

Міністерство освіти і науки України

**Державний заклад
«Південноукраїнський національний педагогічний університет
імені К. Д. Ушинського»**

**Проект «Норвегія-Україна.
Професійна адаптація. Інтеграція в державну систему» (NAPUSS)
Професійна перепідготовка військовослужбовців,
ветеранів та членів їхніх сімей в Україні**

МЕНЕДЖМЕНТ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Навчальний посібник

Випуск 10

Одеса 2021

УДК 378+373.61+33
М 50

Укладачі:

Музиченко Г. В., Доброва Т. Г., Полуяктова О. В., Личковська М. Р., Дуковська І. М.,
Філатова Н. В., Бобро О. В., Тронько С. П., Корабльов В. А., Мазурок Т. Л

Головний укладач:

Полуяктова О. В.

Рецензенти:

Коляда Т. А. – кандидат економічних наук, доцент кафедри фінансів імені Л. Л. Тарангул Університету Державної фіскальної служби України;

Матюк Т. В. – кандидат економічних наук, доцент кафедри економіки та підприємництва ОНУ імені І. І. Мечникова

Рекомендовано до друку рішенням Вченої ради
ДВНЗ «Південноукраїнський національний педагогічний університет
імені К. Д. Ушинського»
(протокол № 11 від 29.04.2021 р.)

М 50 **Менеджмент підприємницької діяльності** : навч. посіб. для професійної підготовки військовослужбовців ЗС України звільнених у запас. Проєкт «Норвегія-Україна». – Вип. 10 , 2021. – Одеса : Видавничий дім «Гельветика» – 2021. – 240 с.

ISBN 978-966-992-467-4

ISBN 978-966-992-467-4

© ДВНЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», 2021
© Проєкт «Норвегія-Україна», 2021

ЗМІСТ

ПЕРЕДМОВА	6
<i>Музиченко Г. В.</i> СТАРТАП: СУЧАСНЕ ВИЗНАЧЕННЯ ТА РОЛЬ В РОЗВИТКУ ЕКОНОМІКИ	7
<i>Доброва Т. Г., Полуяктова О. В.</i> БІЗНЕС-ПЛАНУВАННЯ ЯК ПЕРЕДУМОВА УСПІШНОЇ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ	29
<i>Личковська М. Р.</i> МЕНЕДЖМЕНТ СТВОРЕННЯ ТА РОЗВИТКУ МАЛОГО ПІДПРИЄМСТВА	59
<i>Дуковська І. М.</i> ВІДОКРЕМЛЕНІ ПІДРОЗДІЛИ В ДІЯЛЬНОСТІ ЮРИДИЧНОЇ ОСОБИ	184
<i>Філатова Н. В.</i> РЕСУРС, ЩО ЗАВЖДИ З ТОБОЮ, ЦЕ – ТИ САМ!	188
<i>Філатова Н. В.</i> УКРАЇНСЬКІ ПОЕЗІЇ ЯК ПСИХОЛОГІЧНИЙ РЕСУРС ОСОБИСТОСТІ	213
<i>Бобро О. В., Тронько С. П.</i> ВИЗНАЧЕННЯ ПРЕВЕНТИВНИХ ДІЙ У СТРЕСОВИХ СИТУАЦІЯХ	227
<i>Корабльов В. А., Мазурок Т. Л</i> ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ В КОМЕРЦІЙНІЙ ДІЯЛЬНОСТІ	234



*Корабльов В. А.,
ст. викладач кафедри прикладної математики
та інформатики*



*Мазурок Т. Л.,
д. т. н., кафедра прикладної математики та інформатики*

ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ В КОМЕРЦІЙНІЙ ДІЯЛЬНОСТІ

Розробка програми контролю доступу на основі розпізнавання обличчя Аналіз та практичні засади розпізнавання обличчя

За останні кілька років стало необхідно мати надійну систему безпеки, яка може захистити наші активи найкращим та найбезпечнішим способом.

