
UNIVERSITATEA „SAPIENTIA” DIN CLUJ-NAPOCA
FACULTATEA DE ȘTIINȚE TEHNICE ȘI UMANISTE,
TÎRGU-MUREȘ
SPECIALIZAREA CALCULATOARE

Sistem control acces cu modul de cameră ESP32

LUCRARE DE DIPLOMĂ

Coordonator științific:
dr.ing. Kutasi Dénes Nimród
dr.ing. Szabó László Zsolt

Absolvent:
Olosz Izabella-Noémi

2023

UNIVERSITATEA „SAPIENTIA” din CLUJ-NAPOCA
Facultatea de Științe Tehnice și Umaniste din Târgu Mureș
Specializarea: **Calculatoare**

Viza facultății:



LUCRARE DE DIPLOMĂ

Coordonator științific:
**conf. dr. ing. Kutasi Dénes Nimród, ș.l. dr.
ing. Szabó László Zsolt**

Candidat: **Olosz Izabella-Noémi**
Anul absolvirii: **2023**

a) Tema lucrării de licență:

Sistem control acces cu modul de cameră ESP32

b) Probleme principale tratate:

- Utilizarea ESP Cam într-o aplicație control acces
- Studiu bibliografic și alegere algoritm de recunoaștere față umană
- Realizarea unui sistem de control acces

c) Desene obligatorii:

- Schema bloc al aplicației
- Diagrame UML privind software-ul realizat.

d) Softuri obligatorii:

- Software pentru modul camera ESP32
- Aplicație web pentru supervizarea sistemului control acces
- Modul pentru recunoaștere fețe

e) Bibliografia recomandată:

- J. Anil K.-Patrick Flynn-Arun A. Ross. Handbook of Biometrics. 2008
- Halim, Muhammad Arif Azhari, et al. Face Recognition-based Door Locking System with Two-Factor Authentication Using OpenCV. 2021 Sixth International Conference on Informatics and Computing (ICIC). IEEE, 2021.
- Agus Kurniawan Developing IoT Projects with ESP32, Packt 2021

f) Termene obligatorii de consultații: săptămânal

g) Locul și durata practicii: Universitatea „SAPIENTIA” din Cluj-Napoca,
Facultatea de Științe Tehnice și Umaniste din Târgu Mureș

Primit tema la data de: 31.03.2022

Termen de predare: 27.06.2023

Semnătura Director Departament



Semnătura coordonatorului



Semnătura responsabilului
programului de studiu



Semnătura candidatului



Declarație

Subsemnata/ul Olosz Izabella-Noémi, absolvent(ă) al/a specializării Calculatoare, promoția 2023 cunoscând prevederile Legii Educației Naționale 1/2011 și a Codului de etică și deontologie profesională a Universității Sapientia cu privire la furt intelectual declar pe propria răspundere că prezenta lucrare de licență/proiect de diplomă/disertație se bazează pe activitatea personală, cercetarea/proiectarea este efectuată de mine, informațiile și datele preluate din literatura de specialitate sunt citate în mod corespunzător.

Localitatea,

Absolvent

Data:

Semnătura

Extras

Sistemele de securitate sunt importante atât pentru oameni, cât și instituții în menținerea unui mediu sigur și protejarea bunurilor materiale. Tehnologia modernă ne oferă soluții variate în acest sens. Scopul oricărui astfel de sistem este de a separa intrușii dintre persoanele care au drept de acces. Sistemele de acces oferă o soluție eficientă în timp real pentru acest lucru. Accesul în clădiri este permis doar persoanelor care dețin autorizație adecvată și pot furniza o autentificare validă.

Am ales să abordez în lucrarea mea de diplomă implementarea unui sistem de acces biometric care să identifice oamenii prin recunoaștere facială. Scopul meu a fost de a crea un sistem ușor de utilizat, rapid, eficient și, mai presus de toate, sigur, într-un mod rentabil, pentru a facilita viața oamenilor și pentru a simplifica identificarea persoanelor care doresc să intre în clădiri.

În vederea obținerii unui nivel ridicat de securitate, am ales recunoașterea facială ca metodă de autentificare, o tehnologie cunoscută și utilizată frecvent pentru sistemele informatice sigure, laptopuri, smartphone-uri sau bancomate. În plus față de avantajele sale, trebuie menționat că nu necesită un contact fizic direct în timpul procesului de autentificare și reprezintă o metodă rapidă și eficientă.

Comparativ cu alte metode de autentificare similare, un sistem bazat pe recunoașterea facială este mai sigur și mai dificil de înșelat. Parolele și codurile PIN pot fi ușor obținute sau sparte, cardurile și cheile pot fi pierdute sau furate, ceea ce poate duce la abuzuri în detrimentul măsurilor de securitate. Având în vedere aceste aspecte, am proiectat funcționarea sistemului.

Accesul în clădire este condiționat de adăugarea datelor și fotografiilor persoanelor de către administrator. După îndeplinirea acestei condiții, este permis accesul în clădire. Utilizatorul trebuie doar să se așeze în fața camerei la o distanță corespunzătoare, iar dacă este identificat în sistem, ușa se va deschide, permitându-i să intre. Pentru o utilizare ușoară, am creat și o interfață pentru utilizator, care permite adăugarea simplă a persoanelor și, în scopul urmăririi, lista persoanelor care intră în clădire poate fi vizualizată, împreună cu timpul exact de intrare.

Sistemul implementat de mine facilitează procesul de identificare la intrarea în clădire și oferă o soluție sigură pentru detectarea persoanelor neautorizate în viața de zi cu zi.

SAPIENTIA ERDÉLYI MAGYAR
TUDOMÁNYEGYETEM
MAROSVÁSÁRHELYI KAR
SZÁMÍTÁSTECHNIKA SZAK

Biometrikus beléptető rendszer ESP32-CAM modul segítségével

DIPLOMADOLGOZAT

Témavezető:
dr.ing. Kutasi Dénes Nimród
dr.ing. Szabó László Zsolt

Végzős hallgató:
Olosz Izabella-Noémi

2023

Kivonat

A biztonsági rendszerek az emberek, vállalkozások és intézmények számára egyaránt fontosak a biztonságos környezet fenntartásához és az anyagi javak megóvásához. A mai modern technológia erre változatos megoldásokat nyújt. Minden ilyen rendszernek fő célja kiszűrni az illetéktelen behatolókat a belépő joggal rendelkező emberek közül. A beléptető rendszerek erre egy hatékony valós idejű megoldást kínálnak. Az épületekbe való bejutást csak azoknak a személyeknek teszik lehetővé, akik megfelelő engedéllyel rendelkeznek, tehát hitelesíteni tudják magukat.

A diplomamunkám témájának egy biometrikus beléptető rendszer megvalósítását választottam, ami arcfelismerés segítségével azonosítja az embereket. Célom volt egy könnyen kezelhető, gyors, hatékony és első sorban biztonságos rendszer megvalósítása egy költséghatékony módon, ezzel megkönnyítve az emberek mindennapjait, illetve leegyszerűsítve az épületekbe belépni vágyó személyek azonosítását.

A nagymértékű biztonság érdekében a biometrikus azonosítási módszerek közül az arcfelismerést választottam, ez egy széleskörben ismert és használt technológia, gyakran használják biztonságos számítógépes rendszerekhez, laptopokhoz, okostelefonokhoz vagy bankautomatákhoz. Az előnyei mellett megemlíthető, hogy nem igényel közvetlen fizikai érintést az azonosítás során, illetve gyors és hatékony módszer.

Más hasonló azonosításhoz viszonyítva biztonságosabb, illetve nehezebben átjátszhatóbb egy arcfelismerésen alapuló rendszer. A jelszavak és PIN kódok könnyen kitudódhatnak, feltörhetőek, a különböző kártyák és kulcsok pedig elveszíthetőek vagy ellophatóak, így illetéktelen kezekbe kerülve visszaélés történhet a biztonsági intézkedésekkel szemben.

Ezeket a szempontokat szemelőtt tartva terveztem meg a rendszer működését. A belépéshez feltétel hogy az adminisztrátor hozzáadja a személyek adatait és képeit. Ennek a feltételnek a beteljesülésével belépésre jogosult az épületbe. A felhasználó egyszerűen csak a kamera elé áll, megfelelő ható távolságban és ha megtalálható a rendszerben, akkor kinyílik az ajtó és beléphet. A könnyű használat érdekében létrehoztam egy felhasználói felületet is, amelynek segítségével egyszerűen hozzá lehet adni a személyeket, illetve a követhetőség érdekében megtekinthető az épületbe belépő személyek listája is, pontos belépési idővel együtt.

Az általam megvalósított rendszer megkönnyíti a belépés során az azonosítás folyamatát, és egy biztonságos megoldást nyújt az illetéktelen személyek kiszűrésére a mindennapokban

Kulcsszavak: arcfelismerés, azonosítás, biometria, beléptető rendszer, biztonság

Abstract

Security systems are important for individuals, businesses, and institutions to maintain a secure environment and protect their assets. Modern technology offers various solutions for this purpose. The main objective of such systems is to detect unauthorized intruders among authorized individuals. Access control systems provide an efficient real-time solution to achieve this. They allow entry only to those individuals who have the appropriate permission and can authenticate themselves.

For my thesis, I chose to implement a biometric access control system that utilizes facial recognition to identify individuals. My goal was to create an easily manageable, fast, efficient, and, above all, secure system in a cost-effective manner, thereby simplifying the daily lives of people and streamlining the identification process for individuals seeking entry into buildings.

To ensure a high level of security, I chose facial recognition as the biometric identification method. Facial recognition technology is widely known and used, often employed in secure computer systems, laptops, smartphones, or ATMs. In addition to its advantages, such as not requiring direct physical contact during the identification process and being a fast and efficient method, a face recognition-based system is more secure and harder to bypass compared to other identification methods. Passwords and PIN codes can be easily compromised or hacked, and various cards and keys can be lost or stolen, potentially leading to misuse by unauthorized individuals against security measures.

Taking these aspects into consideration, I designed the system's operation. To gain entry, it is a requirement for the administrator to add the individuals' data and images. Once this condition is met, the person is granted access to the building. The user simply stands in front of the camera at an appropriate distance, and if they are found in the system, the door opens, allowing them to enter. To facilitate ease of use, I created a user interface that allows for easy addition of individuals, and for traceability, the system maintains a list of individuals who have entered the building, along with the exact entry time.

The system I implemented simplifies the identification process during entry and provides a secure solution for detecting unauthorized individuals in everyday situations.

Keywords: facial recognition, identification, biometrics, access control system, security

Tartalomjegyzék

Ábrák jegyzéke	3
Táblázatok jegyzéke	4
1. Bevezető	5
2. Elméleti megalapozás és szakirodalmi tanulmány	7
2.1. Elméleti alapok	7
2.1.1. Biometrikus azonosítás	7
2.1.2. Arcfelismerés	9
2.2. Ismert hasonló alkalmazások	13
2.2.1. Internet-alapú beléptető rendszer mobilalkalmazás segítségével	13
2.2.2. Arcfelismerésen és az IoT technológián alapuló intelligens biztonsági rendszer	14
2.2.3. Élő arc detektálása beléptető rendszerhez	15
2.3. Felhasznált technológiák	17
2.3.1. Kamera modul	17
2.3.2. Arcfelismerő és élőszőrűség érzékelő modul	17
2.3.3. Felhasználói felület	17
3. A rendszer specifikációi és architektúrája	18
3.1. A rendszer architektúrája	18
3.2. Követelmény specifikáció	19
3.3. Funkcionális követelmények	19
3.4. Nem funkcionális követelmények	24
3.4.1. Teljesítmény követelmények	24
3.4.2. Továbbfejleszthetőségi és karbantarthatósági követelmények	25
3.4.3. Biztonsági követelmények	25
3.4.4. Felhasználói élmény követelmények	25
3.4.5. Felhasználói élmény adminként követelmények	25
4. Részletes tervezés	26
4.1. ESP32-CAM modul	26
4.1.1. Infra reflektív távolság szenzor	29
4.1.2. Adatbázis-kezelő rendszer	30
4.1.3. Arcfelismerő modul	32
4.1.4. Élő arc észlelő modul	34

4.1.5. Relé vezérlése	34
4.1.6. Teljes rendszer bemutatása	35
4.1.7. Webalkalmazás tervezése	36
5. Üzembe helyezési lépések	43
5.1. Felmerült problémák és megoldásaik	43
5.2. Kísérleti eredmények, mérések	44
6. Következtetések	47
6.1. Megvalósítások és Továbbfejlesztési lehetőségek	47
Irodalomjegyzék	49
Függelék	50
F.1. Részletes tervezés	50

Ábrák jegyzéke

2.1. Azonosítási módszerek csoportosítása	8
2.2. Jól kiválasztott és rosszul kiválasztott tulajdonságok[10]	9
2.3. Minta alapú és geometriai azonosítás F.1	9
2.4. Internet-alapú beléptető rendszer architektúrája [1]	13
2.5. Intelligens biztonsági rendszer folyamatábrája [3]	14
2.6. Élő arcdetektálás alapú arcfelismerő rendszer folyamatábrája [8]	15
3.1. A rendszer architektúrája	18
4.1. ESP32-CAM modul felépítése F.1	26
4.2. ESP32-CAM modul lábkiosztása F.1	27
4.3. TTL USB-soros átalakító	28
4.4. TFT LCD kijelző	29
4.5. Infra reflektív távolság szenzor felépítése F.1	29
4.6. Adatbázis modell	31
4.7. Arc kódolás példa	32
4.8. Arc jellegzetes pontjai példa	33
4.9. Relé felépítése	35
4.10. Tápegység felépítése	35
4.11. Teljes rendszer kapcsolási rajza	36
4.12. Bejelentkezés	38
4.13. Rendszerbe belépett személyek listája	39
4.14. Rendszer aktív felhasználói	40
4.15. Új felhasználó hozzáadása	41
4.16. Új felhasználó képek hozzáadása	41
5.1. Egyezések valószínűsége [4]	44
5.2. Konfúziós mátrix	45

Táblázatok jegyzéke

3.1. Regisztrálási funkció	20
3.2. Bejelentkezési funkció	20
3.3. Felhasználók listájának megtekintése funkció	21
3.4. Új felhasználó hozzáadása funkció	21
3.5. Felhasználó profiljának megtekintése funkció	22
3.6. Kép készítése a profilhoz funkció	22
3.7. Belépett személyek listájának megtekintése funkció	23
3.8. Felhasználó belépése funkció	23
3.9. Képkockák felvétele és megjelenítése funkció	23
3.10. Kommunikáció a számítógéppel funkció	23
3.11. Arcfelismerés funkció	24
3.12. Életszerűség érzékelés funkció	24
5.1. Arcfelismerési tesztek eredményei	46
5.2. Élő arc felismerési tesztek eredményei	46

1. fejezet

Bevezető

A biztonság érzése egy alapvető szükséglet minden ember számára. Az idők legtöbb részét munkahelyünkön, a tanulmányi intézményekben illetve otthonunkban töltjük, ezért rendkívül fontos, hogy teljes biztonságban érezzük magunkat ezeken a helyeken.

A mai modern technológia széles skálájú megoldást kínál, amelynek segítségével megóvhatjuk környezetünkben levő embertársainkat és vagyontárgyainkat a illetéktelen behatolóktól. Több típusú biztonsági intézkedés közül választhatunk, melyik az, ami adott körülmények szerint a legmegfelelőbb számunkra. Személyes igényeinknek megfelelően válogathatunk rengeteg biztonsági kamera illetve, beléptető rendszer közül.

Minden biztonsági rendszernek, legyen az fizikai vagy informatikai, az alapvető célja a személyek minél megbízhatóbb azonosítása. A kamerarendszerek beszerelése az épület különböző területeire folyamatos megfigyelhetőséget nyújtnak, azonban így, ha nincsen egy kijelölt alkalmazott, aki ezt folyamatosan figyelemmel kövesse, akkor az esetleges idegen betolakodókat csak utólag vehetjük észre.

A beléptető rendszerek ennél sokkal hatékonyabb megoldást nyújtanak, és megelőzik a nem kívánt incidenseket, az épületbe való bejutást csak azon személyek számára teszik lehetővé, akik megfelelő engedéllyel rendelkeznek, hitelesíteni tudják magukat.

Ezeket a rendszereket három főbb csoportba oszthatjuk fel: tudás alapú, birtok alapú és egyedi tulajdonságokra épülő azonosítás. A tudás alapú azonosításhoz szükséges tudnunk egy bizonyos jelszót, a birtok alapú azonosításhoz rendelkezünk kell a megfelelő kulccsal vagy kártyával, ezek nem direkt módon köthetőek a személlyel, illetve könnyebben kitudóthatnak vagy illetéktelen személyek kezébe kerülhetnek. A biometrikus azonosítás viszont egy olyan technológiát jelent, ami által a személy egyedi fizikai adottságait vagy viselkedését használjuk a hitelesítéshez.

