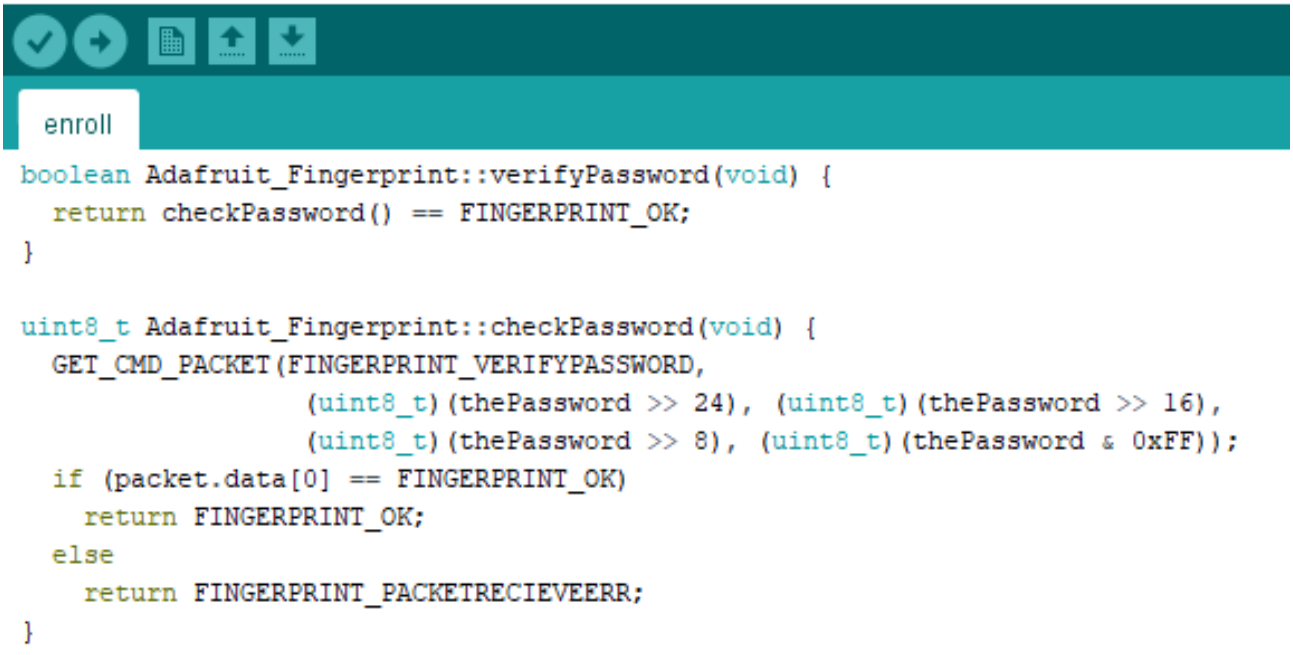

Рис. 2.4. Перевірка паролів доступу до датчиків

Наступний кроком користувач прикладає палець до сенсора. За допомогою зчитувача робиться малюнок відбитку пальця для отримання подальшого шаблону для порівняння. На рис. 2.5. представлена функція отримання малюнку відбитку пальця зі зчитаного пальця.

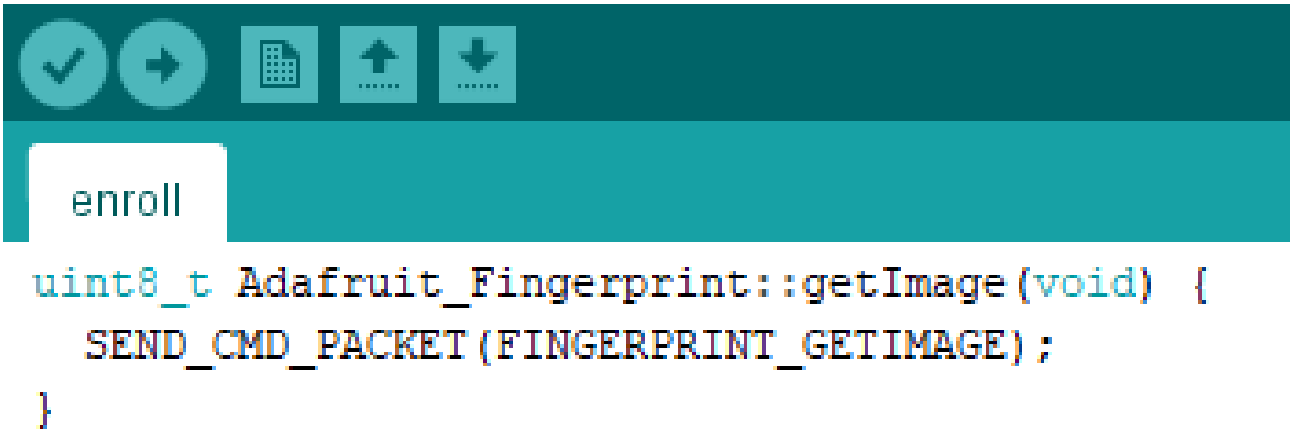

Рис. 2.5. Отримання малюнку відбитку пальця

Отриманий на минулому кроці малюнок необхідно перетворити на шаблон для подальшого створення моделі відбитку пальця. Дане перетворення робиться через функцію image2Tz. Перетворення малюнку відбитку до шаблону представлено на рис. 2.6.

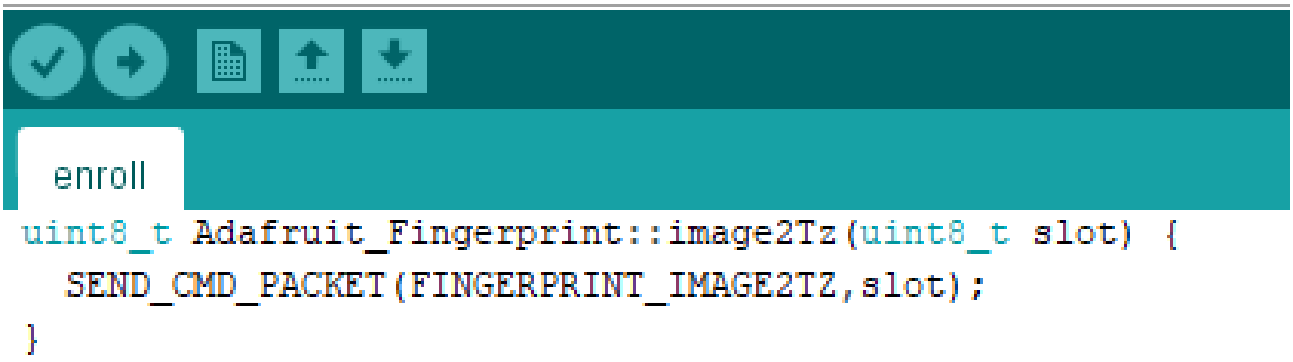

Рис. 2.6. Перетворення малюнку відбитку до шаблону

Отримані шаблони необхідно перетворити на модель для подальшого пошуку збігів. За допомогою функції createModel перетворюємо шаблони на модель. Ни рис. 2.7 представлено перетворення до моделі.

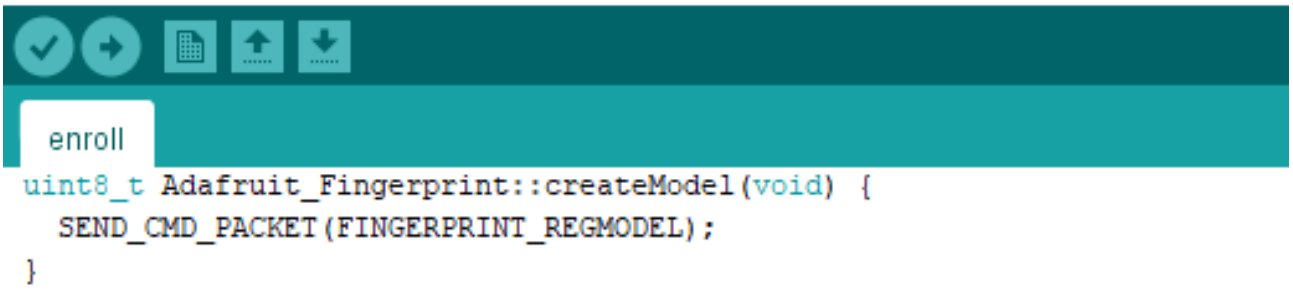

Рис. 2.7. Перетворення шаблону малюнків пальців на модель

Створена у минулому пункті модель зберігається за допомогою функції storeModel для подальшого пошуку на збіг. На рис. 2.8. представлена функція для зберігання.