Традиційні системи безпеки вимагають від користувача ключ, пароль безпеки, RFID-картку або ID-картку, щоб мати доступ до системи. Однак у цих систем безпеки є недоліки, наприклад, їх можна забути або вкрасти. В результаті виникає потреба у розробці програмного забезпечення, що гарантує вищий рівень безпеки. Розпізнавання обличчя – один з найпопулярніших методів біометричних технологій. У порівнянні з іншими біометричними технологіями, такі як відбитки пальців, розпізнавання голосу, та сканування сітківки, розпізнавання обличчя можна розглянути, як більш природний метод. Розпізнавання обличчя також дозволяє отримати доступ для більш ніж одній особі, надаючи привілеї доступу лише певним людям.

У нашому пристрої ми будемо використовувати камеру Pi, яка буде надавати наші вхідні дані у вигляді зображень. Відео трафік буде опрацьований кадрами та збережений. Після збереження зображення будуть перетворені в цифрові зображення. Коли камера сканує особу, яка намагається пройти аутентифікацію, вона порівнює зображення з попередніми, збереженими в базі даних.

Для управління сигналами буде використовуватися обладнання Raspberry, яке пов'язане з магнітним замком. Якщо вхідні дані обличчя будуть розпізнані, система

надішле сигнал про відкриття магнітного замку на 5 секунд, що автоматично заблокується після того. Окрім магнітного замку, ми використовували інші електронні елементи для забезпечення належної роботи пристрою. Ми використовували транзистор TP120, який дозволяє взаємодіяти замку і струму через Raspberry, і резистор 10 кОм, що підключає кнопку, яка приймає сигнал для активації процесу розпізнавання.

Проект був розроблений для використання вдома і для інших системи входу в будівлі, що не обмежує наш проект для використання в інших середовищах, таких як виявлення несанкціонованих людей в службових закладах.

Постановка проблеми.

Системи безпеки з кожним днем стають все важливішими. Ці зміни відбуваються пропорційно до кількості зареєстрованих крадіжок. На основі звітів країн світу, поліція міста Одеса протягом 2019 року налічувала понад 15 725 повідомлень про крадіжки в будинках та інших будівлях, отже, там є потреба у вищому рівні безпеки.

Згадані традиційні системи не є надійними, оскільки вони є можуть бути вкрадені або забуті, наприклад, пароль та посвідчення особи можна забути чи загубити або навіть вкрасти в людини (рис.1).