Az én választásom a biometrikus beléptetőrendszerre esett, mivel ez magas szintű biztonságot nyújt és a felhasználók számára egy kényelmes megoldás, nem szükséges bármilyen kulcs vagy kártya egy ajtó kinyitásához, sőt még jelszavak memorizálása és beírása sem kell, elegendő csupán a saját biológiai adottságaik felismerése a rendszer által. Ezen belül is számtalan hatékony módszer van amiből válogathatunk. Én az arcfelismerést választottam, mivel ez egy egymástól jól elkülöníthető tulajdonságokra alapul, mert minden embernek egyedi vonásai, arckifejezése van. Az előnyei mellett még megemlíthető, hogy nem igényel közvetlen fizikai érintést az azonosítás során, illetve gyors és hatékony módszer.

A diplomamunkámként választott projektem célja egy olyan rendszer létrehozása, ami megkönnyíti az emberek mindennapjait, leegyszerűsíti az épületekbe belépni vágyó személyek azonosítását, ami alapján az engedélyezett és az engedély nélküli személyek megkülönböztethetők, korlátozva az illetéktelen személyek behatolását. Ezek által egy biztonságos közeget teremtve. A felhasználó rendszergazdák számára egy könnyen kezelhető és átlátható felhasználói felületet is létrehoztam, aminek segítségével koordinálhatja a belépésre jogosult személyek tevékenységeit. A rendszer megvalósítása során figyelembe vettem azokat a szempontokat, hogy könnyen kezelhető, gyors, hatékony és főképpen biztonságos legyen, mindez egy költséghatékony módon.

2. fejezet

Elméleti megalapozás és szakirodalmi tanulmány

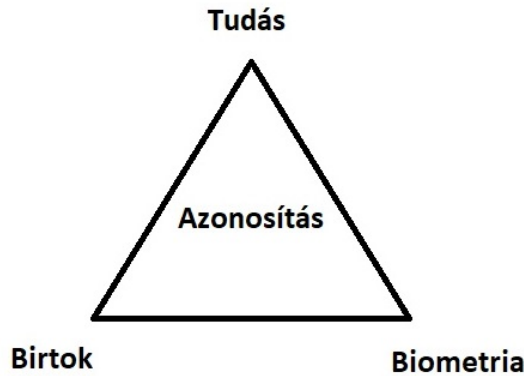
2.1. Elméleti alapok

2.1.1. Biometrikus azonosítás

A dolgozatomban során egy biometrikus beléptetőrendszert fogok ismertetni. Első sorban fontos tisztázni hogy mi is az a beléptetőrendszer? Hozzáférés ellenőrzésen alapuló rendszerek, ami két főbb részre osztható: azonosítás és engedélyezés. Az azonosítás foglalkozik azzal, hogy egy felhasználónak a kilétét vizsgálja, az engedélyezés pedig arra ad választ, hogy a rendszer erőforrásaihoz van-e jogosult hozzáférése az illetőnek.[11] Az emberek azonosítására az alábbi módszerek alkalmazása jellemző:

- valami, amit tudsz (tudás alapú)
- valami, amid van (birtok alapú)
- valami, ami vagy (egyedi tulajdonság alapú)

A tudás alapú azonosítás esetén az egyén olyan információ tudatával rendelkezik, amely az eljárás során ellenőrizhető. Ilyen információ lehet például egy PIN kód, vagy jelszó. A birtok alapú azonosítás egy olyan eszközt igényel, ami a személy birtokában van, lehet ez egy kulcs, smatrcard, mágneses kártyák, QR kód. Az egyedi tulajdonság vagy más néven **biometria** a tudományág, amely azzal foglalkozik, hogy az egyén fizikai vagy viselkedésbeli jellemzői alapján felismerje egy személy azonosságát[10]. A jelszavak és PIN kódok könnyen kitudódhatnak, feltörhetőek, vagy bonyolultabb kódok esetén elfelejthetőek. A fizikai azonosítási tokenek pedig elveszíthetőek vagy ellophatóak, így illetéktelen kezekbe kerülve visszaélés történhet a biztonsági intézkedésekkel szemben. Ezek a hagyományos módszerek már nem elégségesek egy komolyabb biztonsági rendszer kialakítására. Ez ahhoz vezet, hogy szükséges a személy egyedi tulajdonságain alapuló információkat felhasználni. Ezek nem oszthatóak meg másokkal, sokkal kevesebb az esélye a rendszerek feltörésére, mivel jóval nehezebb ezeket ellopni, vagy meghamisítani, így magasabb biztonsági szintet nyújtanak az előbbi módszerekénél. A biometria egyedi tulajdonságokon alapul, amelyek hozzátartoznak az egyénhez, így nem kell aggódni az elfelejtés, elvesztés vagy ellopás veszélyén[9].



2.1. ábra. Azonosítási módszerek csoportosítása

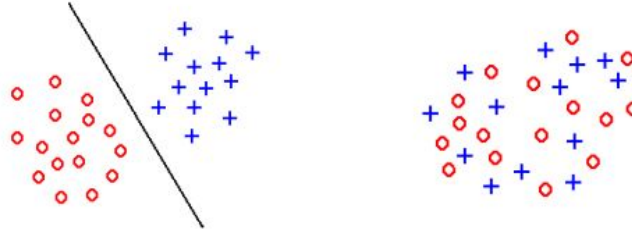
Igazából minden ember biometrikus jellemzők alapján azonosítja az ismerőseit, ha meglátja személyesen, egy fényképről vagy akár csak a hangja hallatán is. Napjainkban erre már nem csak az emberek képesek, hanem a különböző technológiájú rendszerek is ezt a módszert alkalmazzák a hétköznapi életben például biztonságos hozzáférés az épületekhez, számítógépes rendszerekhez, laptopokhoz, okostelefonokhoz, bankautomatákhoz. Ugyanakkor használják ellenőrzés és azonosítás szempontjából határellenőrzés esetén, tanintézményi jelenlét követésére, valamint az egészségügyi rendszerben és a bűnügyi, törvényszéki ügyekben is. [9] A biometria célja biztosítani, hogy kizárólag a jogosult személyek férjenek hozzá a rendszer erőforrásaihoz. Ezáltal lehetőség nyílik egy személy azonosítására az alapján, hogy "ki ő" és nem az alapján, hogy "mivel rendelkezik" vagy "mit jegyzett meg".

A biometrikus azonosításra széles skálájú módszerek közül választhatunk. A biometriai jellemzőket alapvetően két nagy csoportba sorolhatjuk [4]:

- statikus fizikai jellemzők mérésén alapuló módszerek
- viselkedési jellemzőkön alapuló eljárások.

A statikus fizikai jellemzők kategóriához tartoznak például: az arcfelismerés, DNS alapú azonosítás, az ujjlenyomat, a kéz geometriája, a szem (írisz, retina) azonosítása, vagy a fül formája szerinti felismerés is. A viselkedési jellemzők között pedig megemlíthető: a hang alapú azonosítás, a járás alapú azonosítás, vagy akár a kézírás. Ezek után felmerül a kérdés, hogy a biztonságtechnikában melyiket, milyen körülmények között és mikor érdemes választani? A módszer kiválasztása során érdemes szem előtt tartani a következő szempontokat: skálázhatóság, társadalmi elfogadottság, pontosság, az interakció mértéke és a költségek.

A kiválasztott módszer hatékonysága legfőképpen attól függ, hogy milyen sajátosságokat szeretnénk megállapítani (mérni), és ezt milyen pontossággal tudjuk elvégezni, illetve a kiválasztott sajátosság mennyire egyedi egy emberre nézve. Olyan tulajdonságot kell figyelembe venni, ami jól megkülönböztethető egymástól és pontosan mérhető [10]. A tipikusan jól kiválasztott és rosszul kiválasztott tulajdonságokat a következő ábra szemlélteti:



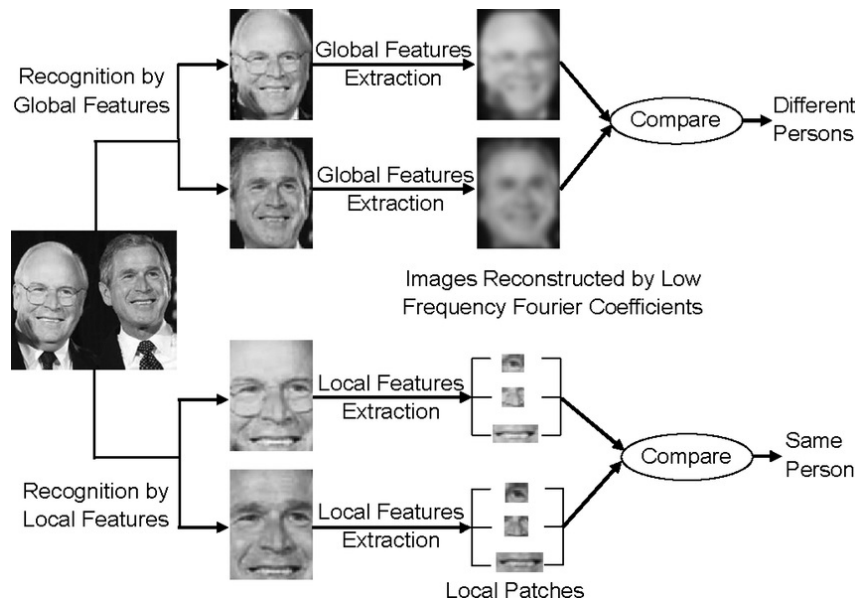
2.2. ábra. Jól kiválasztott és rosszul kiválasztott tulajdonságok[10]

2.1.2. Arcfelismerés

Az arc a legkézenfekvőbb biometrikus azonosító a hétköznapi emberek számára, leginkább ez alapján ismerjük fel egymást. [4] Az arcfelismerésnek több előnye van más biometrikus módszerekkel szemben, nem invazív, tehát nem igényeli a személy fizikai érintését az azonosítás folyamata során, illetve az arckép távolról is jól rögzíthető. Az arcfelismerést két főbb csoportba oszthatjuk fel, a minta alapú és a geometriai felismerés.

A minta alapú azonosítás során az egész arc képe egyszerre kerül feldolgozásra, annak a globális tulajdonságai kerülnek kiemelésre, anélkül, hogy az egyéni pontokat lokalizálná. Bizonyos esetekben ez csupán az arc bizonyos részeire vonatkozik (pl. szem, orr, száj).

A geometriai azonosítás módszere során pedig az arc referenciapontjai kerülnek azonosításra, ezek kevésbé érzékenyek az idő telése következtében létrejött változásokra (pl. szem, az orr oldala, a száj, az arccsontokat körülvevő pontok). Ezeknek a pontoknak a helyzetét használják a pontok közötti geometriai kapcsolatok kiszámításához[9]. Az alábbi ábrán szemléltetem ennek a két módszernek a megvalósítását:



2.3. ábra. Minta alapú és geometriai azonosítás F.1

Mint biometrikus tulajdonságokon alapuló módszer, az arcfelismerő rendszert két részre oszthatjuk fel :

- arcvizsgálat
- arcfelismerés (vagy azonosítás)

Az arcvizsgálat során egy az egyhez párosítást hajtanak végre, amely összehasonlítja egy lekérdezett arcképet egy regisztrált arcképpel.

Az arcfelismerés során egy a többhöz párosítást hajtanak végre, amely összehasonlítja egy lekérdezett arcot a regisztrációs adatbázisban található összes arccal, hogy meghatározzák a lekérdezett arc azonosságát egyezik-e az adatbázisban található arcok közül valamelyikkel. Bizonyos azonosítási alkalmazásokban csak a leghasonlóbb arc megkereséséről van szó. Viszont ez komolyabb rendszerek esetében nem elegendő, egy megbízhatósági szint küszöbértéket határoznak meg, és azok az arcok, amelyek hasonlósági száma meghaladja a küszöbértéket, azok nem léphetnek be az adott rendszerbe és jelentésre kerülnek. [2]

Ismert arcfelismerő algoritmusok

Az arcfelismerési algoritmusok nagyon fontos részét képezik bármely arcfelismerő rendszernek. Az elmúlt évek során számos arcfelismerési algoritmust fejlesztettek és tanulmányoztak, a jobb eredmények elérésének érdekében. A [7] cikk egy általános áttekintést nyújt a különböző arcfelismerési technikákról. Bemutat néhány különösen fontos algoritmust, mint például a Cascade Classifier, a Dlib CNN, a Dlib HOG, az MTCNN, kifejtve a működésüket, jellemzőiket, előnyeiket illetve hátrányaikat.

Az arcfelismerés folyamán azonban számos kihívással kell szembenéznünk, mint például a pozícióváltozás, különböző helyek, megvilágítás, mimikaváltozás, arcszőrzet, szemüveg jelenléte, fényviszonyokban és kép felbontásában. Ezeknek a kihívásoknak a megoldása érdekében különböző módszerek léteznek.

1. Cascade Classifier (Haar Cascades)

Egy olyan módszer, amely több osztályozó réteget tartalmaz, amelyek egymás után végzik az objektum detektálását. A Cascade Classifier képzése néhány száz olyan képből áll, amelyek tartalmazzák a felderítendő objektumot (pozitív képek) és más olyan képeket, amelyek nem tartalmazzák az adott objektumot (negatív képek). Ezek az OpenCV könyvtárral vannak társítva, a tanított XML fájlokkal együtt. Viola-Jones javasolta az objektumfelismerési keretrendszert a valós idejű arcfelismeréshez. A következő lépésekből áll: Haar-jellemző kiválasztása, Integrálkép, Adaboost, Cascading Classifier.

Rengeteg funkciót számolnak ki minden lehetséges méretből és régióból. A szükséges számítás olyan nagy méretű, hogy még a 24x24-es ablak is 160000 jellemzőt ad. Ez az integrálképek bevezetéséhez vezetett. Az Adaboost funkciók segítségével, ez az 160000+jellemző, 6000 jellemzőre csökken. Ezen módszerek időigényessége miatt vezették be a Cascading Classifier-t, aminek segítségével ezek a jellemzők csoportosítva lesznek. Ha egy ablak nem működik az első szakaszban, akkor az adott kaszkádban lévő többi jellemzőt már nem fogják feldolgozni. Amikor egy ablak átmegy az összes szakaszon, hibánélkül, akkor az egy arc régiónak tekinthető.

2. Dlib CNN

A Dlib CNN arcdetektáló algoritmus egy kombinációja a Konvolúciós Neurális Hálózatnak (CNN) és a Dlib-nek, ahogyan ez már a nevéből is kiderül.

A Dlib egy nyílt forráskódú könyvtár, amely számos különböző gépi tanulási algoritmust tartalmaz. A komplex problémák megoldására kitűnő megoldást nyújt.

A CNN egy mély tanulási algoritmus, amit képek elemzésére használnak a rendszer bemeneteként.

Az algoritmus az arcfelismerésre a Dlib eszközkészletét használja a CNN jellemzők mellett, és meghaladja más különböző arcdetektáló algoritmusok teljesítményét, mivel a CNN jellemzők előnyt jelentenek a módszer számára. Ebben az algoritmusban, a CNN alapú jellemzők mellett, használják a MMOD-t (Maximum-Margin Object Detector) is. Más módszerekhez képest itt automatizálódik a szűrők kiválasztására szolgáló a képek jellemzőinek kinyerése. Így az egyetlen teendő a használandó szűrők számának beállítása lesz.

A Dlib CNN arcdetektáló algoritmus lépései a következők: az arcdetektálási modell betöltése, az arcdetektor inicializálása és a CNN-alapú detektor alkalmazása. Az első lépés magába foglalja a betanított modell és a súlyok betöltését. Majd a második fázisban az inicializáláskor, a fent említett súlyokra lesz szükség. Végül pedig alkalmaznunk kell a detektort a teszt képeken, majd ezt követően az megadja nekünk az észlelt arcokat.

A Dlib CNN nagyon könnyen implementálható, jól teljesít különböző arceltakarás esetén is. Azonban nem képes észlelni a 80x80-nál kisebb arcokat.

3. Dlib HOG

Ez a legszélesebb körben használt arcdetektálási moddell. A HOG (Histogram of Oriented Gradients), azaz orientált gradiensek hisztogramján alapuló, jellemző leíró modell, amely lineáris SVM (Support Vector Machine) gépi tanulást alkalmaz az arcdetektáláshoz. Ez a modell öt szűrőre épül, amelyek balra, hátra, jobbra, előlről balra forgatva, valamint előlről jobbra vannak forgatva. A modell lényege, hogy a jellemzőket kinyeri egy vektorba majd ezt egy osztályozó algoritmus az SVM segítségével osztályozza, így meghatározva, hogy egy adott régióban található-e arc.