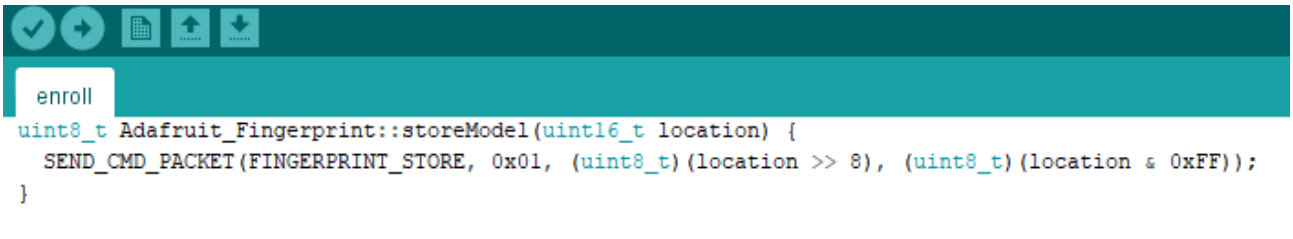

Рис. 2.8. Збереження моделі відбитку пальця

Отриману модель переміщаємо з флеш-пам'яті до пам'яті сенсору. На рис. 2.9. представлено переміщення моделі до пам'яті сенсору.

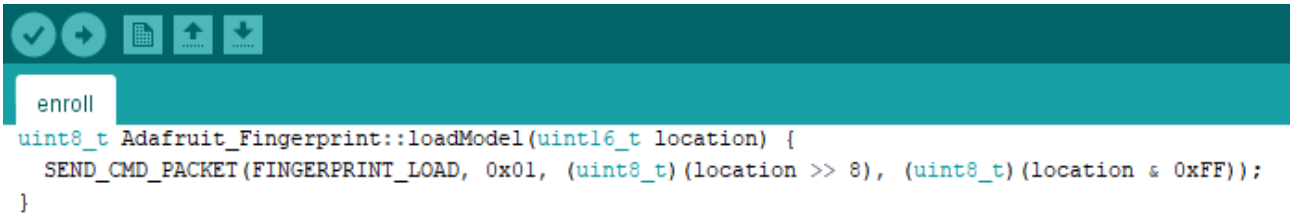

Рис. 2.9. Завантаження моделі до пам'яті сенсору

Переворюємо отриману модель на послідовність цифрових сигналів для можливості передачі даних задля перевірки. Перетворення можливо побачити ни рис. 2.10.

Рис. 2.10. Перетворення моделі на послідовність цифрових сигналів

Видаляємо усю інформацію з флеш-пам'яті для можливості подальшого записування відбитків пальців. Видалення інформації можливо побачити на рис. 2.11.

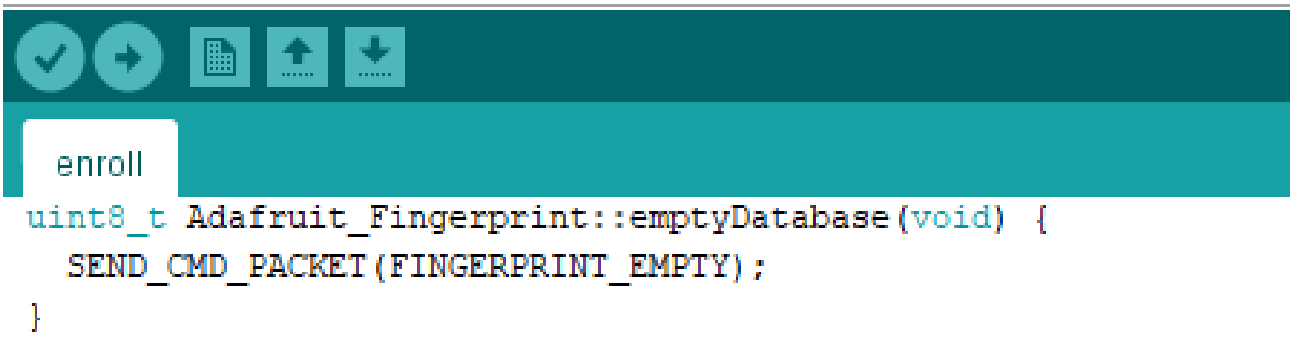

Рис. 2.11. Видалення інформації з флеш-пам’яті

Виконаємо пошук функції відбитку пальця поточного місцерозташування для відповідності збереженим шаблонам. Дане місцерозташування зберігається у fingerID, а ступінь достовірності в confidence. Дану операцію можливово побачити на рис. 2.12.

enroll

```
uint8_t Adafruit_Fingerprint::fingerFastSearch(void) {
  // high speed search of slot #1 starting at page 0x0000 and page #0x00A3
  GET_CMD_PACKET(FINGERPRINT_HISPEEDSEARCH, 0x01, 0x00, 0x00, 0x00, 0xA3);
  fingerID = 0xFFFF;
  confidence = 0xFFFF;

  fingerID = packet.data[1];
  fingerID <<= 8;
  fingerID |= packet.data[2];

  confidence = packet.data[3];
  confidence <<= 8;
  confidence |= packet.data[4];

  return packet.data[0];
}
```

Рис. 2.12. Пошук функції відбитку пальця

Визначаємо кількість шаблонів для перевірки збігу, що зберігаються в пам'яті сенсору. Номер зберігається в templateCount після успішно доданого шаблону. На рис. 2.13. зображена функція визначення кількості шаблонів.

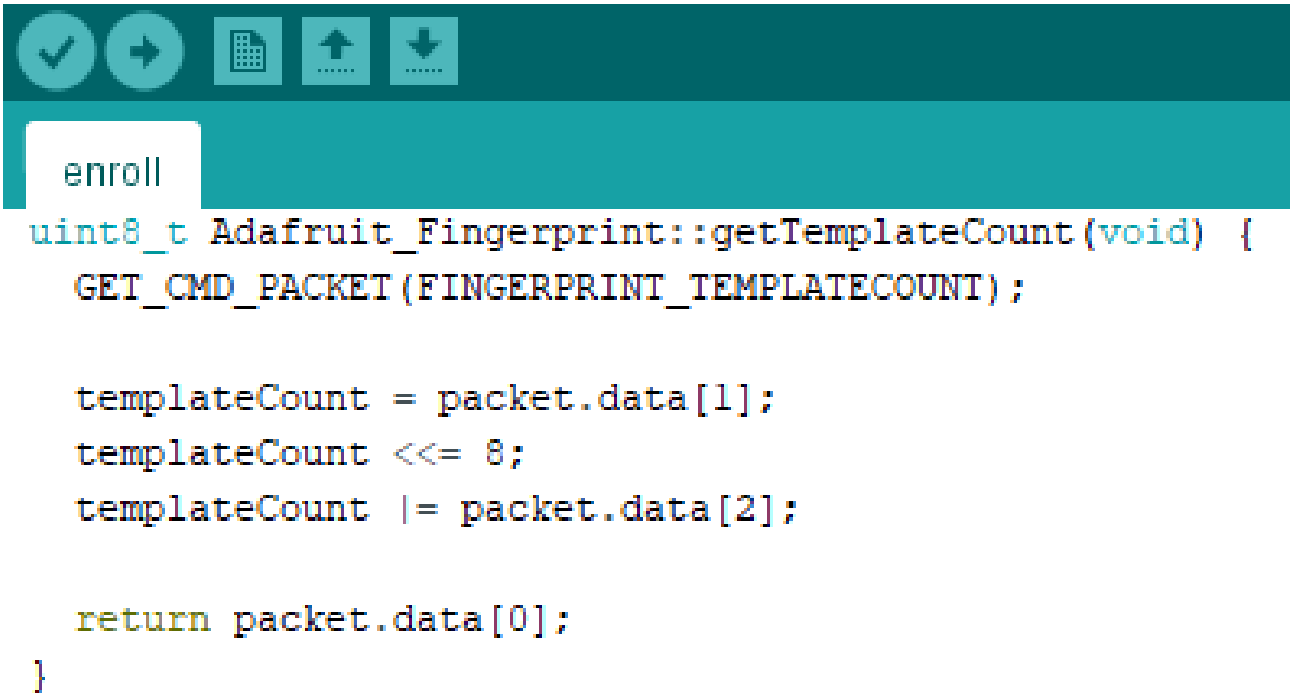

Рис. 2.13. Функція визначення кількості шаблонів

Задля додаткової безпеки використання системи розблокування електронного пристрою з дактилоскопічним захистом встановимо пароль до сенсора. На рис. 2.14 зображено встановлення паролю до сенсора.