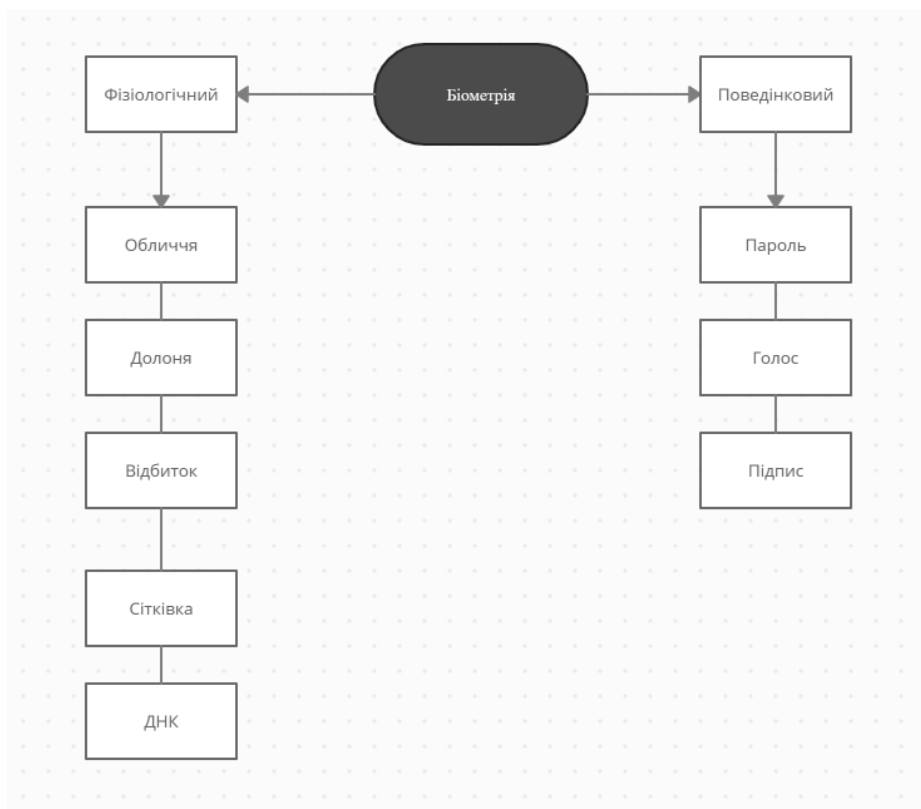


Рис.1. Типи біометричних ключів

Як результат, системи безпеки доступу повинні розвиватися більш безпечним та технологічним шляхом.

Завжди існує потреба усунути традиційні системи «недоліки». Біометричні технології вважається одними з них найбезпечніші та доступних системи аутентифікації, забезпечуючи вищий рівень безпеки, ніж традиційні системи. Вони вважаються таким захищеними, оскільки обличчя не можуть бути викрадені, позичені або підроблені будь-яким способом для отримання вигоди у виді доступу до будівлі.

Ми використовували PCA (аналіз основних компонентів) алгоритм. Ретельно підібрали цей конкретний алгоритм, оскільки він простий у використанні та ефективніший за

інші алгоритми. Використовуючи PCA, ми мінімізували аналіз та необхідний розвиток шляхом аналізу лише деяких подібних зображення з нашої бази даних.

На основі проведеного дослідження ми проілюстрували відмінності між біометричними технологіями. Порівняння було складено на основі 4-хМ факторів: точності, вартості, необхідності обладнання та прийнятність. Ми класифікували ці фактори в три категорії: низький (L), середній (M) та високий (H).

Таблиця 1.

Порівняння біометричних технологій

Метод	Точність	Ціна	Обладнання	Прийнятність
Обличчя	M	L	Камера	M
Долоня	M-L	M	Сканер	M
Відбиток	H	M	Сканер	M
Сітківка	H	H	Сканер	L
ДНК	H	H	Тест	L
Голос	M	M	Мікрофон	H
Підпис	L	M	Планшет	H
Пароль	H	L	Клавіатура	L

У таблиці 1 наведено порівняння між біометричними технологіями. Було порівняно 8 біометричних методів. Можна помітити, що розпізнавання обличчя має середній рівень точності, порівняно з іншими методами. Ця точність може бути вищою коли перевіряються інші функції, такі як фон, освітлення та положення голови. Вартість розпізнавання обличчя дешевше інших методів, що є однією із причини, які ми обрали для розвитку цієї певної системи. Ключовий компонент для розробки такої система – це камера, і звичайно, сервер, який буде навчатися і впізнати обличчя.

В останній категорії прийнятність, порівняно з іншими методами, розпізнавання обличчя показує прийняття середнього рівня. Щоб знизити прийнятність, ми маємо зробив три кроки.

По-перше, ми використовували базу даних AT&T з 90-х, для негативних зображень. Ці зображення навчать нашу система, робити більш точні та правильні вибори на основі нових даних.

Другим кроком було збереження більшої кількості зображень для людини, в різних положеннях. Ми використовували 5 позицій, і для кожної з них ми записали 10 зображень, в результаті – це 50 позитивних 238 ображень на людину.

І останній крок – це зниження рівня прийняття несанкціонованих людей, є зниження позитивної межі. Оскільки наша система видає низький значення для відомих людей (чим нижче значення, тим більше людина надійна), ми спробували використовувати мінімальні значення як позитивний результат для нашої системи. На основі порівняння можемо зробити висновок, що наше система розпізнавання обличчя має шкалу точності понад 62%. Така висока шкала точності була досягнута постійно перевіряючи фон, освітлення та положення голови. Інші речі, які зіграли велику роль у досягненні такої точності – це використання багатьох зображень для розпізнавання, використовуючи існуючу базу даних із зображеннями що допомагає системі стати більш розумною та використання мінімальних значень, як умова для авторизації нових людуй, які намагаються отримати доступ до будівлі.