A következő lépések mutatják be az algoritmus folyamatát: gamma és szín normalizálása, Gradiens számítása, súlyozott szavazás térbeli és orientációs cellákba, kontraszt normalizálása az átfedő térbeli blokkokon, HOG gyűjtése a detektálási ablakon. Az első fázis akár ki is hagyható, mivel nem nyújt túl magas pontossági növekedést. Második lépésben kiszámítjuk a kép gradiensét, így csökkentve a kép dimenzióját, a gradiens a képen levő minden élt rögzít. Ezután súlyozott szavazással elosztjuk a gradienst térbeli és orientációs cellákba, amelyeket egy vektorként lehet felfogni, ami tartalmazza a hisztogram értékeit, ez alapvetően szétválasztja a bemenetet más formátumoktól, ami kisebb dimenziójú lesz. Majd ezt követően normalizáljuk a hisztogramot, azaz normalizáljuk a kontrasztot a blokkban. Végül pedig a képet 8x8-as cellákra osztjuk, hisztogramot építünk 64 gradiens irányának és nagyságának értékeiből, ami a 0-tól 180 fokig terjedő gradiensszögeket közvetíti.

Így két értéket kaptunk meg: az irányt és a nagyságot. HOG építése közben három al-esetet veszünk figyelembe: ha az irány 160 foknál kisebb és nem esik két osztály közé (a szög a megfelelő kategóriához kerül hozzáadásra), az irány 160 foknál kisebb és két osztály közé esik (szög hozzájárul mindkét közeli osztályhoz, és a nagyság értékei is fel vannak osztva a két osztály között), az irány 160 foknál nagyobb (az adott pixel arányosan járul hozzá a 160 fokos, illetve a 0 fokos osztályhoz egyaránt)

Az algoritmus rendkívül jól működik az előrefordított arcokkal, és a kismértékben előrefordított arcokkal is.

4. MTCNN

Az MTCNN (Multitask Convolutional Neural Network), azaz Többfeladatos konvolúciós neurális hálózat, egy olyan módszer, ami egyszerre végzi el a kulcspontok és arcok detektálását. Ez a modell egy kaszkád keretrendszeren alapul. Általános struktúrája 3 részre osztható: P-Net (Proposal Network), R-Net (Refine Network), O-Net (Output Network). Az első rész feladata, hogy amikor arccot észlel visszaadja annak a régióknak ahol az található a koordinátáit, aztán szakaszokra osztva ismétli meg a folyamatot a 12 x 12-es magot 2 képponttal jobbra vagy lefelé tolva. A képen található arcok nagyobbak, mint 2 képpont, ezért nagyon alacsony a kihagyott arcok valószínűsége. Az R-Net tartalmazza az új és pontosabb koordinátákat, valamint ezeknek a konfidencia szintjét is. Megszabadulunk a kisebb konfidencia szintű "dobozoktól". Az O-Net szakaszában több információt kapunk az arc területeinek megjelöléséhez. Itt kapjuk meg az arc jellemző pontjainak a koordinátáit, a határoló dobozok koordinátáit, és ezeknek a konfidencia szintjét. Végül kiszűrve az alacsonyabb konfidencia szinttel rendelkező régiókat megkapjuk a személyarcnak jellemzőit.

Az MTCNN rendkívül nagymértékű pontossággal rendelkezik, azonban időigényes lehet a tanítás.

Következtetés

Az algoritmusok összehasonlítása során szem előtt tartottam a számomra szükséges szempontokat az beléptető rendszer megtervezése során. Számomra fontos, hogy az algoritmus első sorban biztonságos legyen, így kizártam a Haar kaszkádok használatát, mivel azok nyújtották a legkisebb pontosságot, sok hamis eredményt adtak, valamint nem működik oldalra néző arcokon. A Dlib CNN módszere egy kicsit gyorsabb a HOG módszerhez képest, azonban ez nem működik jól valós idejű arcfelismerés esetén aminek egy alap követelmény a rendszert tekintve. Szem előtt tartottam, hogy bizonyos arc eltakarások, fedések esetén is kiválóan kell működnie a rendszernek, ennek eleget tett az MTCNN és a Dlib HOG nagyon hasonló eredményeket nyújtottak, az MTCNN egy enyhe előnyt szerzett, mivel az felismeri a kisebb képeket is, azonban ez az én esetemben nem egy alap feltétel, ugyanis én nem távolról kell kövessem és felismerjem az arcokat, hanem közvetlen a kamera előtt. Így az én választásom a Dlib HOG modelljére esett az arcfelismerő rendszer létrehozása során.

2.2. Ismert hasonló alkalmazások

A dolgozatom megtervezése során megvizsgáltam számos hasonló jellegű alkalmazást, különböző cikkekből és könyvekből dokumentálódva. Az alábbiakban röviden bemutatok néhány hasonló megvalósítású rendszert.

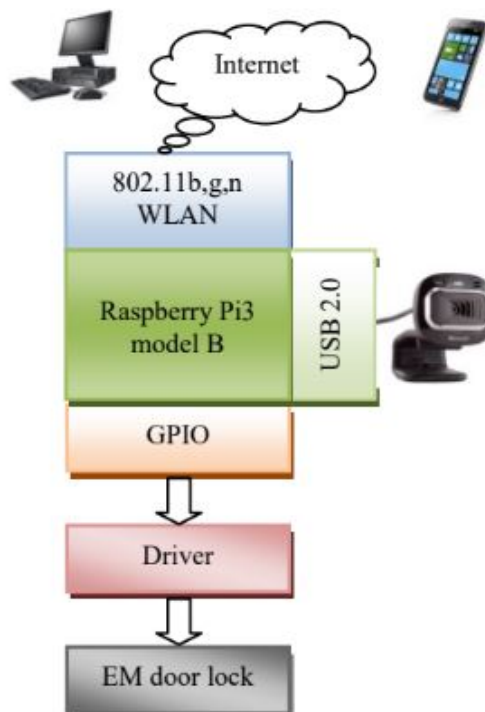
2.2.1. Internet-alapú beléptető rendszer mobilalkalmazás segítségével

A [1] tanulmányban egy beléptető rendszer megvalósítását mutatja be Raspberry Pi3 segítségével, amely a helyi hálózaton keresztül csatlakozik az internethez. A rendszer valós időben követi az eseményeket az ajtóra felszerelt előtérben. Egy kamera és arcfelismerési feldolgozás segítségével dolgozza fel a képeket, és értesíti a rendszergazdát, ha valaki túl sok időt tölt az ajtó előtt. A rendszerbe regisztrált felhasználóknak engedélyezett a belépés. Egy mobilalkalmazás segítségével, három féle hitelesítés van alkalmazva, az ajtót kinyithatják arcfelismerés, jelszó vagy ujjlenyomat segítségével.

A kamera képeinek lekérdezéséhez az OpenCV könyvtárat használták. Az arcok detektálására pedig a Haar kaszkádokat és a Viola Jones algoritmust.

A mobilapplikáció pedig az Android stúdió segítségével valósult meg Java-ban. A rendszer nagy mértékben a Raspberry Pi3 B mini modell köré épül, illetve magába foglal egy Microsoft Lifecam HD 3000 USB 1280x720 webkamerát és egy áramkört a 12V-os elektromágneses ajtózár meghajtásának érdekében.

Az alábbi ábrán látható a rendszer architektúrája:



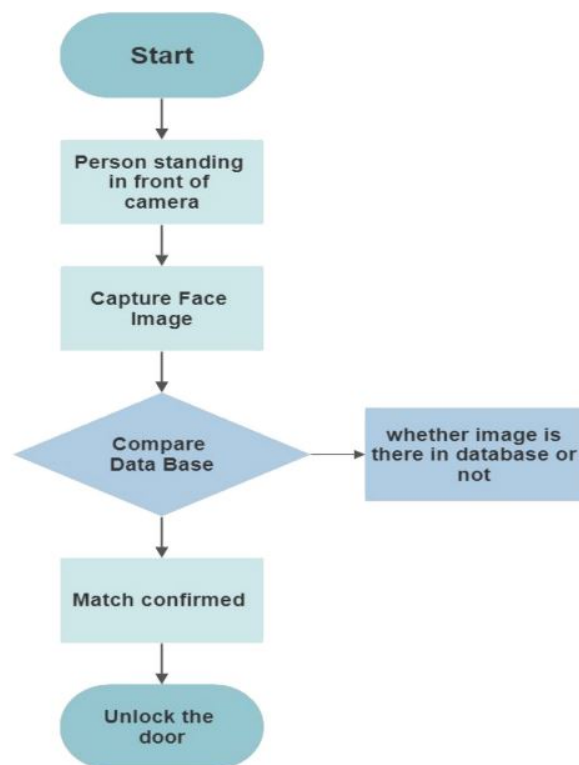
2.4. ábra. Internet-alapú beléptető rendszer architektúrája [1]

A rendszergazdának is hozzáférése van a kamera által rögzített képkockákhoz, illetve szükség esetén, távolról is felnyithatja az ajtót kérésre. Egy Raspberry Pi3 beágyazott rendszeren fut a webszerver, amely tartalmaz egy lokális adatbázist, ahol a regisztrált felhasználók listája és a hozzájuk tartozó adatok találhatóak meg. Valamint létezik egy naplófájl, amely részletes információkat nyújt az észlelt és rögzített eseményekről.

2.2.2. Arcfelismerésen és az IoT technológián alapuló intelligens biztonsági rendszer

A dolgozatomhoz végzett tanulmányi kutatás során rátaláltam a [3] cikkre, amely egy arcfelismerés alapú beléptető rendszert hoztak létre ESP32-CAM modul segítségével. A rendszer valós időben végzi az arcok észlelését és azonosítását, megfelelő gyorsasággal reagálva, amikor egy arc a kamera előtt van.

A folyamat a képek adatbázisba való feltöltésével kezdődik a felhasználók által. A megérkezett kép elemzésre kerül, bizonyos arctulajdonságokat származtatnak egy azonos személy különböző képeiből (pl. szemek közötti távolság, orr hossza). Az arcfelismeréshez az ESP32-CAM modul beépített arcfelismerő algoritmusát használják. Az összehasonlítás után, ha a találat megbízhatósági szintje 90% vagy annál magasabb, akkor az ajtó kinyílik, ellenkező esetben ismeretlen személy esetén. az ajtó zárva marad. Az alábbi ábrán látható a rendszer folyamatábrája:



2.5. ábra. Intelligens biztonsági rendszer folyamatábrája [3]

A kamera modul a további áramköri elemekhez van csatlakoztatva, egy 12,6 V-os akkumulátorhoz, egy konverterhez a feszültség csökkentésére és állandó 5 V-os tápellátás

biztosítására, illetve az elektromágneses zár 12 V-os tápellátást kap az IRF520 MOSFET kapcsolómodulon keresztül. Amikor a ESP32-CAM modul érzékel egy olyan személyt, akinek az arca felismerhető, akkor a zöld LED világít, a relé záródik, és áramot kap az elektromágneses zár, amely 10 másodpercig nyitva marad a bejutást biztosítva.

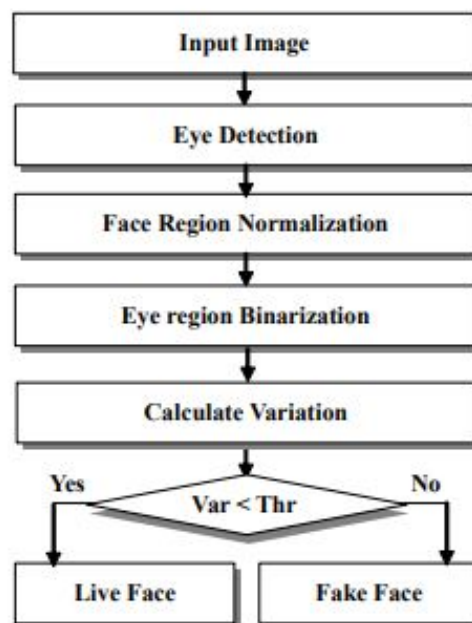
2.2.3. Élő arc detektálása beléptető rendszerhez

Egy biztonságos arcfelismerő rendszer esetében fontos, hogy a rendszer ne legyen könnyen átjátszható fényképek, videók vagy esetleg arcszerű maszkok viseletével. Ennek következtében szükséges ellenőrizni, hogy az adott belépni kívánó személy ténylegesen élő ember.

Élő arc detektálása a szemek mozgása alapján

Erre egyfajta megoldást nyújt a [8] tanulmány, amely egy gyors és memóriahatékony módszert mutat be az élő arcok detektálására. A megvalósítás a szemek mozgására alapul, az egymást követő bemeneti képeken észleljük a szemeket, és kiszámítjuk a szem régiójának változását abból a célból, hogy meghatározhassuk az adott arc valós létét.

Először detektáljuk a bemeneti arcképen mindkét szem középpontját. Az észlelt szemek segítségével normalizáljuk az arc régióját és kinyerjük a szem területét. Az előállított szemrégiókat binarizáljuk, majd összehasonlítjuk egymással és kiszámítjuk a kettő közötti változást. Ha az eredmény meghaladja a küszöbértéket, akkor az input képet élő arcnak tekintjük, ha nem, akkor pedig fényképnek, azaz hamis bemetnek. A rendszer folyamat-ábrája lentebb látható:



2.6. ábra. Élő arcdetektálás alapú arcfelismerő rendszer folyamat-ábrája [8]

A megvalósítás során a Viola Jones és az AdaBoost tanítási módszerrel képezett szem osztályozót alkalmazták. Először kinyerjük a 16x16-os méretű részablakokat minden lehetséges szem körül, miközben csökkentjük az arc képének méretét. Kép-piramist használnak annak érdekében, hogyképesek legyenek különböző szélességű szemekkel dolgozni. Ezután a részablakokat beillesztjük az erős osztályozóba, majd a szemeket azonosíthatjuk azáltal, hogy meghatároztuk a legnagyobb értékkel rendelkező lehetséges eseteket. A Hamming távolság segítségével kiszámoljuk az egyes szemrégiók élőkép pontszámát. Összehasonlítjuk egymással az összes bal és az összes jobb szemet is. Az eltérő képpontok száma, ami a különbséget mutatja a két szemrégió között, lesz az élőkép pontszáma. Miután összeadtuk 10 bal és 10 jobb szem pontszámát és , kiszámítjuk aí átlagot az eredményekből. Ha az átlag meghaladja a küszöbértéket, akkor a bemeneti képet élő arcnak tekintjük.

Élő arc detektálása OpenCV DNN modell segítségével

Egy másik ismert megvalósítást találtam, ami megfelelő az élő arcok felismerésére a [12] projekt dokumentumában is megtalálható. A cikkben egy olyan arcfelismerő rendszert mutatnak be, ami képes felismerni arcmaszkokat helyese és helytelenül viselő személyeket. A rendszert a Covid-19 járvány idején fejlesztették ki és hasznosították. Az alkalmazott módszerek között megemlíthetjük a mély tanulást, a TensorFlow-t, a Keras-t és az OpenCV-t is. Az SSDMNv2 megközelítés a Single Shot Multibox Detektort használja az arcok észleléséhez, és a MobilenetV2 architektúrát keretrendszerként az osztályozáshoz, amely beépített eszközökön (például Raspberry Pi) is valós idejű detektálást végezhet.

A cél ebben a tanulmányban az, hogy növeljék a maszkdetekálás pontosságát. Ehhez a az OpenCV DNN modelljét használták, amely tartalmazza a Single Shot Multibox Detector (SSD) objektumdetektáló modellt együtt a ResNet-10, mély neurális hálózat architektúrával együtt.

Ha az arcokat SSD segítségével sikeresen detektálják, akkor a kimeneten látható egy négyzet az arcokat körülvéve, majd meghatározzák a maszkot helyesen és helytelenül viselt személyeket.

Az elméleti megalapozás során rátaláltam az Adam Brock által létrehozott alkalmazás [13] oldalára, ahol szintén az OpenCV DNN modellt használva valósítanak meg egy élő arc érzékelő applikációt. Részletesen leírja a használt módszereket, elkészít egy tanító halmazt saját adatokkal, ami valós élő arcok képeiből áll és ami képről készült fotókat tartalmaz. Majd ebből felépít és tanítja a modellt a TensorFlow és a Keras csomagjaival felhasználva. Majd ábrázolja a tanulási előzmények eredményének pontosságát. Az éloszerűség detektálásához egy konvolúciós neurális hálózatot implementál. Az alkalmazás megvalósítása során a webkameráról olvassa be a képkockákat, minden képkockán arcfelismerést majd az éloszerűség modellt használja.