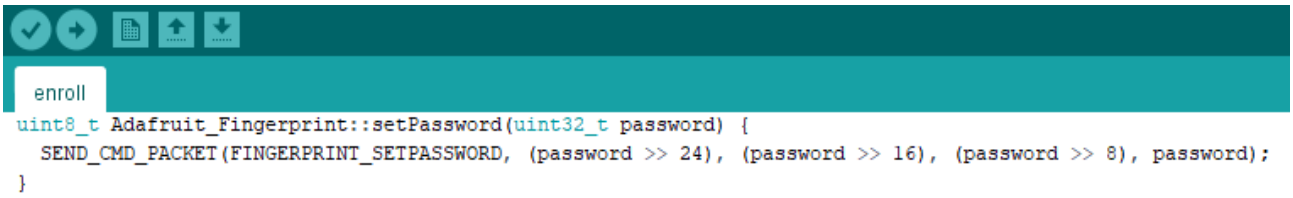

Рис. 2.13. Встановлення паролю до сенсора

Використаємо допоміжну функцію для обробки пакета надісланих даних та надсилання його цифровими сигнали на сенсор. Допоміжну функцію для обробки пакета надісланих даних можливо побачити на рис. 2.14.

Рис. 2.14. Допоміжна функція для обробки пакета надісланих даних

Використаємо допоміжну функцію для обробки даних, які приходять на сенсор з датчика та обробка їх до пакета сигналів. На рис. 2.15. та рис 2.16. (продовження) можливо побачити допоміжну функцію для обробки даних, які приходять на сенсор.

enroll

```
uint8_t Adafruit_Fingerprint::getStructuredPacket(Adafruit_Fingerprint_Packet * packet, uint16_t timeout) {
  uint8_t byte;
  uint16_t idx=0, timer=0;

  while(true) {
    while(!mySerial->available()) {
      delay(1);
      timer++;
      if( timer >= timeout) {
#ifdef FINGERPRINT_DEBUG
  Serial.println("Timed out");
#endif
  return FINGERPRINT_TIMEOUT;
      }
    }
    byte = mySerial->read();
#ifdef FINGERPRINT_DEBUG
    Serial.print("<- 0x"); Serial.println(byte, HEX);
#endif
    switch (idx) {
      case 0:
        if (byte != (FINGERPRINT_STARTCODE >> 8))
    continue;
        packet->start_code = (uint16_t)byte << 8;
        break;
      case 1:
        packet->start_code |= byte;
        if (packet->start_code != FINGERPRINT_STARTCODE)
```

Рис. 2 15. Допоміжна функція для обробки даних, які приходять на сенсор

```
      return FINGERPRINT_BADPACKET;
          break;
        case 2:
        case 3:
        case 4:
        case 5:
          packet->address[idx-2] = byte;
          break;
        case 6:
    packet->type = byte;
    break;
        case 7:
    packet->length = (uint16_t)byte << 8;
    break;
        case 8:
    packet->length |= byte;
    break;
        default:
          packet->data[idx-9] = byte;
          if((idx-8) == packet->length)
            return FINGERPRINT_OK;
          break;
      }
      idx++;
    }
    // Shouldn't get here so...
    return FINGERPRINT_BADPACKET;
}
```

Рис. 2.16. (продовження) Допоміжна функція для обробки даних, які приходять на сенсор

Результатом програми enroll.ino є створення бази шаблонів відбитків пальців в пам'яті сенсору. Відповіді на дії зі сторони користувача можливо побачити на рис. 2.17, рис. 2.18, рис. 2.19.

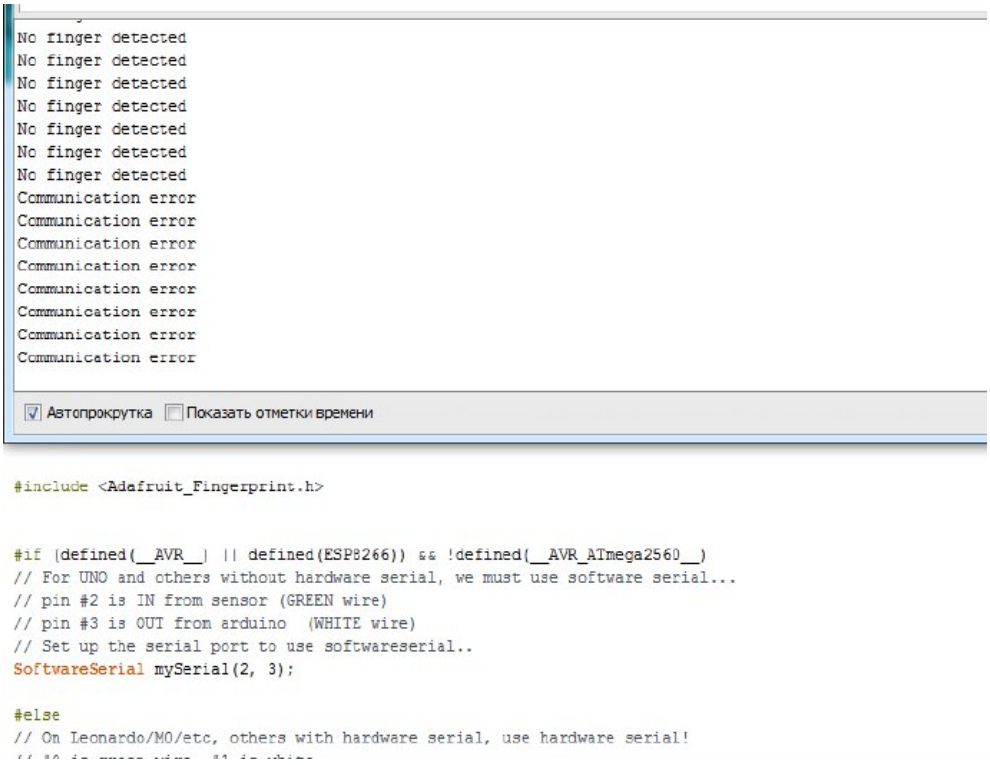

Рис. 2.17. Відповідь програми «Помилка з’єднання»

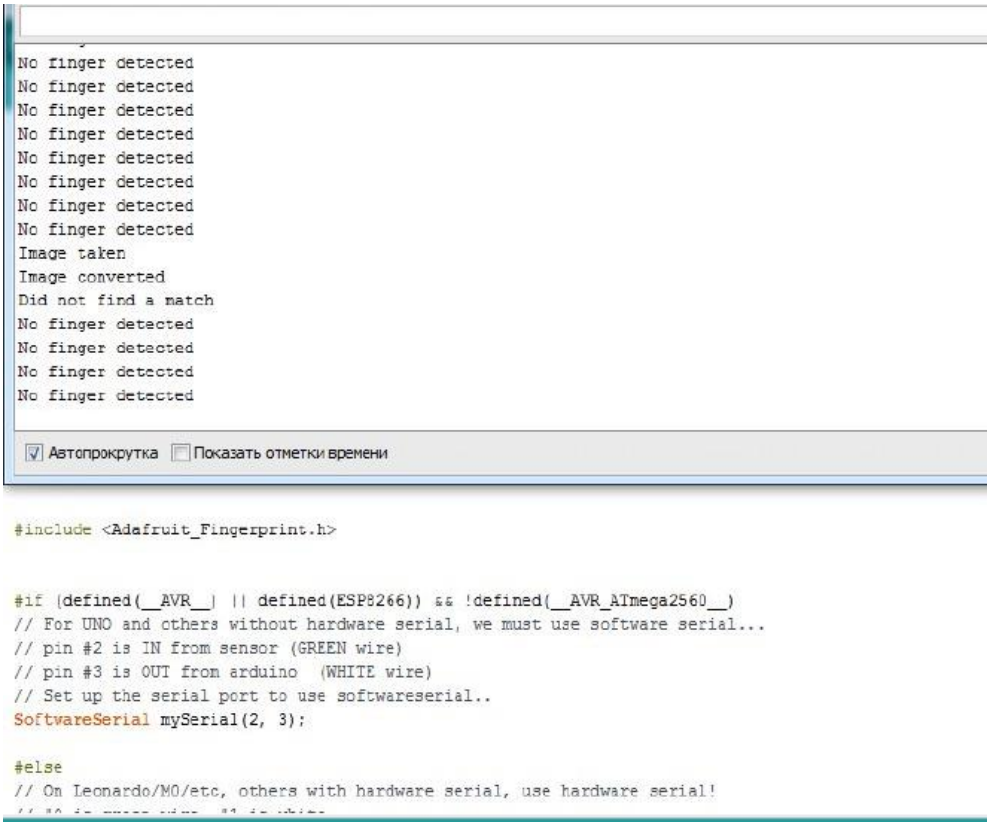

Рис. 2.18. Відповідь програми «Помилка розпізнавання»