Апаратне забезпечення для системи захисту

Для реалізації такого проекту головним і найважливішим кроком було пошук обладнання, яке буде використано для пристрою. Елементами, які використовує наш пристрій, є (рис. 2):

- Raspberry Pi 3 B

- Мікроконтролер
- Камера Pi 5MP
- магнітний замок
- TIP120
- Транзистор
- Резистор 10 кОм
- Кнопка
- Монтажна плата

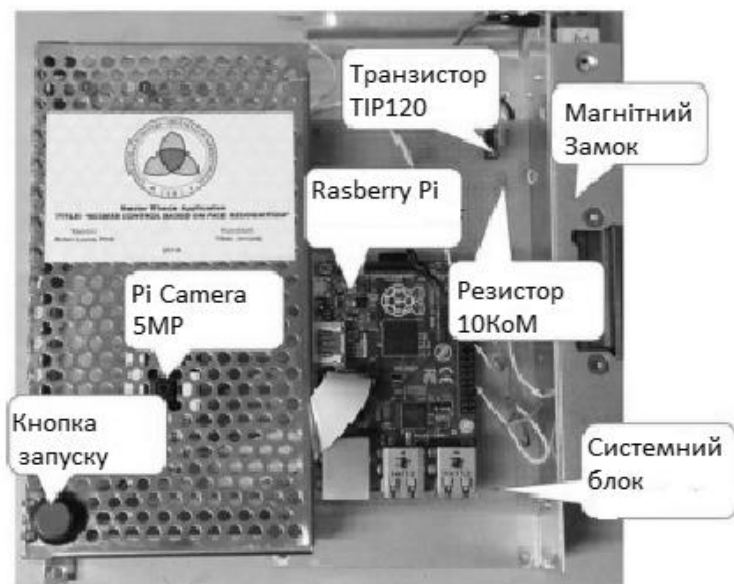


Рис. 2. Схема Raspberry Pi 3 B

Було обрано мікроконтролер Raspberry Pi B для використання у даному пристрої. Ми провели багато досліджень і порівняли елементи в різних мікроконтролерах, наприклад, вартість, обробка, та зручність користування. Основні причини, чому був обраний цей специфічний міні-комп'ютер – це висока обробна здатність, відносно низька ціна та його здатність адаптуватися під різні режими програмування. Пристрій використовує Linux як операційну систему, яка має доступ до великої кількості бібліотек і програм, сумісних з Raspberry (рис. 3).

Плата побудована на базі SoC Broadcom BCM2711, яка містить чотири 64-розрядних ядра ARM Cortex-A72 з тактовою частотою 1.5 ГГц. На відміну від будь-якої попередньої плати, Raspberry Pi 4 Model B доступна в трьох різних моделях, кожна з яких пропонує різні варіанти пам'яті з 1 ГБ, 2 ГБ, 4 ГБ або 8 ГБ LPDDR4 SDRAM оперативної пам'яті.

Найбільш помітне відміну від попередніх моделей полягає в тому, що на новій платі відсутня мікросхема LAN7515, яка виконувала функції USB і Ethernet. На його місці VLI VL805, яка забезпечує USB 3.0 Hub через шину PCI Express. Використання шини PCI Express, що надається новим BCM2711, означає, що тепер є не тільки можливість USB 3.0, але і Gigabit Ethernet, який тепер надається з використанням Broadcom BCM54213PE окремо від USB. Бездротовий зв'язок забезпечується тим же чіпом Cypress CYW43455, який ми бачили на Raspberry Pi 3 модель B+. Пропонується двухдиапазонная бездротова мережа IEEE 802.11.b / g / n / ac 2,4 ГГц і 5 ГГц, а також Bluetooth 5.0 і Bluetooth LE.

Ще одним великим відмінністю є роз'єм живлення, відсутній роз'єм micro-USB від попередніх моделей, а на його місці роз'єм USB-C. Raspberry Pi 4 Model B може знадобитися до 3 А, що не могло забезпечити попередній джерело живлення через micro-USB.

4-я модель може харчуватися і від джерела постійного струму 5 В через роз'єм GPIO і, як і Raspberry Pi 3 Model B +, від Power over Ethernet (PoE) з використанням офіційної PoE HAT, випущеної раніше поряд з попередньою моделлю.