2.3. Felhasznált technológiák

2.3.1. Kamera modul

Az általam tervezett beléptető rendszer több modulból áll. A valósidejű arcfelismeréshez az ESP32-CAM modulját választottam a képkockák beolvasására. ESP32-CAM az ESP32 családjába tartozik, egy OV2640 kamerát, több lábat tartalmaz a perifériák csatlakoztatásához, valamint egy microSD kártya behelyezési lehetőséget biztosít, amely hasznos lehet a kamerával készített képek vagy más fájlok tárolásához. Valamint rendelkezik Wifi modullal is, amely lehetővé teszi azon keresztül a kommunikálást. Az iparban rendkívül népszerű lett a használata napjainkban, a viszonylag alacsony költség mellett nyújtott kiváló teljesítményével. Rugalmasan alkalmazható az okos otthonokban, biztonsági berendezésekben vagy más komplexebb rendszerek összetevőjeképpen.

2.3.2. Arcfelismerő és és éloszerűség érzékelő modul

A modul által továbbított képfolyamot egy Python program segítségével dolgozom fel. Az alkalmazás megvalósításához több beépített könyvtárat, illetve csomagot is használtam, ezek közül a fontosabbak az alábbiak: az OpenCV, face_recognition, keras.

Az OpenCV egy nyílt forráskódú könyvtár, amely lehetővé teszi a képek és videók feldolgozását, valamint azokkal való műveletek elvégzését. Számos algoritmust és funkciót tartalmaz az objektumfelismerés, arcfelismerés, alakfelismerésig, képjavításig és hasonló műveletek megvalósítását magába foglalva.

A face_recognition csomag, amint már a neve is sugallja arcfelismerési feladatokhoz volt kifejlesztve. A csomag az OpenCV-t és a Dlib könyvtárat használja, számos funkciót és eszközt nyújtva a magas szintű arcfelismerési feladatokhoz, mint az arcdetektálás, felismerés és arcvonások azonosítása.

Keras egy magas szintű neurális hálózatokat építő és képző könyvtár, amelyet a gépi tanulás és a mély tanulási feladatokra fejlesztettek ki. Leegyszerűsíti és gyorsítja a neurális hálózatok létrehozását és tanítását a fejlesztők számára. Az élő arcok felismerésére alkalmazom az applikáción belül.

2.3.3. Felhasználói felület

A könnyebb kezelhetőség érdekében létrehoztam egy felhasználói felületet, amelyen keresztül az adminok leegyszerűsítve megvalósíthatják az adatok feltöltését, módosítását, illetve az eredmények megfigyelését. Céлом egy dinamikus weboldal létrehozása volt, amelyhez PHP-t, HTML-t és a Bootstrap keretrendszert használtam. A PHP segítségével dinamikus tartalmat generáltam, például adatbázis lekéréseket és adatok feldolgozását végeztem el. A Bootstrap keretrendszer lehetővé tette számomra, hogy gyorsan és egyszerűen reszponzív és egyszerűen dizájnolható elemeket használjak az oldal kialakításához. Továbbá, a weboldal fejlesztése során alkalmaztam egy előre elkészített ?? templatet is, amely segített a tervezési folyamat felgyorsításában és a konzisztens megjelenítés elérésének érdekében. A sablon tartalmazott előre definiált CSS osztályokat és komponenseket, amelyeket egyszerűen alkalmazhattam az megvalósítás különböző fázisaiban.

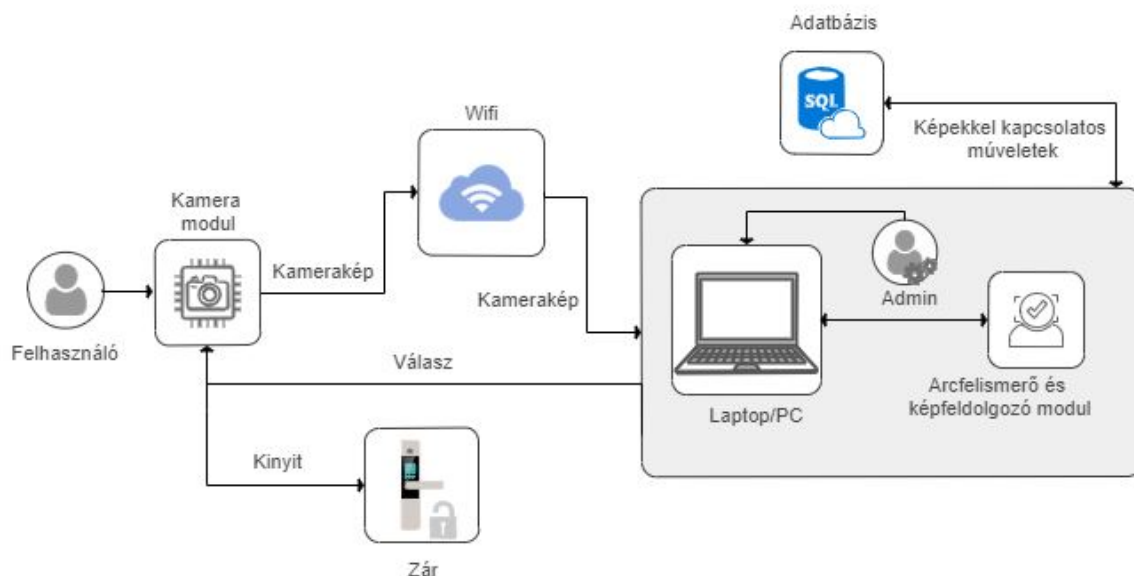
A teljes rendszer részletes leírását és megvalósításhoz használt technológiákat a következőkben részletesen kifejtem és bemutatom.

3. fejezet

A rendszer specifikációi és architektúrája

3.1. A rendszer architektúrája

A dolgozatomban célom volt egy beléptető rendszert létrehozni, ami biometrikus tulajdonság alapján, a mi esetünkben arcfelismeréssel azonosítja a személyeket. A rendszer különböző hardver és szoftver komponensekből tevődik össze, amelynek a működését és elhelyezkedését a következő ábrán szemléltetem:



3.1. ábra. A rendszer architektúrája

Első fázisban a kamera modul készíti a kameraképet, majd Wifi csatlakozás segítségével továbbítja egy Számítógépre vagy Laptopra, amelyen fut a képfeldolgozó modul. A beolvasott framek összehasonlításra kerülnek az adatbázisban levő képekkel, ha valamelyikkel azok közül megegyezést talál, akkor egy értesítést küld tovább a kamera modulnak,

amelyen keresztül majd kinyílik a zár, ellenkező esetben, ha ismeretlen személyt talál, akkor zárva marad.

3.2. Követelmény specifikáció

Ebben a részben a rendszer pontos követelményit mutatom be, amezek által működőképes állapotba lehet hozni. A felhasználókat először az admin szükséges regisztrálja. Erre létrehoztam egy felhasználói felületet, aminek segítségével feltöltheti a szükséges adatokat, illetve flóényképeket. A személyek regisztrálása után, a felhasználók esetén a kamera modul használata lesz igénybe véve, ugyanis a belépésre vágyó személynek csupán annyi dolga van, hogy a kamera elé álljon, ami majd azonosítja őt.

3.3. Funkcionális követelmények

A funkcionális követelmények olyan specifikációk, amelyek meghatározzák egy rendszernek milyen funkcionalitásokkal kell rendelkeznie, és milyen feladatokat kell elvégeznie. A mi esetünkben ezt több alkomponensre bonthatjuk: a kamera modul (ESP32-CAM), egy webes felhasználói felület (az admin számára), az arcfelismerő és képfeldolgozó rendszer és a felhasználók.

Admin funkcionalitásai:

- Regisztrálás
- Bejelentkezés
- Kijelentkezés
- Jelszó megváltoztatás
- Felhasználók listájának megtekintése
- Felhasználók profiljának megtekintése
- Új felhasználó hozzáadása
- Felhasználó törlése
- Felhasználó profiljának módosítása
- Belépett személyek listájának megtekintése
- Kapcsolatfelvétel a szolgáltatóval

Felhasználó funkcionalitásai:

- Belépés

Kamera modul funkcionalitásai:

- Képkockák felvétele és megjelenítése

- Kommunikáció a számítógéppel
- Zár kinyitása

Arcfelismerő alrendszer funkcionálisai:

- Képkockák fogadása és feldolgozása
- Arcfelismerés
- Kép készítése a profilhoz
- Életszerűség érzékelés
- Kommunikáció az adatbázissal

Az alábbiakban néhány fontosabb funkcionálitást szeretnék kiemelni és részletesen bemutatni:

3.1. táblázat. Regisztrálási funkció

Regisztrálási funkció	
Leírás	Az adminnak regisztrálnia kell a felhasználói felületen, hogy bekerüljön a rendszerbe.
Kiváltás	Az admin megnyitja a felhasználói felületet és a főoldalon rákattint a "Sign Up" gombra.
Funkcionális követelmény	A főoldalon a "Sign Up" gombra kattintva átlép a regisztrációs űrlapra. Ott az email címe és egy jelszóra, és a jelszó megerősítésére lesz szükség. A regisztráció akkor sikeres, ha az előbb említett mezőket helyesen kitöltötte, ami alatt azt értem, hogy egy valódi email címet adott meg, amivel még nincsen más regisztrálva, illetve egy megfelelő erősségű jelszót ad meg, és a megerősített jelszónak meg kell egyeznie a jelszóval. Ellenkező esetben hibaüzenetet kap, hogy melyik mező kitöltésével van probléma és azt kijavítva újra próbálhatja a regisztrációt.
Megszorítás	

3.2. táblázat. Bejelentkezési funkció

Bejelentkezési funkció	
Leírás	A már regisztrált admin be tud jelentkezni.
Kiváltás	Az admin a felhasználói felület főoldalán rákattint a "Login" gombra.

Funkcionális követelmény	A főoldalon a bejelentkezési űrlapban kitölti a mezőket. Az email címére és a jelszávára lesz szükség. Ezt követően megnyomja a "Login" gombot. A belépés akkor sikeres, ha az előbb említett mezőket helyesen kitöltötte, tehát a már regisztrált email címét és a hozzá tartozó jelszót adta. Ellenkező esetben hibaüzenetet kap, hogy melyik mező kitöltésével van probléma és azt kijavítva újra próbálhatja a bejelentkezést.
Megszorítás	

3.3. táblázat. Felhasználók listájának megtekintése funkció

Felhasználók listájának megtekintése funkció	
Leírás	Az admin megtekintheti a már hozzáadott felhasználók profiljainak listáját.
Kiváltás	Az admin a menüben rákattint a "Profiles" gombra.
Funkcionális követelmény	Bejelentkezés után az admin a menüben a "Profiles" gombra rálépve megtekintheti a már eddig hozzáadott profilok listáját. Az egyes profiloknál látszik a profilhoz tartozó kép, név, illetve munkakör. Ha egy profilt részletesen szeretne megtekinteni, akkor a kép fölé helyezve az egeret előjön egy ember ikon, amelyre rákattintva tovább navigál a "Profile Detail" oldalra. Ha egy felhasználót törölni szeretne, akkor a kép jobb felső sarkában megjelenő szemetes ikonra kattintva megteheti, ekkor beugrik egy üzenet ahol megkérdezi, hogy biztos benne, hogy törölni szeretné a profilt? Ha ezt megerősíti akkor a kiválasztott személy profilja törlésre kerül a rendszerből. Ha új profilt szeretne létrehozni, akkor az "Add New Member" gombra kattintva átirányítódik a "Create a new profile" oldalra.
Megszorítás	Be kell legyen jelentkezve az admin.

3.4. táblázat. Új felhasználó hozzáadása funkció

Új felhasználó hozzáadása funkció	
Leírás	Az admin hozzáad egy új felhasználói profilt.
Kiváltás	Az admin a "Profiles" oldalon rákattint az "Add New Member" gombra.

Funkcionális követelmény	A "Profiles" oldalon az admin rákattint az "Add New Member" gombra és átirányítódik a "Create a new profile" oldalra. Itt ki kell töltsen a mezőket személy adataival: név, email cím, telefonszám, nem, illetve munkakört. Ha a formot helyesen kitöltötte és rákattint a "Submit" gombra, akkor létrejön az új felhasználó és kidob egy üzenetet, hogy "New member successfully added!", ellenkező esetben pedig kiírja melyik mezővel kapcsolatban van hiba és kijavítva újrapróbálhatja műveletet. Erről az oldalról a "Back" gomb megnyomásával visszaugorhat a profilok listájához.
Megszorítás	Be kell legyen jelentkezve az admin.

3.5. táblázat. Felhasználó profiljának megtekintése funkció

Felhasználó profiljának megtekintése funkció	
Leírás	Az admin megtekintheti egy felhasználó profilját.
Kiváltás	Az admin a "Profiles" oldalon rákattint a megtekinteni kívánt személy képén levő ikonra.
Funkcionális követelmény	"Profiles" oldalon rákattint a megtekinteni kívánt személy képén levő ikonra megtekintheti az illető személy profilját. Itt láthatóak a profilhoz tartozó adatok: név, képek, email cím, telefonszám, nem, illetve munkakör. Ugyanitt kell hozzáadja az ember profiljához a képeket a "Take Picture" gomb segítségével, amit ha megnyom akkor a kamera 3 képet készít az előtte álló személyről. A képeket megtekintheti, előre és hátra navigálva közöttük. Erről az oldalról a "Back" gomb megnyomásával visszaugorhat a profilok listájához. Ha szeretné módosítani az adott profilt "Edit Profile" gombra kattintva átirányítja az "Edit Profile" oldalra.
Megszorítás	Be kell legyen jelentkezve az admin, létre kell legyen hozva legalább egy profil.

3.6. táblázat. Kép készítése a profilhoz funkció

Kép készítése a profilhoz funkció	
Leírás	Az admin képeket készít a felhasználóról a profiljához.
Kiváltás	Az admin a "Profile Detail" oldalon rákattint a "Take Picture" gombra.
Funkcionális követelmény	A "Profile Detail" oldalon az admin a "Take Picture" gombra kattint és ennek következtében beindul a kamera modul. Az előtte álló személyről három képkockát készít és ezeket hozzáadja a személy profiljához.
Megszorítás	Be kell legyen jelentkezve az admin, létre kell legyen hozva legalább egy profil.

3.7. táblázat. Belépett személyek listájának megtekintése funkció

Belépett személyek listájának megtekintése funkció	
Leírás	Az admin megtekintheti a belépett személyek listáját.
Kiváltás	Az admin a menüben rákattint a "Services" gombra.
Funkcionális követelmény	Az admin a menüben rákattint a "Services" gombra és átirányítódik a "Services" oldalra. Itt megtekintheti a rendszerbe belépő személyek aktivitását, név és időpont szerint időrendi sorrendben.
Megszorítás	Be kell legyen jelentkezve az admin.

3.8. táblázat. Felhasználó belépése funkció

Felhasználó belépése funkció	
Leírás	A felhasználónak kinyílik a zár és beléphet az ajtón.
Kiváltás	A felszerelt kamera modul elé áll.
Funkcionális követelmény	A felhasználó a felszerelt kamera modul elé áll. Ha sikeresen felismeri a rendszer, összehasonlítva a rendszerben lévő személyekkel, és élő személynek bizonyul, akkor kinyílik a zár, és beléphet az ajtón.
Megszorítás	Hozzá kell adni a felhasználót az admin által, és képeknek kell lenniük a profiljában.

3.9. táblázat. Képkockák felvétele és megjelenítése funkció

Képkockák felvétele és megjelenítése funkció	
Leírás	A felhasználónak kinyílik a zár és beléphet az ajtón.
Kiváltás	Egy ember szükséges a kamera modul elé álljon, hogy elinduljon a folyamat.
Funkcionális követelmény	A kamera modul felébredése után elkezd a képkockákat felvenni, azokat továbbítja az arcfelismerő modul fele, valamint megjeleníti a képernyőn.
Megszorítás	A rendszer áramforráshoz kell legyen csatlakoztatva és kamera modul fel kell ébredjen alvó állapotából.

3.10. táblázat. Kommunikáció a számítógéppel funkció

Kommunikáció a számítógéppel funkció	
Leírás	A felhasználónak kinyílik a zár és beléphet az ajtón.
Kiváltás	A kamera modul és a számítógép WiFi hálózaton keresztül kommunikál egymással.

Funkcionális követelmény	A kamera modul továbbítja a képkockákat az arcfelismerő modulnak. Majd a megkapott választ fogadja, hogy sikeres volt a felismerés vagy sem.
Megszorítás	Megfelelő erősségű WiFi jel a kapcsolat megteremtéséhez.

3.11. táblázat. Arcfelismerés funkció

Arcfelismerés funkció	
Leírás	A rendszer felismeri a felhasználónak az arcát.
Kiváltás	A kamera modul elküldi a képkockákat.
Funkcionális követelmény	Az arcfelismerő modul fogadja és feldolgozza a képkockákat az kamera modultól. Maj összehasonlítja a már hozzáadott felhasználókkal a kapott képkockákat, ha megegyezést talál, akkor a következő funkciónak adja át a helyet.
Megszorítás	Képkockák a kamera modultól.