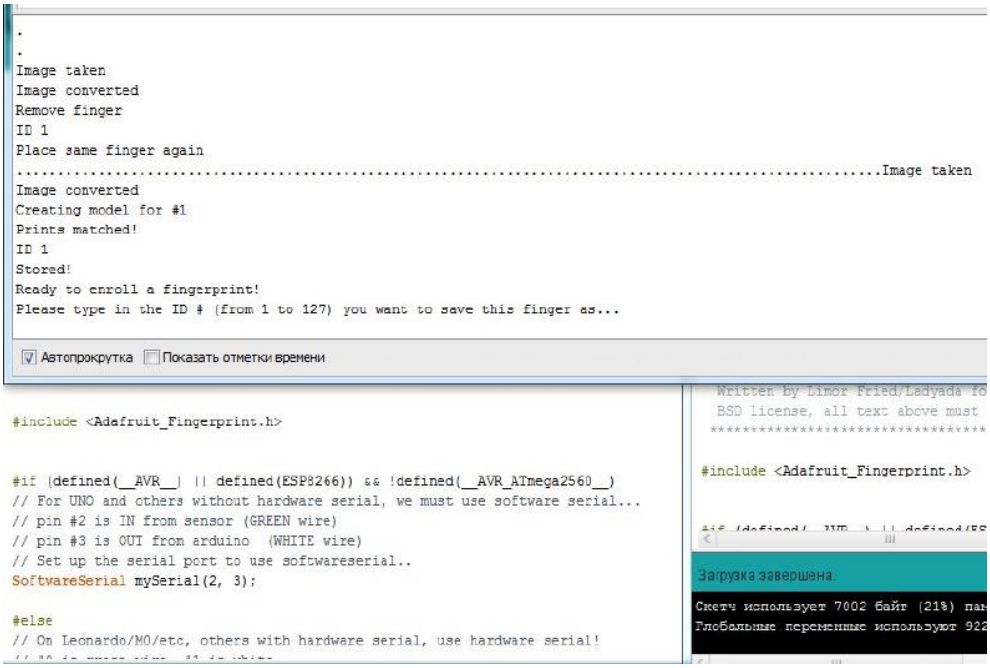

Рис. 2.19. Відповідь програми «Успішне завершення»

4.2.2. Програма 2 - Fingerprint.ino

Оголошуємо змінну finger, на яку будуть записуватися відсканований для збігу відбиток пальця. На рис. 2.20. можливо побачити дану функцію


```
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
```

Рис. 2.20. Оголошення змінної, на яку будуть записуватися відскановані для збігу відбитки пальців

Використаємо рядок безпосереднього впливу на Arduino. У даному рядку показано, що з 12 pin буде виходити ток. Тобто дана конструкція працює, як транзистор. При поданні току з 12 pin коло замикається, що приводить до подачі

току на замок, включається електромагніт, який притягує до себе язичок замку. На рис. 2.21. представлено рядок безпосереднього ввпливу.

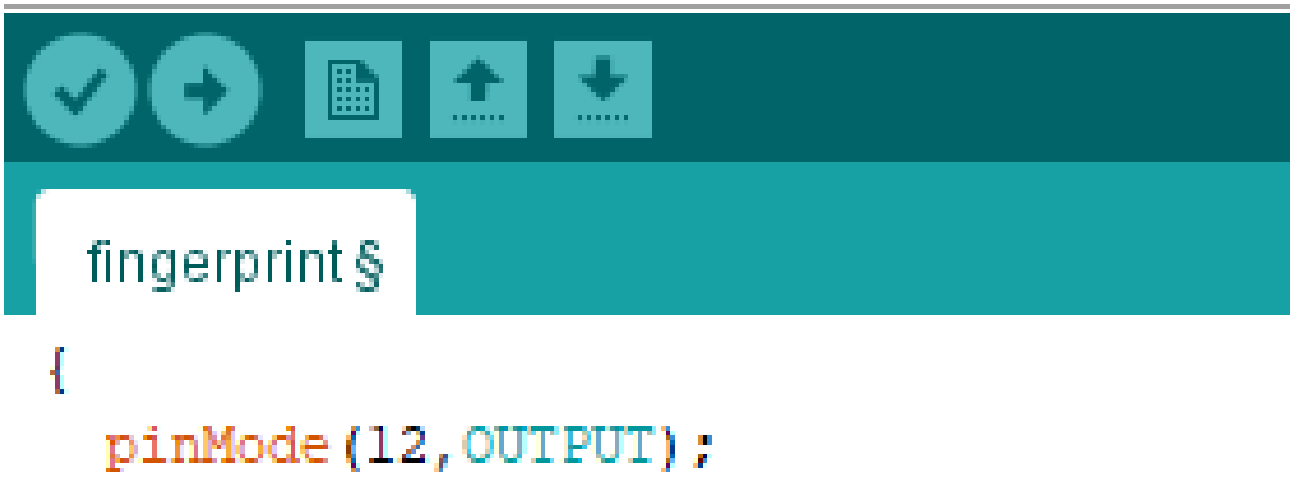

Рис. 2.21. Рядок безпосереднього ввпливу

Ініціалізацуємо сенсор (перевіримо роботоспроможність датчиків) вбудованими бібліотеками Arduino. На рис. 2.22. можливо побачити ініціалізацію сенсору.

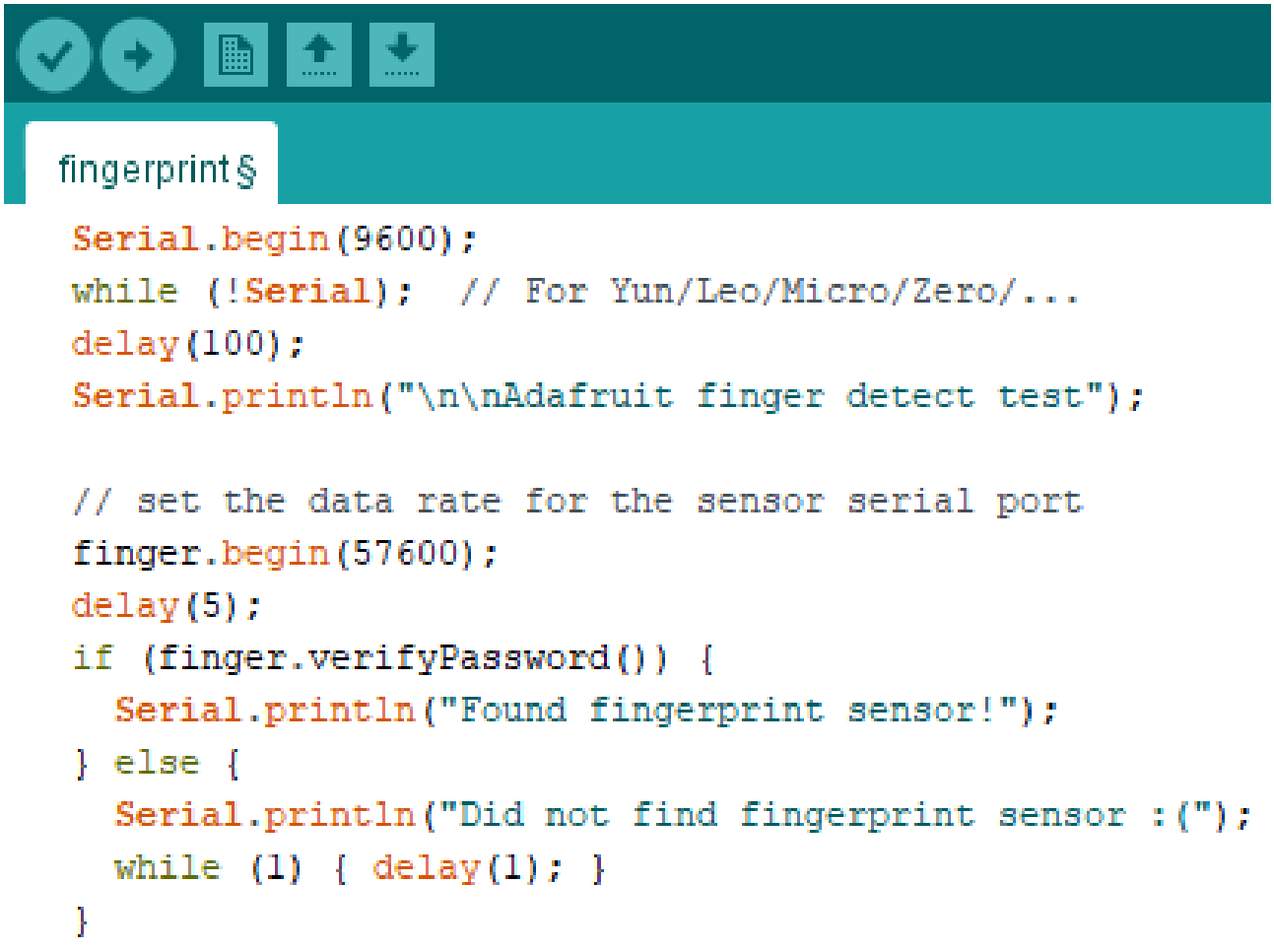

Рис. 2.22. Ініціалізація сенсору вбудованими бібліотеками Arduino

Виведемо на екран основні характеристики сенсору. На рис 2.23. зображено виведення на екран основних характеристик сенсору.