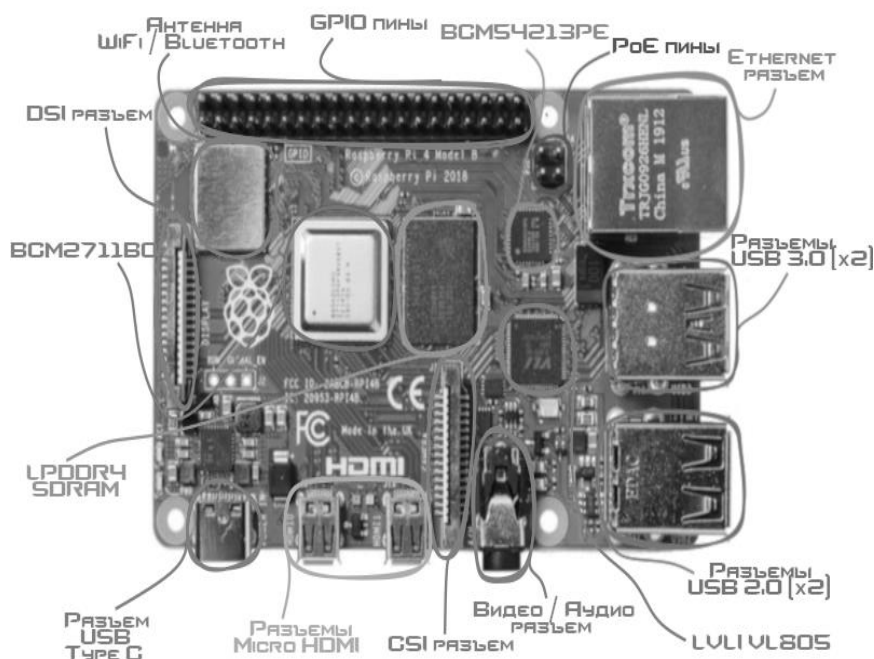


Рис. 3. Схема Raspberry Pi 3 B

Також змінено відео порти. Відсутня повнорозмірне гніздо HDMI, на його місці два порти micro-HDMI, це означає, що новий Raspberry Pi 4 Model B має підтримку двох моніторів – одного екрану в 4K зі швидкістю 60 кадрів в секунду або двох екранів 4K зі швидкістю 30 кадрів в секунду. Поруч з двома портами місто-HDMI є 4-полосний стереовиход і композитний відеороз'єм.

Поряд з великими змінами деякі речі не змінилися. Зберігання і раніше забезпечується картою Micro-SD з роз'ємом в звичному місці на нижньому боці плати. Як і раніше підтримує роз'єм порту дисплея MIPI DSI і роз'єм камери MIPI CSI, а також стандартний 40-контактний роз'єм GPIO. Однак є деякі зміни для 40-контактного роз'єму, хоча він все ще сумісний. Роз'єм нового Raspberry Pi має підтримку додаткових роз'ємів 4 × UART, 4 × SPI і 4 × I2C.

Для нашого пристрою ми вибрали камеру Raspberry Pi, яку можна інтегрувати безпосередньо в мікроконтролер. Це підключення здійснюється через CSI (послідовний інтерфейс камери) шину, яка пропонує надзвичайно високу віддачу даних, у нашій справі, передача пікселів зображення. Її розміри 25 мм x 20 мм, і вагою всього 3 г, це робить дуже сумісною для нашого проекту. Ця камера має 5-мегапіксельний сенсор пропонує статичні зображення з роздільною здатністю 2592x1944 пікселів, та відео з роздільною здатністю 1080p30 та 720p60.

Транзистор TIP120 використовувався для управління струмом, який надходить магнітний замок. Так як магнітний замок отримує струм безпосередньо ззовні, необхідно використовувати цей транзистор для управління струмом через мікроконтролер. TIP120 – це транзистор, який має 3 головні частини, основу, колектор та емітер. Основний шлейф підключається безпосередньо до мікроконтролера, а коли додаток розпізнає обличчя, воно посиляє сигнал на транзистор протягом 5 секунд, де також знаходиться зв'язок з магнітним замком. Через 5 секунд, сигнал, надісланий в основі транзистора, зупиняється, і не дозволяють направляти струм на магнітний замок.