3.12. táblázat. Életszerűség érzékelés funkció

Életszerűség érzékelés funkció	
Leírás	A rendszer ellenőrzi a felhasználónak a valódi személy létét.
Kiváltás	A kamera modul elküldi a képkockákat.
Funkcionális követelmény	Az arcfelismerést követően megvizsgálja az életszerűség modul, hogy a kamera előtt álló személy egy bizonyos küszöbérték alatt vagy felett rendelkezik az élőség érzékelésénél, ha fölött van, akkor az eredmény, hogy élő személy és továbbítódik egy üzenet a kamera modulnak, hogy sikeres a belépés, ellenkező esetben hamis, nem valódi személynek lesz besorolva és a nem sikeres belépés üzenet kerül elküldésre.
Megszorítás	Az arcfelismerő modulnál sikeres megegyezés a rendszerben levő felhasználók között.

3.4. Nem funkcionális követelmények

Ezek a követelmények az rendszer általános minőségi jellemzőire és korlátozásaira vonatkoznak, nem a rendszer funkcionális működésére. Az alá részletezett csoportokba sorolhatóak az arcfelismerő rendszer nem funkcionális követelményei.

3.4.1. Teljesítmény követelmények

Teljesítmény szempontjából a rendszernek minél gyorsabb válaszidő elérésére van szükség, képes kell legyen nagy adatmennyiségek feldolgozására, ehhez szükség van megfelelő stabil WiFi hálózati kapcsolatra a zökkenőmentes és gyors kommunikáció érdekében. Valamint még szükséges egy számítógép, ameleyn a rendszer futtat a Python 3.3 verziószámmal és a megfelelő könyvtárak letöltése, .

3.4.2. Továbbfejleszthetőségi és karbantarthatósági követelmények

Az alkalmazásnak képesnek kell lennie rugalmasan növekedni és alkalmazkodni a növekvő felhasználói igényekhez és terheléshez, ha a rendszert bővíteni kell, így új felhasználók kerülnek bevezetésre, ezt a mennyiségű adatkezelést is el fogja bírni a rendszer. Valamint a rendszer jól elkülönített modulokból áll, hogy egy hiba esetén könnyen orvosolható legyen.

3.4.3. Biztonsági követelmények

A rendszernek magas szintű biztonságot kell nyújtania a felhasználók számára az azonosítás és hitelesítés során, így a belépni vágyó személyek arcfelismerés segítségével és eletszerűség érzékelés sikeressége után juthatnak be.

3.4.4. Felhasználói élmény követelmények

A rendszernek egyszerű és könnyen használható élményt kell nyújtania a felhasználók számára, ezért a belépés úgy van megvalósítva, hogy a személynek ne kelljen fizikai interakciót, érintést alkalmaznia, csupán a kamera elé áll.

3.4.5. Felhasználói élmény adminként követelmények

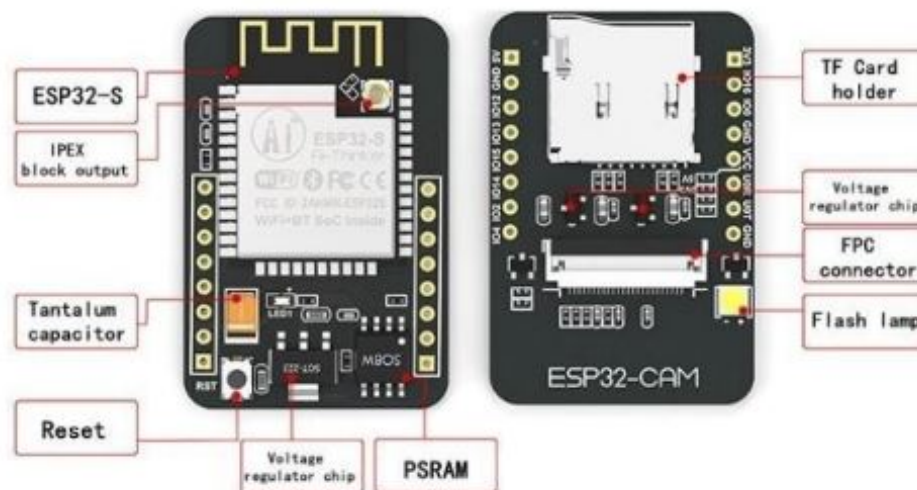
A felhasználói felületnek egyszerűnek, könnyen kezelhetőnek, átláthatónak és responszvnak kell lennie, ezért ajánlott a Bootstrap keretrendszer használata és a PHP szkriptek használata Xampp szerver futtatása segítségével.

4. fejezet

Részletes tervezés

4.1. ESP32-CAM modul

A rendszer fő komponense, mint már a fentiekben is említettem, az ESP32-CAM modul, ami egy olyan mikrovezérlő, amely az ESP32-S chipet tartalmaz. Az ESP32 az Espressif által kifejlesztett kétmagos chip, amely Wi-Fi és Bluetooth vezeték nélküli kommunikációt biztosít.

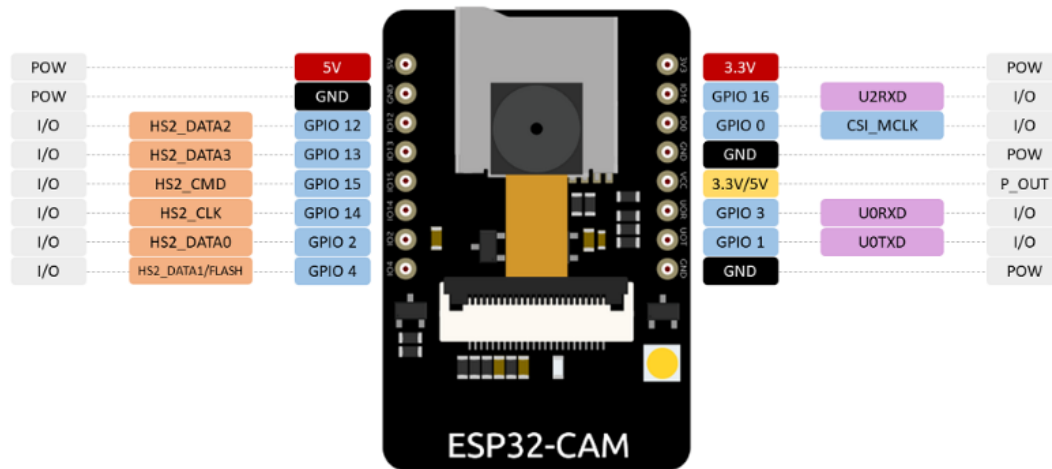


4.1. ábra. ESP32-CAM modul felépítése [F.1](#)

Az ESP32-CAM lehetővé teszi webserverek létrehozását, így egyszerűen összeállíthatóak megfigyelőkamera berendezések, amelyek integrálhatóak otthoni automatizálási rendszerrel. Képes arcdetektálást és arcfelismerést is elvégezni, valamint sok más projekt esetén hasznos lehet a Okos Otthon és az IoT (Internet of Things) területén. [\[14\]](#)

A pontos felépítése tartalmaz egy OV2640 kamerát, amely 2 megapixeles, 1600x1200 pixeles, képek elkészítését teszi lehetővé, valamint 10 hozzáférhető lábat nyújt a felhasználó rendelkezésére, a perifériák csatlakoztatásához. Illetve rendelkezik egy microSD kártya behelyezési lehetőséggel, így a kamera által készített képek vagy kliensek számára szolgáltatott fájlok könnyedén tárolhatóak. Rendelkezik beépített flash memóriával, amely

lehetővé teszi programok, képek és egyéb adatok tárolását. Az alábbi ábrán látható az ESP32-CAM modul lábkiosztása:



4.2. ábra. ESP32-CAM modul lábkiosztása [F.1](#)

A fontosabb szerepet betöltő lábak és funkciók a következők:

- VCC: az alkatrész táplálásához szükséges, és a modulra adott feszültséget jelenti
- GND: a földeléshez kapcsolódik, és a készülék elektromosan stabil működéséhez szükséges.
- U0T és U0R: az UART(Universal Asynchronous Receiver-Transmitter) kommunikációs portjának kimeneti és bemeneti lábai. Ezeket a lábakat használhatjuk a soros kommunikációhoz más eszközökkel.
- 3V3: 3,3 V-os tápfeszültséget szolgáltat a modulnak.
- IO0: a programozáshoz vagy a firmware frissítéséhez használjuk
- IO2: általában az SD kártyaolvasó vezérlésére van használva
- RESET: lehetővé teszi a modul visszaállítását az alapbeállításokra
- WiFi antenna: lehetővé teszi külső antenna csatlakoztatását a vezeték nélküli kommunikációhoz

A projektem megvalósításában az ESP32-CAM modult használtam, mint a rendszer központi egysége. Rajta keresztül történik meg az élő képkockák továbbítása, Wifi hálózatra csatlakozva és a megadott hálózati címen keresztül elérhetővé teszi a hozzáférést. A továbbított képkockák 800x600-as felbontásúak. Az alábbi kódrészlet [F.1](#) segítségével szemléltetem a képek felvételét és továbbítását megvalósító függvényt, ami előtt a szükséges könyvtárak hozzá vannak adva, valamint a hálózati csatlakozás létrejött:

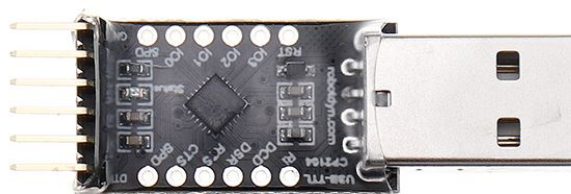
4.1. kódrészlet. ESP32-CAM képek felvétele és továbbítása

```
void serveJpg()
{
    auto frame = esp32cam::capture();
    if (frame == nullptr) {
        Serial.println("CAPTURE FAIL");
        server.send(503, "", "");
        return;
    }
    Serial.printf("CAPTURE OK");

    server.setContentLength(frame->size());
    server.send(200, "image/jpeg");
    WiFiClient client = server.client();
    frame->writeTo(client);
}
```

Első lépésben lekérjük a képfolyamot az `esp32cam::capture()` függvény segítségével, majd ezt követően megvizsgáljuk hogy a képkocka elkészítése ténylegesen sikerült, tehát nem nullpointer, ha hibát észlel, akkor az 503-a HTTP státusszal tér vissza, ha sikerül akkor a 200 státusz számot és a kép tartalmat a kliensnek. A képkockát kiírja a kliensnek a `frame->writeTo(client)` művelet segítségével, amely majd továbbítja azt a kliensnek.

A modulon alapjáraton nincsen hagyományos USB port, ezért egy TTL modul használatával lehet csatlakoztatni a számítógéphez, ami következő ábrán van szemléltetve:



4.3. ábra. TTL USB-soros átalakító

A CP2104 TTL UART modul egy USB-soros átalakító, amely hidat képez a számítógép USB-portja és a mikrovezérlő között.

A kameraképet egy TFT 128x160-as RGB LCD kijelzőn teszem láthatóvá, hogy a belépni vágyó személy láthassa megfelelő helyen áll-e a felismeréshez. A képernyő az alábbi ábrán látható:



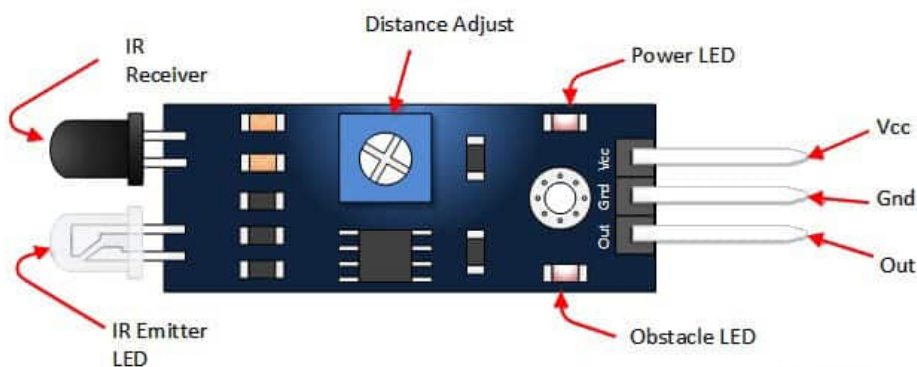
4.4. ábra. TFT LCD kijelző

A kijelző képes megjeleníteni színes képeket és grafikákat és SPI interfészen keresztül kommunikál a mikrovezérlővel, valamint az ST7735 chip felelős a kijelzővezérléséért.

A kamera modul alapjáraton alvó állapotban van (deep sleep), amelyet egy külső fizikai jelzésre felébresztünk. Ehhez a művelethez külső inputként egy Infra reflektív távolság szenzort használtam.

4.1.1. Infra reflektív távolság szenzor

Az MH-Sensor-Series Flying-Fish nevű infra reflektív távolság érzékelő alkalmazkodik a fényviszonyokhoz, rendelkezik infravörös kibocsátóval, illetve fogadóval. Amikor egy akadályt észlel, tehát van egy visszaverő felület, akkor a zöld LED felkapcsol. Széles körben használják az iparban robotok akadály elkerülése esetében, vonal számláláshoz, fekete-fehér vonal követéshez és számos más megvalósításhoz. A szenzor felépítése a következő ábrán látható:



4.5. ábra. Infra reflektív távolság szenzor felépítése [F.1](#)

Három pinje van: az OUT, amely közvetlenül köthető mikrovezérlő portjára, a VCC, a bemeneti tápfeszültségnek, és a GND, a földelésnek. A jeldetektálás érzékenysége állítható egy potenciométer segítségével, ez a távolság 2 és 30 cm intervallumban szabályozható, az érzékelés pontos szöge, az akadályt illetően pedig 35 fokok. A kamera modul felébresztését és elalvását a következő kódrészletben mutatom be:

4.2. kódrészlet. ESP32-CAM felébresztése és alvó állapota

```
void enableDeepSleep(){
    Serial.println("Deep sleep enabled");
    esp_sleep_enable_ext0_wakeup(WAKEUP_PIN, LOW);
    esp_deep_sleep_start();
}
```

A `enableDeepSleep()` függvényben beállítom a mélyalvásra történő felébresztést a `WAKEUP_PIN` segítségével. Ezután aktiválom a mélyalvást a `esp_deep_sleep_start()` függvény meghívásával. Majd a következő lépésben lekérem az aktuális időt, beolvasom a pin állapotát és ha az állapot `HIGH`, akkor azt jelenti, hogy a CAM modul felébredt. Ha `LOW`, akkor ellenőrizzük, hogy az utolsó felébredés óta eltelt idő meghaladja a `MINIMUM_WAKE_PERIOD_MILLIS` értéket (60 másodperc). Ha a meghaladja, akkor meghívódik a `gotoSleep` függvény, ami elindítja az alvó üzemmódot.

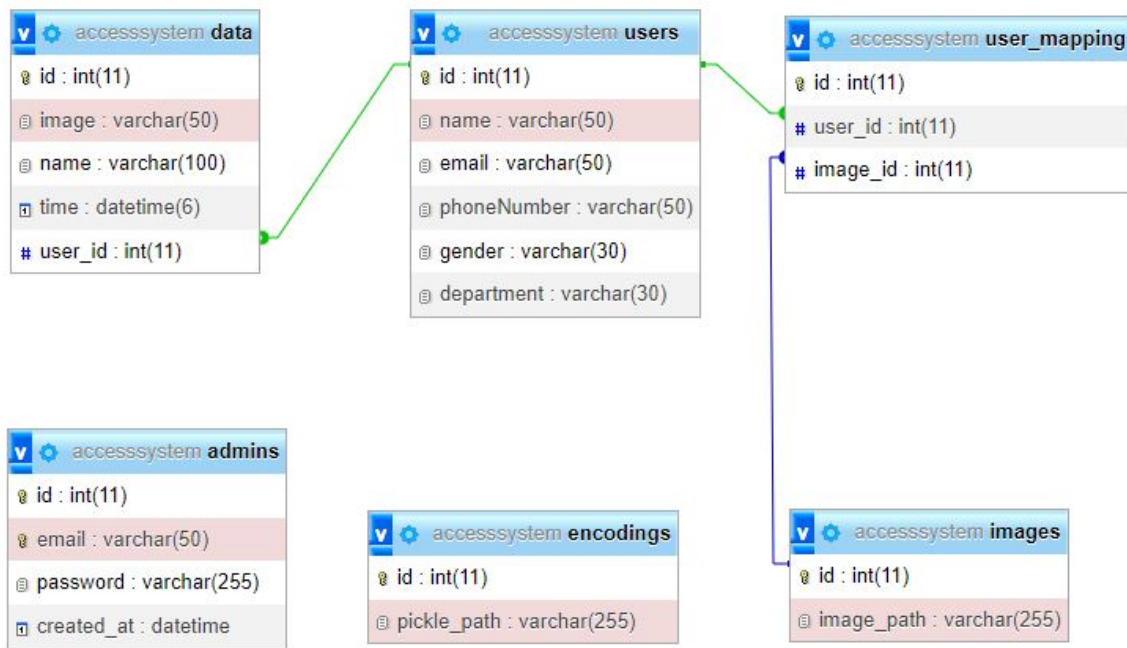
4.3. kódrészlet. ESP32-CAM felébresztése és alvó állapota

```
pinMode(WAKEUP_PIN, INPUT_PULLUP);
```

Beállítom a `GPIO_PIN_WAKEUP` lábat bemenetként.