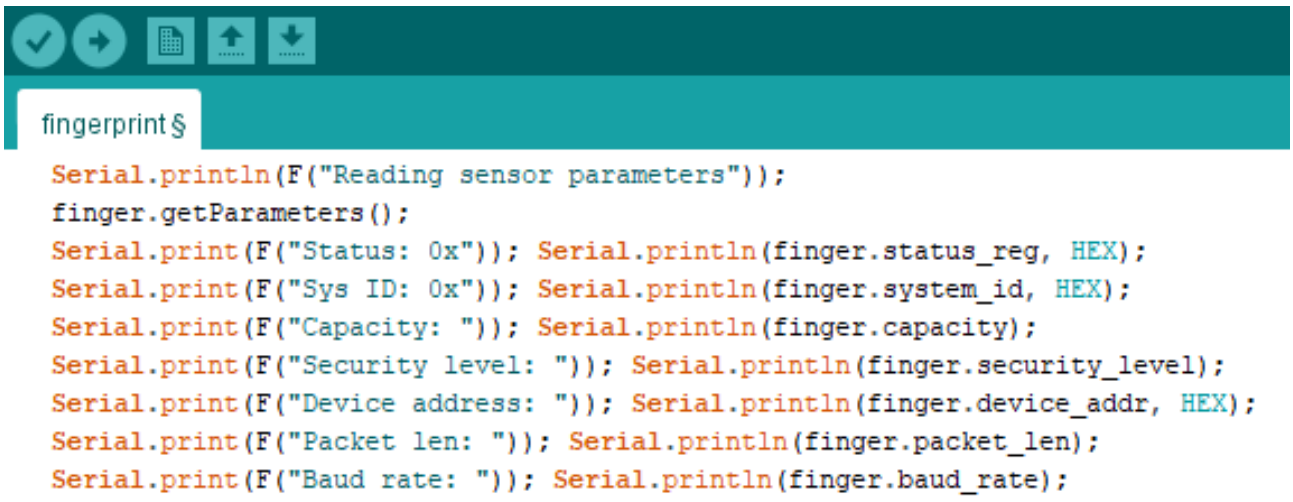

Рис. 2.23. Виведення на екран основних характеристик сенсору

Проводемо перевірку на наявність відбитків пальців у пам'яті сенсору. При відсутності даних у пам'яті, робимо зауваження про дану відсутність та просимо повторно зареєструвати відбитки, у іншому випадку виводимо на екран інформацію про наявність даних у пам’яті. На рис. 2.24. Зображено перевірку на наявність відбітків пальців у пам’яті сенсору.

Рис. 2.24. Перевірку на наявність відбітків пальців у пам’яті сенсору

Реалізуємо функцію, що чекає на відбиток пальця, призначеного для первірки на збіг з наявними. На рис. 2.25. зображено функцію, що чекає на відбиток пальця.

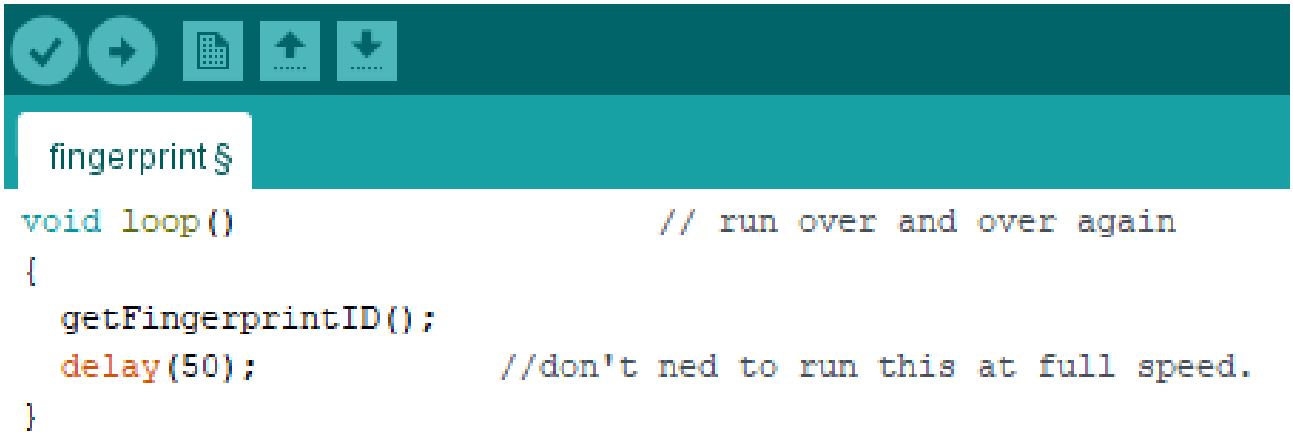

Рис. 2.25. Функція, що чекає на відбиток пальця

Зчитуємо відбиток пальця для подальшої роботи. Реалізуємо перевірки можливих помилок та успішно завершених дій серед яких: «зроблено зображення», «не виявлено пальця», «помилка зв’язку», «помилка зображення», «невідома помилка». Реалізація даної перевірки показана на рис. 2.26.

fingerprint §

```
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;
}
```

Рис. 2.26 Перевірки можливих помилок та успішно завершених дій при зчитуванні пальця

Перетворюємо зчитуваний шаблон до необхідного нам формату малюнку. Реалізуємо перевірки можливих помилок та успішно завершених дій серед яких: «зображення занадто брудне», «помилка зв’язку», «не вдалося знайти

особливості відбитку пальця», «невідома помилка». Реалізація даної перевірки показана на рис. 2.27.

fingerprint §

```
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;
}
```

Рис. 2.27 Перевірки можливих помилок та успішно завершених дій при перевторенні малюнку відбитка пальця до необхідного формату

Шукаємо шаблон серед збережених у пам'яті сенсору. При знайденні відповідності реалізуємо подачу току на 12 pin, чекає дві секунди на вимикаємо подачу току. Реалізація функції пошуку шаблону серед збережених зображено на рис. 2.28.