Резистор 10КΩ використовується для стабілізації схеми. Як згадано раніше, мікроконтролер має ніжки, які використовуються для прийому сигналів. У нашому випадку головні ніжки будуть записувати зображення, коли людина стикається з камерою. Сигнал має напругу 3В, тому необхідно використовувати цей вид резистора для стабілізації напруги в ланцюзі. Він має опір 10 кОм та потужність 0,25 Вт з допуском від 1%.

Висновки

Протягом нашого проекту ми пояснювали реалізацію програми, яка контролюватиме доступ до будівлі. Ми бачили, як рівень точності вищий, коли такі фактори, як: фон, освітлення та кількість зображень контролюються. Ми помітили, що якщо контролювати всі фактори, рівень точності буде вищим. Тому, як висновок, бажано контролювати такі фактори, як фон, освітлення та мати принаймні 50 зображень для людини, враховуючи, що пристрій має достатньо пам'яті. Якщо вам вдається контролювати всі фактори, наша система пропонує точність 62%.

Першою метою нашого проекту було навчання та ідентифікація у вбудованих пристроях. Хоча наш пристрій може проводити навчання та ідентифікацію самостійно, не підключаючись до жодної іншої машини, ми робимо висновок, що наша мета була досягнута. Оскільки ми знаємо, що на ринку існує багато подібного обладнання, але ми вирішили реалізувати такий вид додатків з огляду на вартість. На основі порівнянь наше обладнання пропонується за нижчою ціною, ніж комерційне обладнання.

Другою метою нашого проекту була реалізація програми розпізнавання облич з використанням алгоритму РСА (Principal Component Analysis). Цей конкретний алгоритм дуже підходить і швидко. Його використання дозволяє зменшити кількість зображень у нашій базі даних. Крім того, використання цього алгоритму дозволяє нам використовувати прості камери, які пропонуються за низькою ціною. В результаті ми можемо зробити висновок, що наша мета – впровадити систему розпізнавання облич за допомогою РСА (аналіз основних компонентів) була досягнута.

ЛІТЕРАТУРА

1. Nazeer S. A., Omar N., and Khalid M. «Face Recognition System using Artificial Neural Networks Approach» International Conference on Signal Processing, Communications and Networking. ICSCN. 2007. 420-425, 22-24 February 2007 <http://dx.doi.org/10.1109/icscn.2007.350774>.
2. Liu S. and Silverman M. «A Practical Guide to Biometric Security Technology» IT Professional, 27-32, 2001. <http://dx.doi.org/10.1109/6294.899930>
3. Jain A. K., Ross A. and Prabhakar S. «An Introduction to Biometric Recognition» IEEE Transaction on Circuits and System for Video Technology, 4-20, 2004.
4. Faundez-Zanuy M. «Biometric Security Technology» IEEE Transaction on Aerospace and Electronic System, 15-26, 2006. <http://dx.doi.org/10.1109/MAES.2006.1662038>
5. Kar S., Hiremath S., Joshi D. G., Chadda V.K. and Bajpai A. «A MultiAlgorithmic Face Recognition System» International Conference on Advanced Computing and Communication, 321-326, 2006.
6. Agarwal M., Agarwal H., Jain N. and Kumar M. «Face Recognition Using Principle Component Analysis, Eigenface and Neural Network» International Conference on Signal Acquisition and Processing, 310-314, 2010. <http://dx.doi.org/10.1109/icsap.2010.51>
7. Riddhi C., and Neha P. «Details Study on 2D Face Recognition Technique Using Local and Global Features» Indian Streams Research Journal, 1-17, 2013.
8. Juwei L., Plataniotis K.N. and Venetsanopoulos A.N. «Regularization Studies of Linear Discriminant Analysis in Small Sample Size Scenarion with Application to Face Recognition» Pattern Recognition Letter, 181-191, 2005.
9. Xueguang, W. and Xiaowei D. «Study on Algorithm of Access Control System Based on Face Recognition» International Colloquium on Control and Management, 336-338, 2009.