4.1.2. Adatbázis-kezelő rendszer

Az adatok biztonságos és egyszerű tárolásához a MySQL nyílt forráskódú relációs adatbázis-kezelő rendszert választottam, ami széles körben ismert és használt. A fejlesztői környezetben gyakran alkalmazzák a megbízhatósága és hatékony adatkezelése miatt, akár nagy adatmennyiségek esetén is. Az adatbázisban látható táblákat és a közöttük levő kapcsolatokat a következő ábrán szemléltetem:



4.6. ábra. Adatbázis modell

1. Az **admins** tábla tartalmazza az adminisztrátor azonosítóját(id), email címét(email), jelszavát(password), és a profilja létrehozásának az időpontját (created_at).
2. Az **encodings** nevű táblában megtalálható az azonosító(id), illetve az arckódolókat tartalmazó pickle fájl elérési útja(pickle_path). Ez tartalmaz egy listát a rendszerben levő összes arckép 128 dimenziós arckódolásáról, illetve a hozzá tartozó személy nevééről.
3. A felhasználó adatainak tárolására a **user** táblát használom, ami tartalmazza a felhasználó azonosítóját(id), nevét(name), email címét(email), telefonszámát(phoneNumber), nemét(gender) és munkakörét(department).
4. A képekhez tartozó információkat az **images** táblában találhatjuk meg: a kép azonosítója(id), a kép fájl elérési útja(image_path). Az images és a user_mapping és a user_mapping és users táblák közötti kapcsolat lehetővé teszi hogy egy felhasználóhoz több kép is hozzá legyen rendelve.
5. A **user_mapping** tábla ennek következtében a felhasználó azonosítóját(user_id) és a kép azonosítóját tartalmazza(image_id).
6. A **data** táblában találhatóak a rendszerbe belépett személyhez társítható adatok: azonosító(id), fénykép(image), név(name), belépés pontos ideje(time), illetve a személy azonosítóját(user_id).

4.1.3. Arcfelismerő modul

Az arcfelismerés megvalósításához, a Python `face_recognition` könyvtárát alkalmaztam, amely a `Dlib` és `OpenCV` könyvtárakat használja a pontos és hatékony arcdetekcióhoz és arcfelismeréshez. A könyvtár részletes leírásának és funkcióinak tanulmányozásához az Adam Geitgey: Face Recognition github oldalát használtam [6], amely alapjaira építettem fel az arcfelismerő modulom kódját. Az arcok észleléséhez a `Dlib` HOG algoritmusát alkalmaztam, ami az arcok jellegzetes alakját és textúráját használja a detektáláshoz, ez az algoritmus egy előre betanult modellt használ, ami `ResNet` segítségével valósult meg. Ugyanarról a személyről készült két különböző képnek nagyon hasonló a kódolása, és két különböző embernek teljesen eltérő a kódolása, mivel különbözőek az arcvonásaik és egyediek. Minden ember arckódolását egy 128 dimenziós vektorban tároljuk, például egy adott személy arckódolása a következőképpen nézhet ki:

```
[-0.13132419  0.02472093  0.02014901 -0.07782259  0.02326948 -0.05741551
-0.02088581 -0.0920793  0.10156108 -0.1509438  0.17178449 -0.04773222
-0.27832264 -0.01937654 -0.061489  0.1693414 -0.13475136 -0.14730313
-0.16759585 -0.05530329  0.04455725  0.07321294  0.01638173  0.14383592
-0.04087877 -0.33222267 -0.1008816 -0.08387823 -0.10978469 -0.09017216
 0.0886569  0.03340603 -0.10086253  0.03351042  0.0229741  0.09323654
-0.01905034 -0.1510416  0.20501204  0.00139503 -0.26228091 -0.02550532
 0.10922007  0.30092797  0.23804064 -0.00813567 -0.01505752 -0.06718352
 0.16171804 -0.3178378  0.02950494  0.12509316  0.01910315  0.12553313
 0.099477 -0.18221319  0.06298522  0.18745475 -0.21321936  0.02968143
-0.04337997 -0.16527195  0.08974091 -0.06006373  0.19923851  0.13365649
-0.19234926 -0.12136683  0.23777457 -0.24089518 -0.02411565  0.11206377
-0.13711785 -0.23564905 -0.27692622  0.02055722  0.358298  0.20660131
-0.09296207  0.04048689 -0.05009681 -0.03320209  0.00572491  0.23460524
 0.02521258 -0.02547138 -0.07579754  0.0023976  0.21616623  0.06513755
-0.08013825  0.29804528 -0.0393314 -0.05207748  0.06383666  0.11051901
-0.13839963 -0.03770785 -0.14360979  0.02200669 -0.08801195 -0.06904167
-0.00992454  0.09092753 -0.10284273  0.18784982 -0.06222714  0.01092728
-0.07533871 -0.01031715  0.00130794  0.02129768  0.12582421 -0.22807105
 0.17440389  0.14777312  0.1178188  0.18854006  0.01049358  0.09915299
-0.00735098 -0.10857491 -0.22500677 -0.05378329  0.01345587  0.02587205
 0.07043982  0.04995482]
```

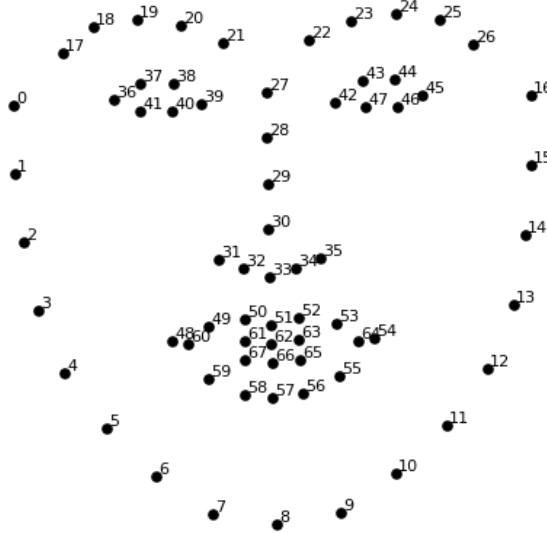
4.7. ábra. Arckódolás példa

Ennek a modulnak az implementálását a `face_recognition.py` `recognize_faces` nevű függvényében valósítottam meg. Első sorban elvégezzük a beolvasott képkocka előfeldolgozását, ami magába foglalja az eredeti kép(image) átkonvertálását a BGR színtérből az RGB színtérbe, és az eredményt a `rgb_image` változóba mentem el, a képek átméretezését pedig az `imutils` könyvtár `resize` függvényével oldottam meg, ezzel optimalizálva a feldolgozási sebességet.

4.4. kódrészlet. Beolvasott képkocka előfeldolgozása

```
rgb_image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
rgb_image = imutils.resize(image, width=750)
r = image.shape[1] / float(rgb_image.shape[1])
borders = face_recognition.face_locations(rgb_image, model='hog')
encodings = face_recognition.face_encodings(rgb_image, borders)
```

Az arc kódolásainak meghatározásához a a háttérben felhasználásra kerül egy előre betanított model ami az 68 jellegzetes pontját foglalja magába. Ez az alábbi árbrán látható:



4.8. ábra. Arc jellegzetes pontjai példa

Ezt követően végigmegyünk az encodings listán összehasonlítva az adott arckódot(encoding) az data változóban tárolt arckódokkal és nevekkal, amit előre már betöltöttünk az encoding.pickle fájlból, és meghatározzuk, hogy az adott arckód melyik archoz tartozik.

Az összehasonlítás a `compare_faces()` függvény segítségével történik, ami az előbb említett két paramétert hasonlítja egy bizonyos küszöbérték mellett, ami alapértelmezetten 0.6 a `face_recognition` modulban. A küszöbérték választása függ az adathalmaz változatosságától és az azonosítási pontosság céljától, általában az értéke 0.6 vagy 0.5 körül van. Ha nagy a változatosság és különböző körülmények között rögzített arckódok találhatók, akkor egy magasabb tolerancia értéket ajánlott használni.

A `compare_faces()` függvény az arctávolságok kiszámításához meg kell határozza euklidészi távolságot minden aktuálisan a kameraképen levő arc kódolása és a már ismer el-tárolt arcok kódolása között, ez a távolság jelzi, mennyire hasonlóak az arcok egymáshoz. Euklidészi távolság általános képlete:

$$d(p, q) = \sqrt{\sum_{i=1}^n (q_i - p_i)^2} \quad (4.1)$$

Az összehasonlítás eredményeként a függvény egy boolean értékeket tartalmazó listát térít vissza.

Ha egyezést találunk, akkor az archoz tartozó nevet hozzáadja a `names` listához, ami a már eddig hozzáadott személyek neveit tartalmazza. Ez úgy történik, hogy kiválasztjuk a leggyakoribb nevet az archoz illő javasolt nevek közül. Ha a személyt sikeresen azonosítottuk, akkor következik az éloszerűség ellenőrzése, amit a 4.1.4 pontban ismertetek részletesen. Ha ez is sikeresen "Real", azaz élő arc üzenettel tér vissza, akkor a belépés megtörténhet, így értesítjük a kamera modult, hogy kinyílhat a zár. Majd ezt követően a legutóbb felismert személy nevét beszúrjuk az adatbázisba a pontos idővel együtt, ha nem ismert személyt találunk akkor a listában az "Unknown" értéket adjuk hozzá és nem

illesztjük be az adatbázisba. A belépett személyek belépési adatait az adatbázisban a már fentebb említett data táblában tároljuk.

4.1.4. Élő arc észlelő modul

Az arcok élőségének felismerésére az OpenCV DNN modelljét alkalmaztam. Ez egy Caffe (Convolutional Architecture for Fast Feature Embedding) keretrendszerben előre betanított modellt jelent. Az alkalmazás létrehozása során, mint már a fentiekben is említettem [2.2.3](#), az általam tanulmányozott hasonló megvalósítások közül a [\[13\]](#) webkameráról élő arc felismerő applikáció szolgált alapul.

A beolvasott frame méreteit a eltároljuk a h és w változóknban, majd átméretezzük 300x300-asra, majd létrehozunk egy blob objektumot a cv2.dnn.blobFromImage függvénnyel. A blob készítésekor normalizáljuk és átalakítjuk a képet, hogy megfeleljen a hálózat bemeneti követelményeinek, ami magába foglalja a következő paramétereket: a bemeneti kép, a skálázási faktor (1.0), méret(300x300), illetve az RGB értékek átlaga, amelyekkel a bemeneti képet normalizáljuk((104.0, 177.0, 123.0)). Ez után átadjuk az objektumot a detektornak, amit az alábbi kódrészlet szemléltet:

4.5. kódrészlet. Elő felismerés előfeldolgozás

```
image = imutils.resize(image, width=600)
(h, w) = image.shape[:2]
img_blob = cv2.dnn.blobFromImage(cv2.resize(image, (300, 300)), 1.0,
                                  (300, 300), (104.0, 177.0, 123.0))

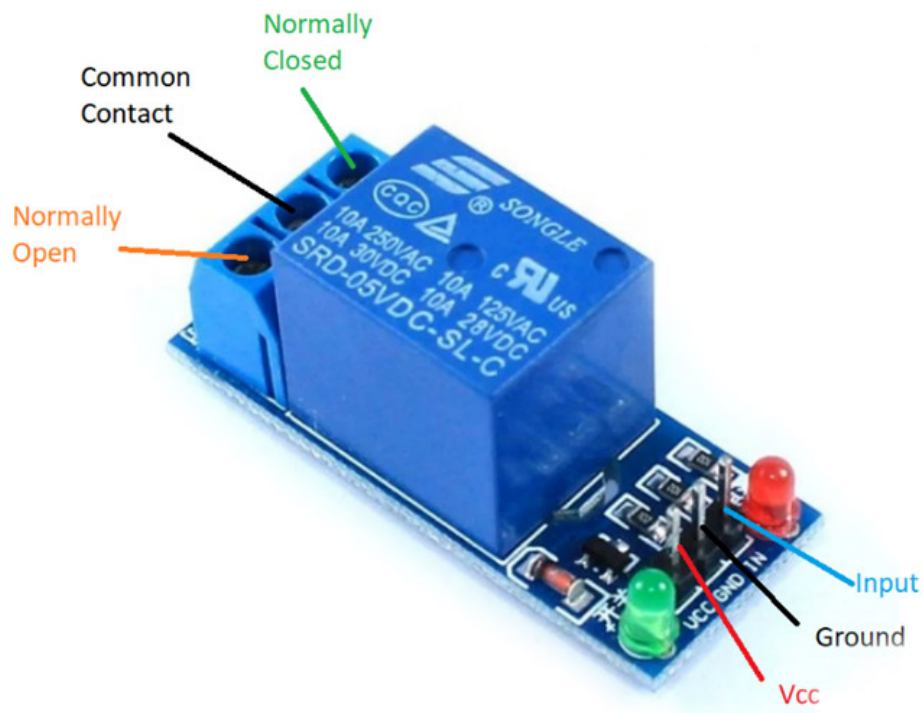
net.setInput(img_blob)
detections = net.forward()
```

Végig iterálunk a detektált arcok listáján majd kiszűrjük közülük a gyengén detektáltakat, amik egy bizonyos konfidencia szint alá esnek. Kinyerjük az arc határoló dobozának a koordinátáit, és kiválasztjuk relevánsnak vélt területeket (ROI-Region of Interest). A modell segítségével prediktáljuk az életszerűséget a model.predict metódussal, majd innen meghatározva a label változóból, hogy élő(real) az arc, vagy hamis(fake). Ennek implementálása a face_recognition.py detect_liveness függvényben történik.

4.1.5. Relé vezérlése

A fent említett üzenetet fogadom az ESP32-Cam modulon, ha sikerült az arcfelismerés és az élő detektálás. Majd ennek következtében egy 5 Voltos relé állapotát megváltoztatom, aminek segítségével majd a továbbiakban csatlakoztatni lehet a körülményekhez alkalmazkodva megfelelő zárat vagy eszközt amit a relé vezérelni fog.

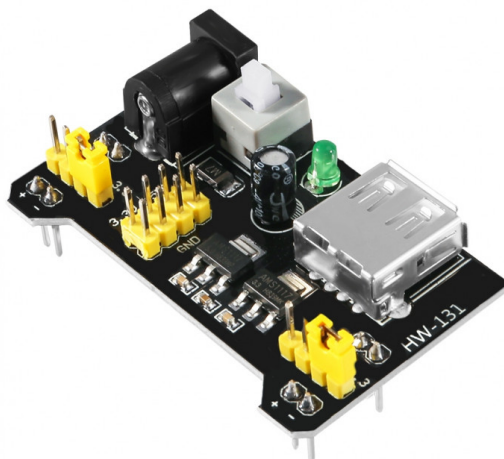
A relé két részből tevődik össze: egy vezérlőoldal és egy terhelésoldal. A vezérlőoldalhoz csatlakoztatom az ESP32-cam digitális kimenetét, amelyen keresztül vezérelni fogom a relét, a másik oldalához majd tetszés szerint lehet a vezérelni kívánt berendezést csatlakoztatni. Az 5 voltos relé felépítése a következő ábrán megtekinthető:



4.9. ábra. Relé felépítése

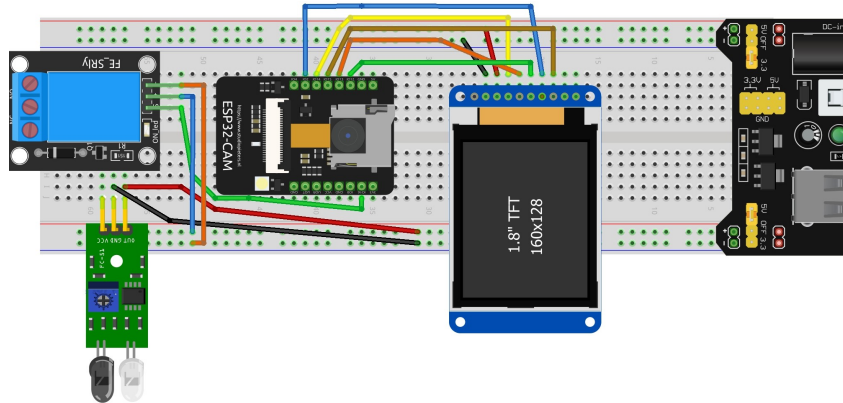
4.1.6. Teljes rendszer bemutatása

A rendszer áram ellátása biztosításához egy tápegységet használtam, amely egy bemeneten keresztül képes energiát fogadni, akkumulátorból, 12V-os adapterből, vagy más forrásból. Majd ezután 3,3V-os és 5V-os feszültséget szolgáltat az áramkörnek. Ez a következő ábrán látható:



4.10. ábra. Tápegység felépítése

A TFT kijelzőnek 3,3V-os feszültség szükséges, a többi áramköri elem, pedig az 5V-os feszültséget használja a működéshez. A rendszer beindulásához egy személy szükséges elé álljon, ezt érzékeli az nfra reflektív távolság szenzor, ennek következményében felébred az ESP32-CAM modul, majd elkezdődik a képkockák folyamatos továbbítása az arcfelismerő modul felé, és a kijelzőre. Ha az arcfelismerés sikeres volt, akkor a kamera modul segítségével a relé HIGH állapotba kerül és megtörténhet a belépés. Az alábbiakban látható a teljes rendszer kapcsolási rajza:



4.11. ábra. Teljes rendszer kapcsolási rajza

4.1.7. Webalkalmazás tervezése

A Webalkalmazás megvalósításához több különböző technológiát alkalmaztam. Az alapvető felépítést HTML (Hypertext Markup Language) nyelv segítségével hoztam létre, ez felelős a strukturált tartalom megjelenítéséért, például képek, szövegek vagy egyéb különböző elemek. A Bootstrap keretrendszer felhasználása a reszponzív elrendezés alapját nyújtja, rengeteg előre elkészített UI komponenst tartalmaz, mint például gombok, navigációs sávok, kártyák, űrlapok. Emellett különböző előre elkészített témákat és testreszabási lehetőségeket is kínál, amelyek használatára a weboldalak saját egyedi stílusra szabhatóak. Ehhez kiindulópontként a ThemeWagon Securex nevű [15] sablonát alkalmaztam a felhasználói felület egyszerűbb és gyorsabb létrehozása végett.