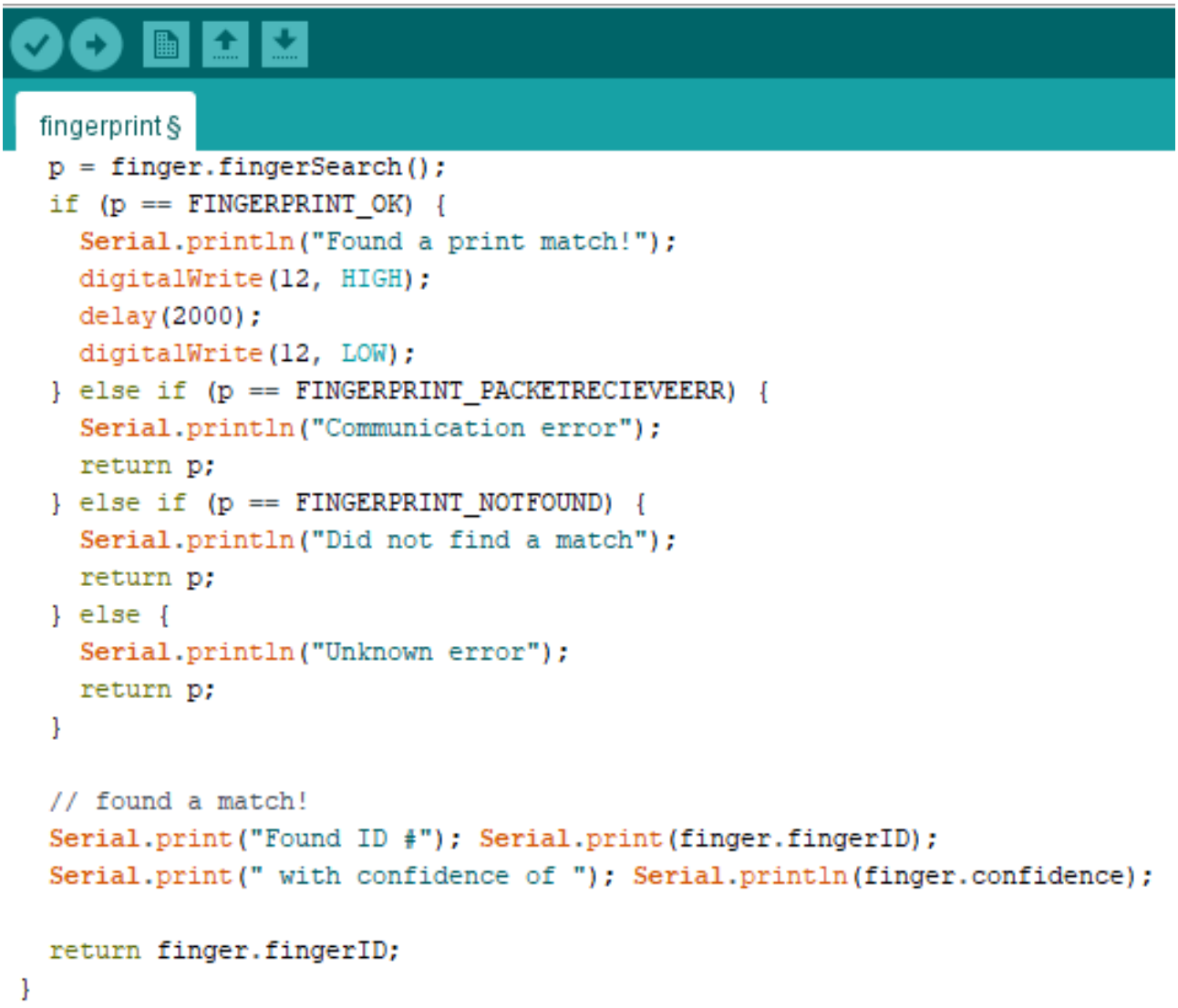

Рис. 2.28. Реалізація функції пошуку шаблону серед збережених

Проводимо повторну перевірку на помилки. Якщо помилка існує та не підпадає під описані вище, то завершуємо програму достроково. Реалізація повторної перевірки на помилки зображено на рис. 2.29.

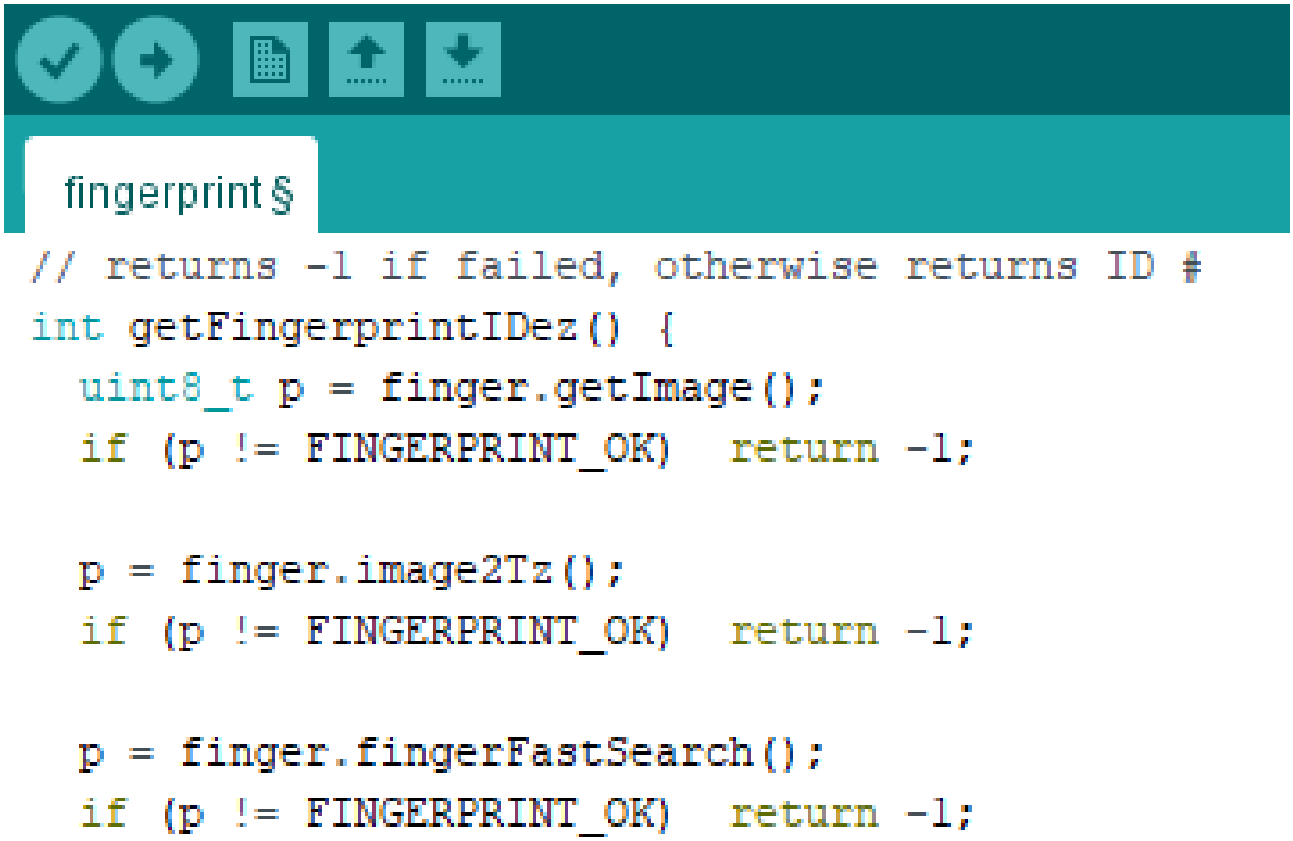

Рис. 2.29. Повторна перевірка на помилки

Виводимо ID збереженого відбитку пальця, який співпадає зі зчитуваним відбитком пальця. Реалізацію виведення ID збереженого відбитку пальця зображено на рис. 2.30.

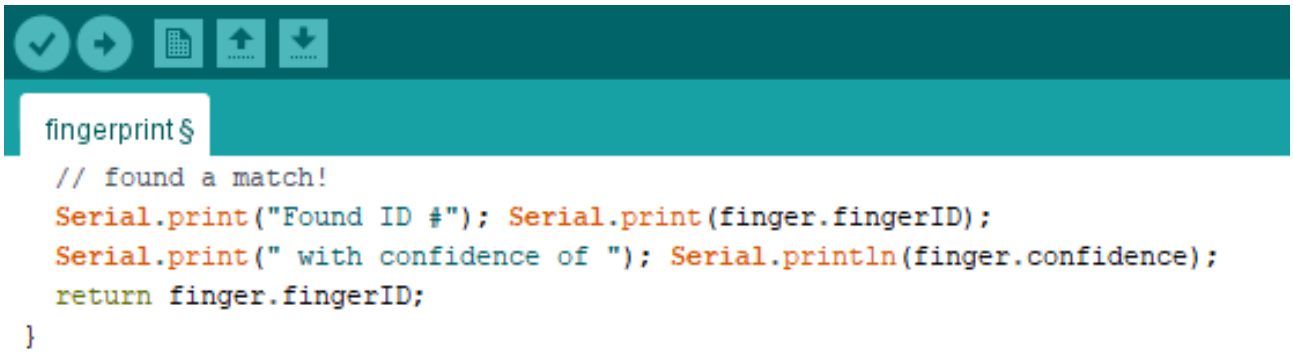

Рис. 2.30. Виведення ID збереженого відбитку пальця

Результатом програми fingerprint.ino є успішно реалізований алгоритм, який дозволяє зчитувати відбиток пальця зі сканера та шукати збігі у базі

моделей відбитків пальців у пам’яті сенсора. На рис. 2.31, рис. 2.32, рис. 2.33. зображені помилки та успішно реалізовані дії програми fingerprint.ino.

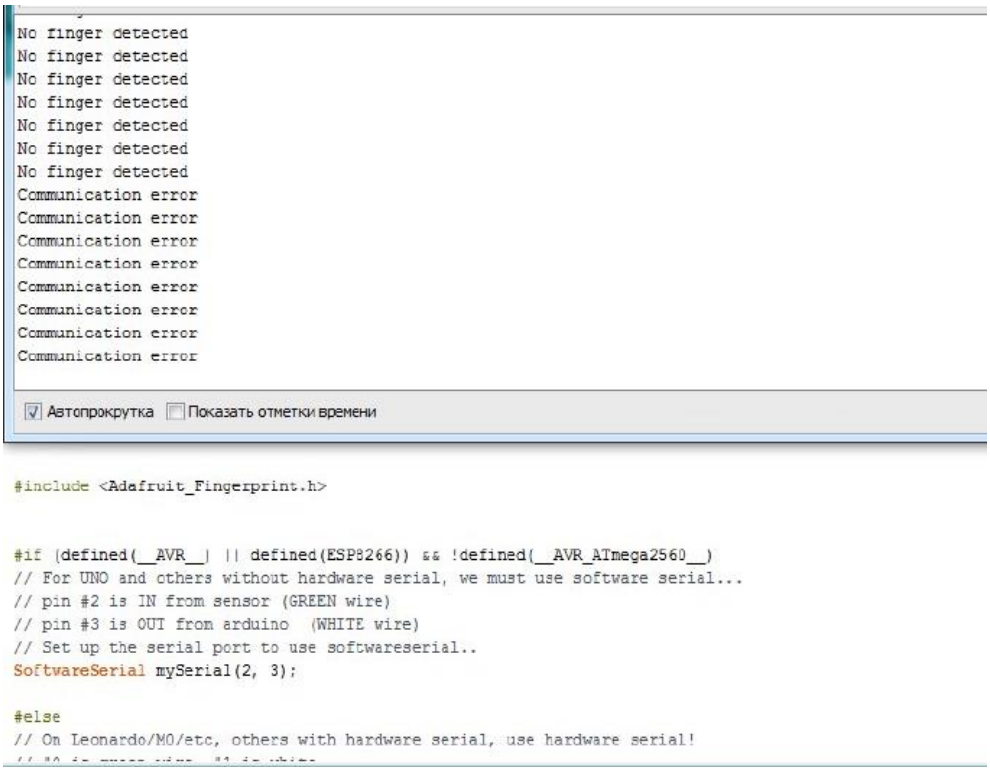

Рис. 2.31. Відповідь програми «Помилка з’єднання»

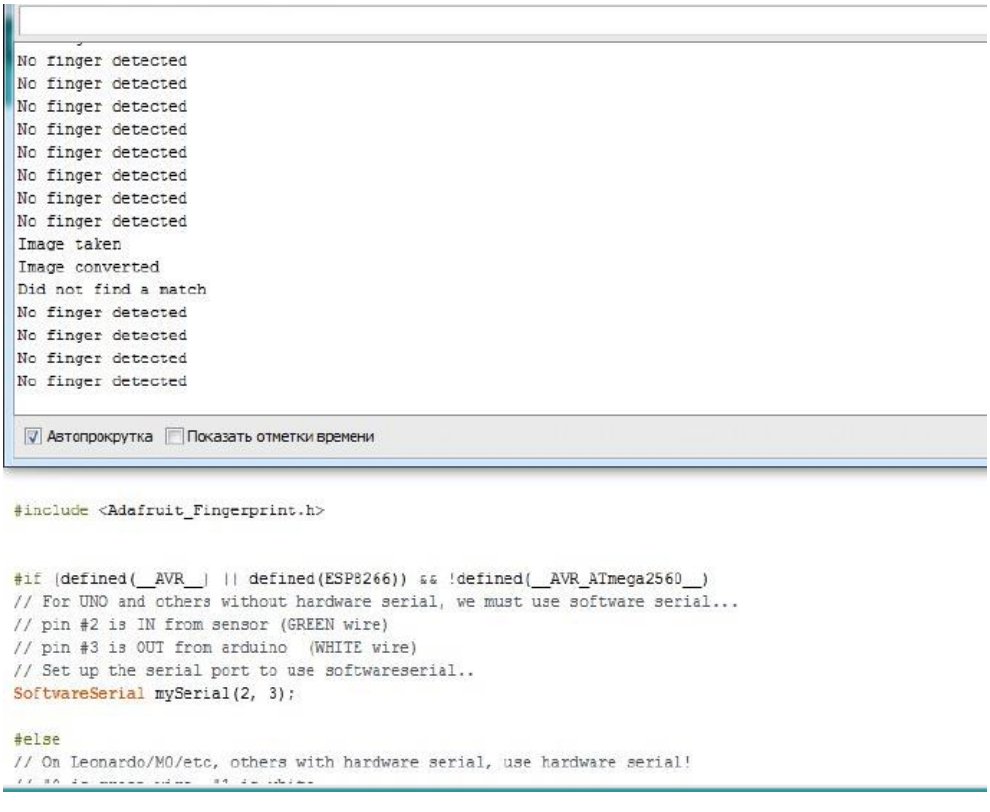

Рис. 2.32. Відповідь програми «Помилка розпізнавання»

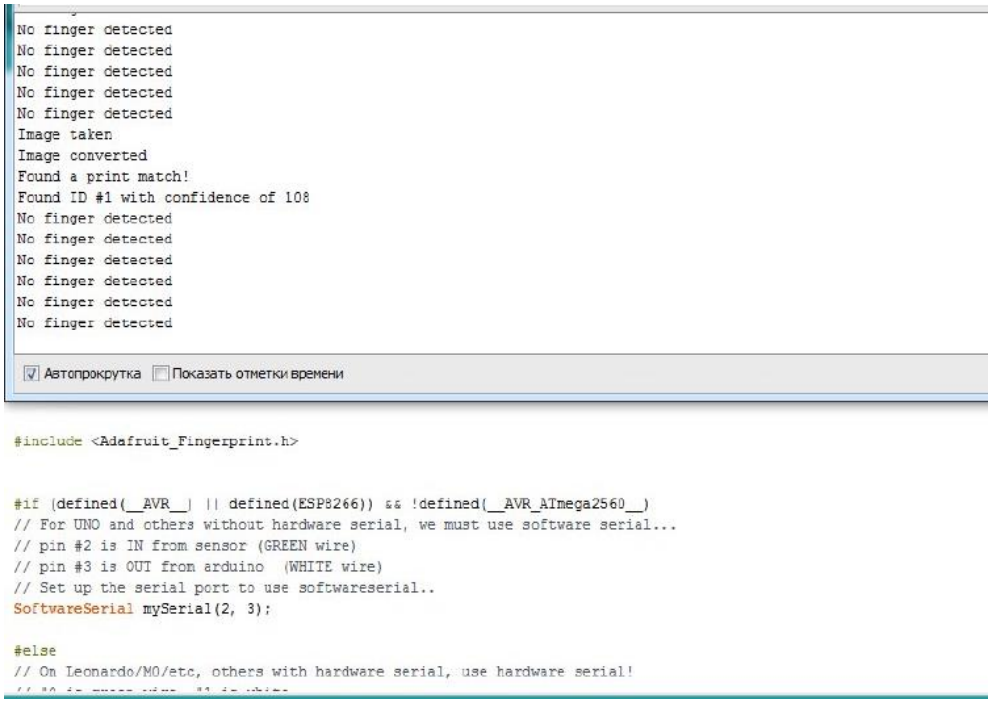

Рис. 2.33. Відповідь програми «Успішне завершення»

На рис. 2.34. зображений початковий стан системи за відсутності відбитку пальця на сканері, замок закритий.

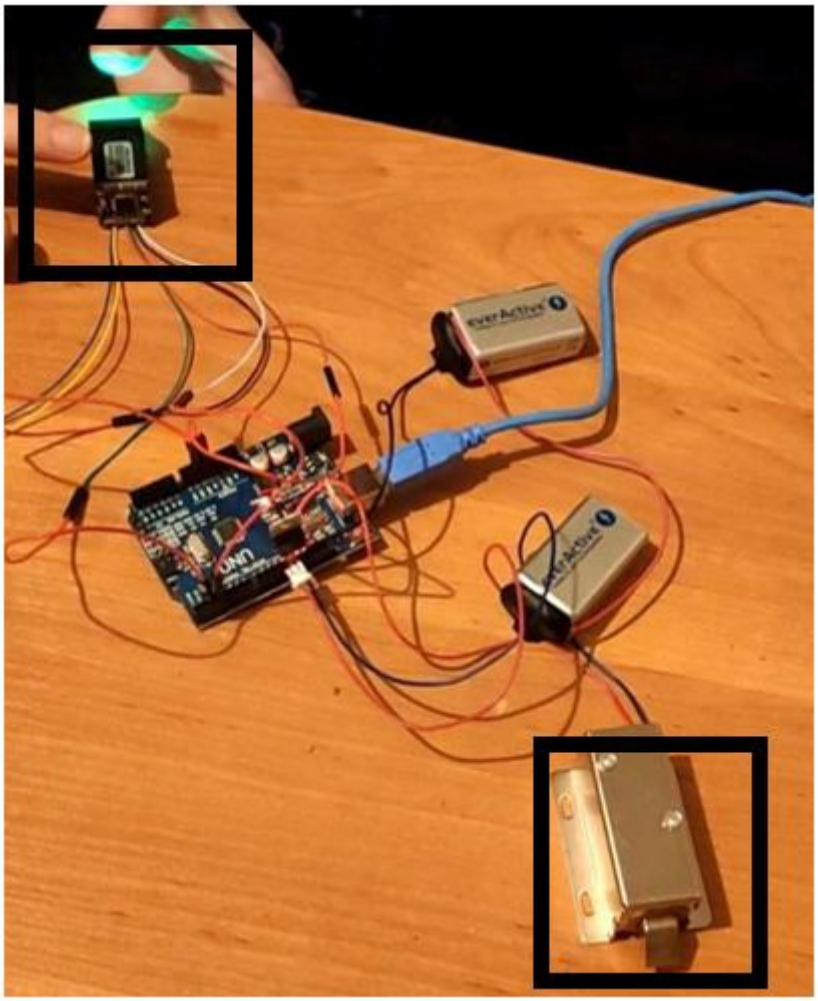

Рис. 2.34. Початковий стан системи за відсутності відбитку пальця на сканері

На рис. 2.35. Кінцевий стан системи за присутності коректного відбитку пальця на сканері, замок відкритий.