A felhasználói interakciók kezeléséhez és az adatok dinamikus feldolgozásához a PHP nyelv használata segített, ami egy szerveroldali nyelv, lehetővé teszi a dinamikus és interaktív webes alkalmazások készítését. Segítségével a fejlesztők adatokat küldhetnek és fogadhatnak az adatbázisokból, kezelhetik a felhasználói űrlapokat, valamint különböző logikai illetve számítási műveleteket végezhetnek el. A felhasználói szerepek kezelésére PHP szessziókezelést alkalmaztam. A felhasználói adatok biztonságos tárolása érdekében a PHP lehetőséget biztosít a jelszavak hashelésére. Ez azt jelenti, hogy a jelszavakat nem tárolják tisztán, hanem egy irreverzibilis hash-függvény segítségével átalakítják. Így megakadályozva hogy a jelszavak könnyen visszafejthetőek legyenek, még akkor is, ha a támadó hozzáférést szerez az adatbázishoz.

A lokális webservert létrehozásához a XAMPP nyílt forráskódú szoftvercsomagot használtam, ami egy Apache webszerver, amely felelős a HTTP kérések fogadásáért és a webes tartalmak szolgáltatásáért, illetve MySQL adatbázis kezelő rendszer hozzáférést biztosít, amit fentebb már ismertettem a 4.1.2 alfejezetben.

Az interaktív elemek működésének egy része JavaScript segítségével került implementálásra.

Egy funkcionalitás megvalósítása a következőképpen történik:

- Az alkalmazásom főoldal index.php kódjában vannak implementálva a menü pontok, ha újabb funkciót szeretnénk hozzáadni, akkor itt tehetjük meg.
- Minden egyes funkcionalitásnak a végrehajtó kódját egy külön php fájlban írjuk meg, ez alapértelmezetten tartalmazza az említett HTML sablon kódját. A sablon tartalmi részében, pedig megírjuk a szükséges kódot, és HTML választ generálunk.

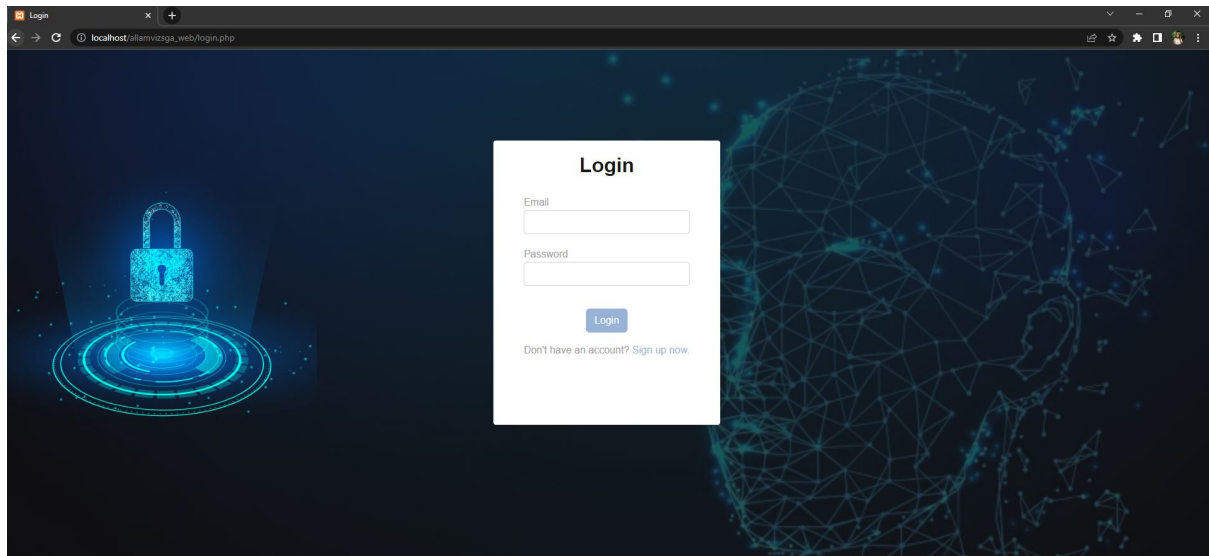
A webalkalmazás megvalósításához a 3.3 pontban említett funkcionalításokat implementáltam és az előzőleg bemutatott adatbázist használtam.

Minden egyes funkcionalitáshoz megírtam a megfelelő szkriptet, amelyek a következők:

- Regisztrálás: registration.php
- Bejelentkezés: login.php
- Kijelentkezés: logout.php
- Jelszó megváltoztatás: resetPassword.php
- Felhasználók listájának megtekintése: profile.php
- Felhasználók profiljának megtekintése: profileDetail.php
- Új felhasználó hozzáadása: createProfile.php
- Felhasználó törlése: deleteProfile.php
- Felhasználó profiljának módosítása: updateProfile.php
- Belépett személyek listájának megtekintése: service.php
- Kapcsolatfelvétel a szolgáltatóval: contact.php

A felület könnyen átlátható és kezelhető, az adminisztrátorok számára készült, akik karban tartják és felügyelik a rendszer működését. Az alábbiakban bemutatom a Webalkalmazás fontosabb oldalait:

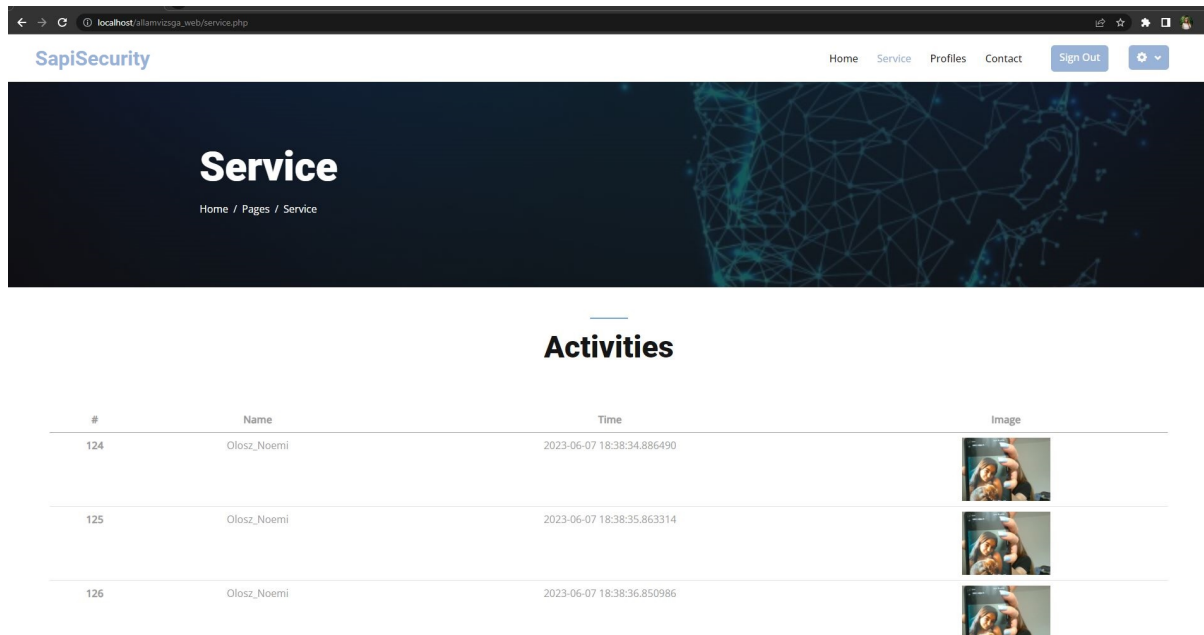
Bejelentkezés



4.12. ábra. Bejelentkezés

Az admin a főoldalon a bejelentkezési űrlapban kitölti a mezőket. Az email címére és a jelszávara lesz szükség. Ezt követően pedig megnyomja a "Login" gombot a bejelentkezéshez, ha még nincs regisztrálva akkor át navigál a regisztrációs oldalra és ott majd elvégzi a regisztrációt az email címe és egy jelszó segítségével. A belépést követően lehetősége nyílik az oldal megtekintésére. Ha a jelszavát szeretné megváltoztatni, akkor az is megteheti a jobb felső sarokban levő ikont megnyomva legördülő opcióval.

Rendszerbe belépett személyek

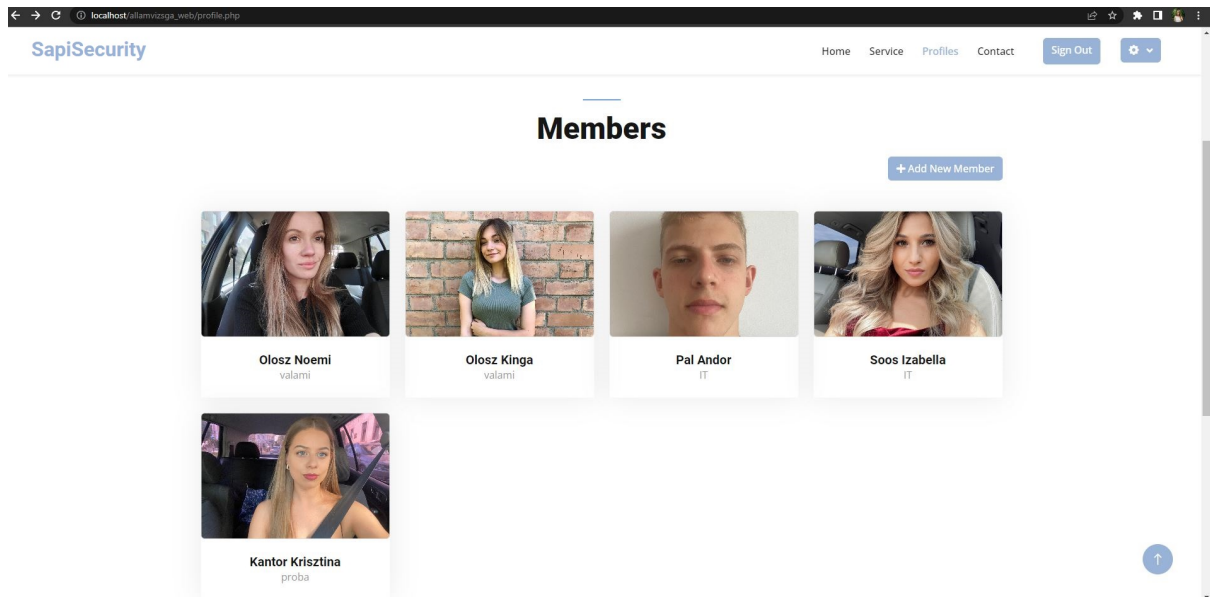


4.13. ábra. Rendszerbe belépett személyek listája

Az egyszerű követhetőség érdekében, a Service oldalon megtekinthetőek a rendszerbe belépett személyek aktivitása, ez a fenti ábrán van szemléltetve. Tartalmazza a belépett személy nevét és pontos belépési időpontot, időrendi sorrendben megjelenítve.

Ezt követően az adminisztrátor létrehozza a rendszerbe belépni jogosult személyek listáját. Majd minden létrehozott profilhoz hozzáadja a megfelelő képeket a "Take Picture" gomb megnyomásának segítségével, amely a kameráról három képkockát ad hozzá a személyhez.

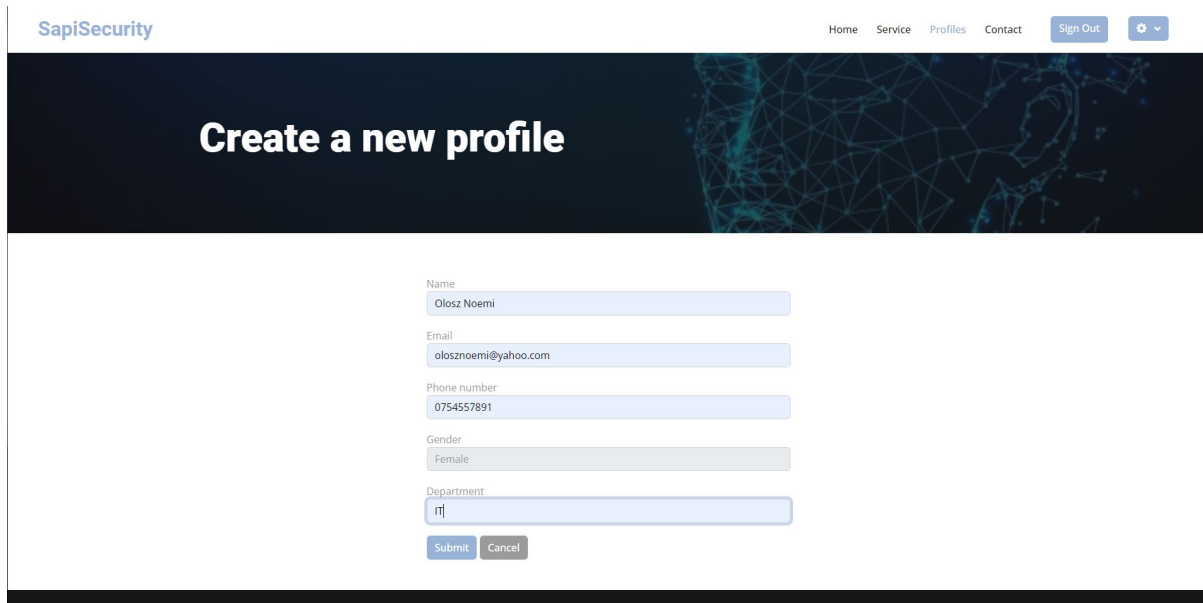
Rendszer aktív felhasználói



4.14. ábra. Rendszer aktív felhasználói

Az admin megtekintheti a már eddig hozzáadott profilok listáját. A különböző profiloknál látszik a profilhoz tartozó kép, név, illetve munkakör. Szükség szerint ha új felhasználói profilt szeretne létrehozni, akkor az "Add New Member" gombra kattintva megteheti ezt, illetve törölheti az egyes profilokat a kép jobb felső sarkában megjelenő szemetes ikonra kattintva. Továbbá megnézheti a bizonyos személyek részletes profilját a képükre kattintva.