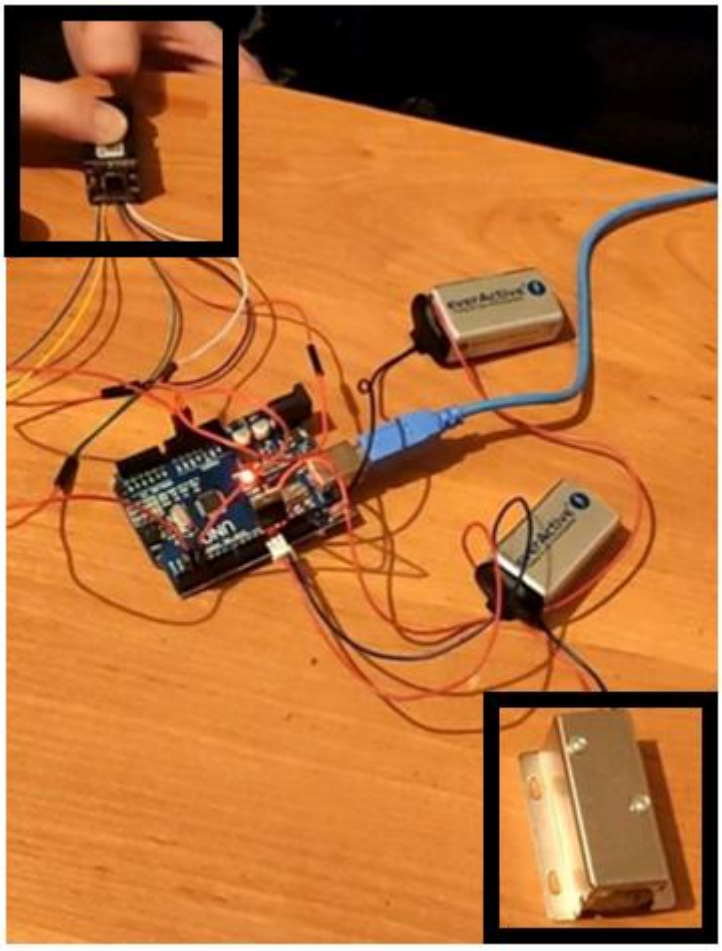

Рис. 2.35. Кінцевий стан системи за присутності коректного відбитку пальця на сканері

Висновки до розділу 2

У другому розділі за допомогою середовища програмування Arduino.ide було реалізовано систему розблокування електронного пристрою з дактилоскопічним захистом. Дана система була реалізована за допомогою двох програм: enroll.ino, fingerprint.ino.

У рамках першої програми було реалізовано зчитування відбитків пальців та перетворення відбитків пальців на модель для подальшого зчитування та пошуку збігів відбитків пальців.

У рамках другої програми було реалізовано зчитування ймовірно правдивого відбитку пальця, пошук співпадіння з існуючим шаблоном, відповідь про співпадіння або неспівпадіння відбитку пальця та розблокування або нерозблокування електронного замка.

ВИСНОВКИ

Результатом виконаної роботи є вирішення задачі побудови системи розблокування електронного пристрою з дактилоскопычним захистом.

У процесі виконання роботи отримані наступні результати:

1. Проведено аналіз існуючих стандартів в сфері біометричної ідентифікації в Україні, Європі та Сполучених Штатах Америки; проведено аналіз існуючих методів біометричної ідентифікації; проведено аналіз існуючих сканерів відбитків пальців.

2. У процесі створення системи розблокування електронного пристрою з дактилоскопічним захистом було використано Arduino. Arduino - це електронна платформа з відкритим кодом, заснована на простому у використанні апаратному та програмному забезпеченні. Для використання плати необхідно надіслати набір інструкцій мікроконтролеру на платі. Для цього використовується мова програмування Arduino (на основі підключення) та програмне забезпечення Arduino (IDE) на основі обробки.

3. Розроблено алгоритми та програмне забезпечення з використанням середовища програмування Arduino.ide для створення системи розблокування електронного пристрою з дактилоскопічним захистом. Перша програма (enroll.ino) використовується для зчитування, завантаження та зберігання відбитків пальців у пам’яті сенсору для можливості подальшої перевірки на збіг нових відсканованих відбитків пальців з моделями, які завантажені до пам’яті сенсору. Дана програма використовується одноразово, оскільки плата Arduino може працювати лише з однією програмою. Друга програма (fingerprint.ino) використовується безпосередньо для перевірки на збіг нових відсканованих відбитків пальців з моделями, які завантажені до пам’яті сенсору. Дана програма завантажується другою та є активною увесь час.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ПОСТАНОВА від 27 грудня 2017 р. N 1073 Про затвердження Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства
2. Проект Закону вноситься народним депутатом України О. І. Тищенком (N 481) ЗАКОН УКРАЇНИ «Про ідентифікацію людини шляхом дактилоскопії»
3. БІОМЕТРИЧНІ СИСТЕМИ ІДЕНТИФІКАЦІЇ ЛЮДИНИ [Електронний ресурс] – Режим доступу до ресурсу: http://confopcb.iee.kpi.ua/proc/article/download/114924/109370.
4. АНАЛІЗ ЕФЕКТИВНОСТІ ТА НАДІЙНОСТІ МЕТОДІВ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ [Електронний ресурс] – Режим доступу до ресурсу: http://www.rusnauka.com/1_NIO_2011/Medecine/77655.doc.htm.
5. Біометрична ідентифікація обличчя [Електронний ресурс] – Режим доступу до ресурсу: https://studlib.info/tehnologii/1001519-iii-biometrichnaidentifikaciya-oblichchya/.
6. How fingerprint scanners work: optical, capacitive, and ultrasonic variants explained [Електронний ресурс] – Режим доступу до ресурсу: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/.
7. FINGERPRINT RECOGNITION [Електронний ресурс] – Режим доступу до ресурсу: http://www.biometric-solutions.com/fingerprint-recognition.html.
8. Fingerprint Scanners [Електронний ресурс] – Режим доступу до ресурсу: https://computer.howstuffworks.com/fingerprint-scanner3.htm.
9. Fingerprint Scanner [Електронний ресурс] – Режим доступу до ресурсу: https://www.360biometrics.com/faq/fingerprint_scanners.php08.html.
10. Современные технологии идентификации личности по отпечатку пальца с использованием емкостных датчиков [Електронний ресурс] -

Режим доступу до ресурсу: http://www.radioradar.net/articles/scientific_technical/identif_otpech.html

11. Arduino Language Reference [Електронний ресурс] – Режим доступу до ресурсу: http://www.arduino.cc/en/Reference/HomePage
12. Петин В.А. Проекты с использованием контроллера Arduino. – СанктПетербург, 2014. с. 25.
13. Засіб захисту персональних даних від несанкціонованого доступу/ Барсукова О. С.//МАТЕРИАЛИ ЗА XVI МЕЖДУНАРОДНА НАУЧНА ПРАКТИЧНА КОНФЕРЕНЦИЯ ДИНАМИКАТА НА СЪВРЕМЕННАТА НАУКА – 2020, 15 – 22 ЮЛИ 2020. С. 72-74
14. СИСТЕМА РОЗБЛОКУВАННЯ ЕЛЕКТРОННОГО ПРИСТРОЮ З ДАКТИЛОСКОПІЧНИМ ЗАХИСТОМ/ Барсукова О. С., канд. техн. наук Єлізаров А. Б.// MATERIŁY XVI MIĘDZYNARODOWEJ NAUKOWIPRAKTYCZNEJ KONFERENCJI NAUKA I INOWACJA – 2020, 07 - 15 października 2020 roku, Przemyśl Nauka i studia 2020. c. 64-6