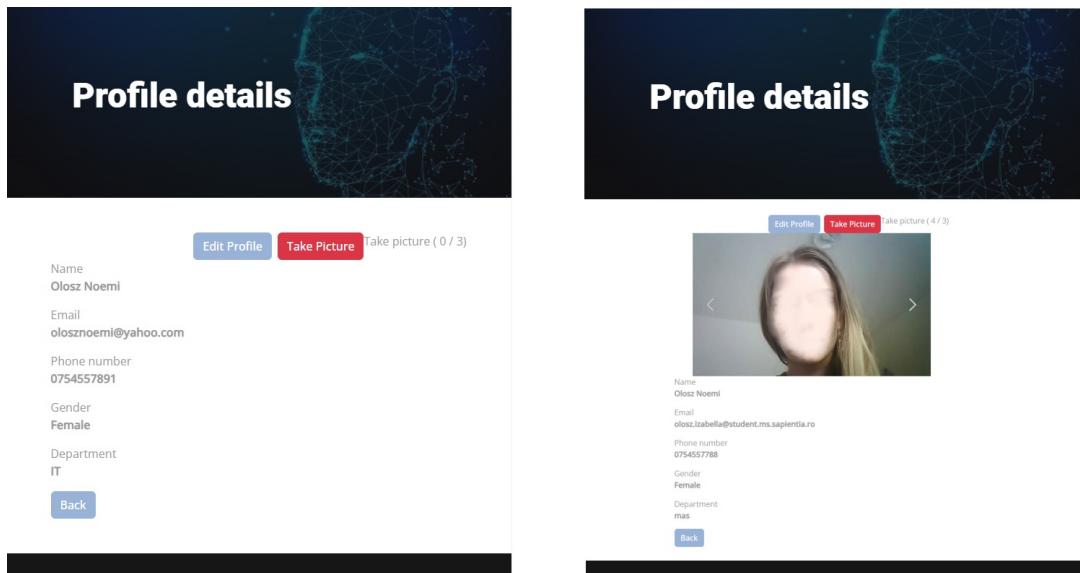
Új felhasználó hozzáadása



4.15. ábra. Új felhasználó hozzáadása

Új felhasználó hozzáadáshoz a már fent említett "Add New Member" gombra kattintva kerülünk a createProfile oldalra, ahol kitöltjük az űrlapot a szükséges adatokkal, majd a "Submit" gombra kattintva elküldjük.

Új felhasználó hozzáadása



4.16. ábra. Új felhasználó képek hozzáadása

Majd ezt követően a fényképeket a "profileDetail" nevű oldalon adhatjuk hozzá a személyhez a "Take Picture" gomb megnyomásával aminek hatására a kamera az előtte álló személyről három képkockát rögzít és ad hozzá a profiljához, ami meg is jelenik egyből, ezt a fennebbi [4.16](#) ábrán szemléltetem.

5. fejezet

Üzembe helyezési lépések

5.1. Felmerült problémák és megoldásaik

Az arcfelismerés során számos tényező befolyásolhatja ennek a folyamatnak a pontosságát és hatékonyságát. A következő általánosságban ismert problémák léphetnek fel az arcok detektálása során:

- Megvilágítás: a fényviszonyok változása nagy mértékben befolyásolhatja a felismerés folyamatát, fény hiányában a rávetült árnyékok vagy erős irányított fényforrások nehezíthetik és gyengíthetik a pontosságot
- Eltérő arc pozíció: az arcképek különböző pozíciókból vagy távolságokból készülnek
- Eltakarás,elfedés: például szemüveg viselete megnehezíti az azonosítást
- Hamis személyazonosság: gyakran előfordul, hogy a belépni nem jogosult személyek hamis ellopott személyazonossággal próbálnak belépni, például képek felmutatásával
- Öregedés: az emberi arc nagy mértékű változásokon mehet keresztül az évek eltelte során, például a bőr ráncosodása
- Rezolúció és zaj: Az alacsony felbontású képek esetén az arcvonások részletei elveszhetnek vagy torzulhatnak, illetve a zajos képek nehezebben értelmezhetőek
- Etikai és adatvédelmi kérdések: az emberek személyes adatainak védelme(GDPR jogok)

A rendszer tervezése és megvalósítása során én személyesen a fényviszonyok problémájával ütköztem, ennek megoldására, amint a nem funkcionális követelményekben is említettem egy megfelelő fényforrás felszerelése szükséges a rendszer fölé. Az illetéktelen személy behatolását megelőzően használtam az élő személy ellenőrzést. A szemüveget viselő felhasználók esetében a rendszerbe eltárolt képekhez szemüveget viselés közben készült képeket is hozzáadtam. Az öregedés ellen pedig hosszútávú megoldás lehet ha rendszerben lévő felhasználókról bizonyos időközönként frissítjük a képeket, például 3 évenként el, de erre nincsen pontos meghatározható idő, mivel minden egyén testének változásai eltérőek, ez a frissítés megoldja az esetleges

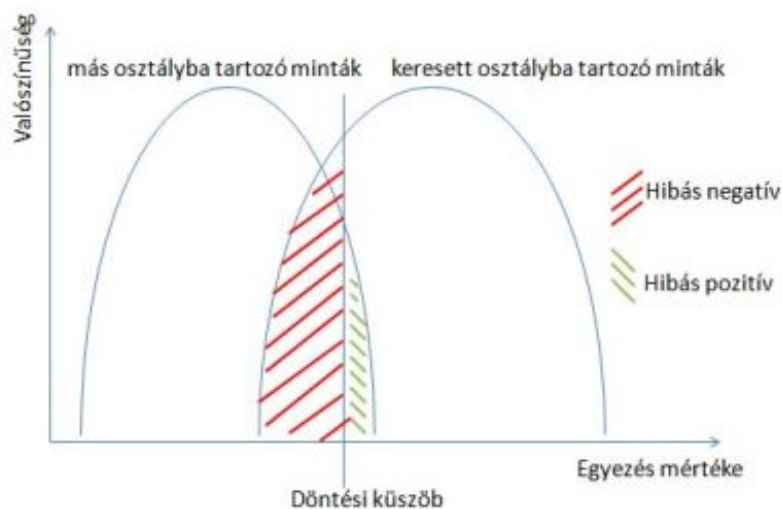
balesetek vagy plasztikai beavatkozások során keletkezett elváltozások kezelhetőségét. Az általam használt kamera modul felbontásával nem észleltem problémákat a megvalósítás során. A személyes jogok védelme érdekében az adatokat biztonságosan tároltam, illetve képeiket és adataikat csak kutatási célokra használtam az államvizsga dolgozatom elkészítése során.

5.2. Kísérleti eredmények, mérések

Egy biometria azonosító rendszer felhasználói számára rendkívül fontos a megbízhatóság. Ez egy összetett kérdés, mivel különböző típusú hibák léphetnek fel. Minden osztályozás esetén felmerülhet a probléma, hogy hibát követ el a rendszer, például nem mindig sorolja be a megfelelő a felismerendő személy mintáját, korábban látott minta által meghatározott osztályba. Ha nem történik hiba elkövetés, akkor az egyezés esetén a minta pozitív lesz, ha nincs egyezés, akkor pedig negatívként jellemezzük. A döntési hibákat két nagy csoportra lehet felosztani:

1. hibás/fals pozitív(FP)
2. hibás/fals negatív(FN)

Az első esetben egyezést mutatott a rendszer, pedig nem lett volna szabad, mivel az összehasonlított minták más személyhez tartoznak, ez egy nagyobb problémát jelent a megvalósításra nézve. A második esetet tekintve, pedig nem talált megegyezést a minták között, azonban az ott volt[4]. Az egyezés mértékének valószínűségét a következő ábra szemlélteti:



5.1. ábra. Egyezések valószínűsége [4]

A fent említett két hiba típus összefüggésben áll egymással, egyik csökkenése a másik növekedését fogja okozni és ezt a döntési küszöb segítségével befolyásolhatjuk. Így kiszűrhetjük egy bizonyos küszöb érték alatt levő mintákat, ellenkező esetben pedig elfogadjuk

helyesnek ítélve. Ezt mutatja be a fenti ábra. Ha a rendszer helyesen működik akkor azt a következő osztályozókkal jellemezzük:

1. igaz/fals pozitív(TP)
2. igaz/fals negatív(TN)

Első állítás esetén felismerésre került a minta, ami a személyhez tartozik, második esetben pedig a minta negatív és ezt az osztályozó is annak titulálja. Az alábbi ábrán látható konfúziós mátrixon szemléltetem az osztályozó algoritmusokat:

		Actual values	
Predicted values		TP	FP
		FN	TN

5.2. ábra. Konfúziós mátrix

Az rendszert beltéri fényviszonyok mellett teszteltem, amelyben figyelembe vettem az élő személyek felismerését, valamint az azonosítást, ahol az adatbázisban levő képekkel vettem össze. A teszt képeket is a kamera modul segítségével készítettem, így egyforma az felbontásnak köszönhetően könnyebb lesz a képek feldolgozása.

Az alábbi képletek [5] elvégzésével jutottam az eredmények pontos kiszámolására:

$$\text{Igaz pozitív arány(TP rate)} = \frac{\text{helyesen osztályozott pozitívák száma}}{\text{összes pozitívák száma}}$$

$$\text{Hamis pozitív arány(FP rate)} = \frac{\text{helytelenül osztályozott negatívák száma}}{\text{összes negatívák száma}}$$

$$\text{Precízió(precision)} = \frac{\text{igaz pozitívák száma}}{\text{igaz pozitívák száma} + \text{igaz negatívák száma}}$$

$$\text{Pontosság (accuracy)} = \frac{\text{igaz pozitívák száma} + \text{igaz negatívák száma}}{\text{összes pozitívák száma} + \text{összes negatívák száma}}$$

A valós működést 5 személyen próbáltam ki, melyekről 3-3 képet rögzítettem az adatbázisban. A rendszerbe való regisztrálást követően és a képek feltöltése után ellenőriztem a funkciókat.

5.1. táblázat. Arcfelismerési tesztek eredményei

Teszt neve	igaz pozitív arány	hamis pozitív arány	precízió	Pontosság
Azonosítás	$\frac{22}{25} = 0.88$	$\frac{0}{15}$	$\frac{23}{23 + 10} = 0.69$	$\frac{23 + 10}{25 + 15} = 0.82$

Az azonosítás része magasabb pontossági eredményeket nyújtott, az összes tesztesetet illetően, azaz 25 alkalommal teszteltem a pozitív találatok számát, ebből csupán 3-szor, tévedett, vagyis nem ismert fel egy már regisztrált személyt. Egyszer sem fordult elő olyan, hogy egy adott személyt aki nincsen regisztrálva felismerjen. A negatív felismerési arányra összesen 15 kísérlet volt, amiből 5-ször előfordult, hogy egy regisztrált személyt a bizonyos arc pozíciók vagy fényvetülések következtében nem ismert fel a rendszer.

5.2. táblázat. Élő arc felismerési tesztek eredményei

Teszt neve	igaz pozitív arány	hamis pozitív arány	precízió	Pontosság
Elő arc detektálás	$\frac{16}{25} = 0.64$	$\frac{7}{15} = 0.46$	$\frac{16}{16 + 8} = 0.66$	$\frac{16 + 8}{25 + 15} = 0.6$

Az azonosítás része alacsonyabb pontossági eredményeket nyújtott, a teszteseteket illetően, azaz 25 alkalommal teszteltem a pozitív találatok számát, ebből 16-szor adott helyes választ, vagyis felismert egy már regisztrált személyt. 7-szer fordult elő olyan, hogy egy adott képet személyként felismerjen, akinem egy élő ember. A negatív felismerési arányra összesen 15 kísérlet volt, amiből 5-ször előfordult, hogy egy élő személyt a bizonyos arc pozíciók vagy árnyékok miatt a rendszer nem azonosította élő személyként.

A továbbiakban célom a rendszer tesztelése nagyobb adathalmazokon, változatosabb környezeti tényezőkkel.

6. fejezet

Következtetések

6.1. Megvalósítások és Továbbfejlesztési lehetőségek

A diplomamunkámként választott téma keretein belül sikerült megvalósítanom egy biometrikus beléptető rendszert ESP32-CAM modul segítségével, amely arcfelismerésen alapul. Szerettem volna megkönnyíteni az épületekbe belépni vágyó személyek azonosítását, kiszűrve az engedély nélküli illetéktelen behatolókat.

Célkitűzéseim között szerepelt egy könnyen kezelhető, hatékony és első sorban biztonságos rendszer megvalósítása, ami nagymértékben sikerült is. Így nincsen szükség hosszú, bonyolult jelszavak és PIN kódok memorizálására, amik könnyen kitudódhatnak, feltörhetőek, vagy kulcsok és kártyák sokaságára, amik elveszíthetők vagy ellophatóak. Ezekre megoldást nyújt az arcfelismerésen alapuló beléptető rendszer, amely kevésbé sebezhető más biztonsági intézkedésekkel szemben.

Az általam megvalósított rendszer még további fejlesztési lehetőségeket igényel, az élő arc felismerés még további pontosításokra szorul, hogy az alkalmazás helyesebben és gyorsabban működjön. Valamint a továbbiakban a tesztelést is szeretném elvégezni nagyobb adathalmazon a pontosabb mérési számítások elvégzése érdekében.

A rendszer könnyen bővíthető új modulokkal, amik a még nagyobb biztonság érdekében szolgálnák, például más biometrikus azonosítást alkalmazva. A felhasználói felületet is ennek következtében bővíteni lehetne, és a optimalizálni az arcfelismerési módszereket nagyobb adatok feldolgozására

Összegzésképpen elmondhatom, hogy sikerült kivitelezni egy olyan élő arcfelismerésen alapuló beléptető rendszert, amely eleget tesz a 21.század technológiai elvárásainak, egyszerűen kezelhető a felhasználók számára, megkönnyítve a belépést. Mindezt egy költség hatékony módon, így több ember számára elérhetővé válhat.

Irodalomjegyzék

- [1] A. Agape. Internet-enabled access control system using a mobile application. *International Conference on System Theory, Control and Computing*, 2018.
- [2] J. Anil K.-Patrick Flynn-Arun A. Ross. *Handbook of Biometrics*. 2008.
- [3] T. Bagchi, A. Mahapatra, D. Yadav, D. Mishra, A. Pandey, P. Chandrasekhar, and A. Kumar. Intelligent security system based on face recognition and iot. *Materials Today: Proceedings*, 62:2133–2137, 2022.
- [4] L. Czúni. Biometria a számítógépes személyazonosításban. *Pannon Egyetem*, 2015.
- [5] T. Fawcett. An introduction to roc analysis. *Pattern recognition letters*, 27(8):861–874, 2006.
- [6] A. Geitgey. Face recognition. https://github.com/ageitgey/face_recognition/, 2018. [Online; accessed 20-June-2023].
- [7] A. Jadhav, S. Lone, S. Matey, T. Madamwar, and S. Jakhete. Survey on face detection algorithms. *Int. J. Innov. Sci. Res. Technol*, 6:291–297, 2021.
- [8] H.-K. Jee, S.-U. Jung, and J.-H. Yoo. Liveness detection for embedded face recognition system. *International Journal of Biological and Medical Sciences*, 1(4):235–238, 2006.
- [9] K. Khairwa, A. and Abhishek, S. Prakash, and T. Pratap. A comprehensive study of various biometric identification techniques. *Third International Conference on Computing, Communication and Networking Technologies*, 2012.
- [10] C. Körmöczi. *Integrált biometrikus azonosító rendszerek-Irodalomkutatás kötet*. Addison-Wesley Professional, 1st edition, 2011.
- [11] S. Mark. *Information security principles and practice*. Wilfey-Interscience, 1st edition, 2011.
- [12] P. Nagrath, R. Jain, A. Madan, R. Arora, P. Kataria, and J. Hemanth. Ssdmnv2: A real time dnn-based face mask detection system using single shot multibox detector and mobilenetv2. *Sustainable cities and society*, 66:102692, 2021.
- [13] A. Rosebrock. Liveness detection. <https://pyimagesearch.com/2019/03/11/liveness-detection-with-opencv/>, 2019. [Online; accessed 15-May-2023].

- [14] S. Rui and S. Sara. *ESP32-CAM Projects*. eBook, 1st edition.
- [15] ThemeWagon. Securex – security service website template. <https://themewagon.com/themes/security-service-website-template-securex/>, 2022. [Online; accessed 15-Feb-2023].

Függelék

F.1. Részletes tervezés

ESP32-CAM modul lábkiosztása kép: <https://randomnerdtutorials.com/esp32-cam-ai-thinker-pinout/> ESP32-CAM modul: <https://www.esp32.com/viewtopic.php?t=10184>

Képküldés webserveren: <https://www.esp32.com/viewtopic.php?t=10184>

IR szenzor: <https://medium.com/deeplift/introduction-to-input-output-devices-on-arduino>

Arcfelismerés ábra : https://www.researchgate.net/figure/Illustration-of-the-different-roles-of-global-and-local-features-in-face-recognition-fig1_224529777

UNIVERSITATEA SAPIENTIA DIN CLUJ-NAPOCA
FACULTATEA DE ȘTIINȚE TEHNICE ȘI UMANISTE,
TÎRGU-MUREȘ
SPECIALIZAREA CALCULATOARE

Vizat decan:
Conf. dr. ing. Domokos József

Vizat director departament:
Ș.l. dr. ing Szabó László Zsolt