Sustavi kontrole pristupa

Zoričić, Ivan

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka, Faculty of Engineering / Sveučilište u Rijeci, Tehnički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:190:770492

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Diplomski sveučilišni studij elektrotehnike

Diplomski rad

Sustavi kontrole pristupa

Rijeka, studeni 2023

Ivan Zoričić

0069072494

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Diplomski sveučilišni studij elektrotehnike

Diplomski rad

Sustavi kontrole pristupa

Mentor: prof.dr.sc. Nino Stojković

Rijeka, studeni 2023

Ivan Zoričić

0069072494

TEKST ZADATKA

IZJAVA

Sukladno s pravilnikom o diplomskom radu, diplomskom ispitu i završetku diplomskih sveučilišnih studija, izjavljujem da sam diplomski rad na temu „Sustavi kontrole pristupa“ izradio samostalno uz pomoć mentora iz firme Alarm Automatika d.o.o. uz svu potrebnu literaturu.

Rijeka, studeni 2023

Ivan Zoričić

0069072494

ZAHVALA

Na kraju svog akademskog obrazovanja moram zahvaliti svim osobama koje su me pratile na ovom dugom putu. Hvala svim profesorima, asistentima i ostalim djelatnicima Tehničkog fakulteta na prenesenom znanju. Posebne zahvale idu mojoj obitelji koja me sve ove godine podržavala i bila uz mene na putu do ovog velikog životnog uspjeha. Također, posebne zahvale idu mojim mentorima prof.dr.sc. Ninu Stojkoviću i Filipu Manceu koji su dijeljenjem svoga znanja sa mnom uvelike pridonijeli izradi ovog diplomskog rada, te prijateljima Dominiku Dončeviću i Ivanu Dražiću.

SADRŽAJ

1. UVOD ... 1

2. TEHNOLOGIJA KONTROLE PRISTUPA ... 3

2.1. Čitači i tipkovnice ... 4

2.1.1. Čitači ... 5

2.2. Kontroleri ... 12

2.2.1. Kontroleri za n vrata ... 13

2.2.2. Samostalni sustavi ... 14

2.3. Komunikacija komponenti sustava kontrole pristupa ... 15

2.3.1. RS-232 ... 15

2.3.2. RS-422 ... 16

2.3.3. RS485 ... 18

2.3.4. Wiegand ... 20

2.3.5. OSDP ... 21

2.3.6. TCP/IP ... 22

2.4. Ostale komponente sustava kontrole pristupa ... 23

3. BIOMETRIJA ... 26

3.1. Prepoznavanje lica ... 27

3.2. Otisak prsta ... 30

3.2.1. Optički senzor otiska prsta ... 33

3.2.2. Kapacitivni senzor otiska prsta ... 34

3.2.3. Termalni senzor otiska prsta ... 35

3.2.4. Ultrazvučni senzor otiska prsta ... 36

3.4. Prepoznavanje šarenice ... 39

3.5. Skeniranje mrežnice ... 41

3.6. Prepoznavanje glasa ... 45

4. PROJEKT ... 50

4.1. LPR kamera ... 50

4.2. Opis elemenata korištenih u električnom ormaru ... 54

4.3. Idejno rješenje projekta ... 62

4.4. Izrada projekta ... 63

4.5. Podešavanje LPR kamere ... 68

5. ZAKLJUČAK ... 75

6. LITERATURA ... 76

POPIS SLIKA ... 82

SAŽETAK I KLJUČNE RIJEČ ... 84

ABSTRACT AND KEYWORDS 85

1. UVOD

Kontrola pristupa je sigurnosni koncept i tehnologija koja se koristi za upravljanje pristupom sustavima, resursima i podacima kako bi se osiguralo da samo ovlaštene osobe ili ovlašteno osoblje imaju pristup danim resursima, informacijama i sustavima. Osnovna svrha kontrole pristupa je zaštita sustava, resursa i podataka od oštećenja, zlouporabe i neovlaštenog pristupa. Da bi se to postiglo, potrebno je postaviti određena pravila i ograničenja koja određuju tko pod kojim uvjetima i kada može pristupiti određenim podacima, resursima i sustavima.

Povijest kontrole pristupa predstavlja značajnu evoluciju u kontekstu zaštite informacija i resursa unutar različitih sustava i organizacija. Kontrola pristupa razvijala se tijekom mnogo desetljeća kako bi se suočila s izazovima povećane digitalizacije i kompleksnosti informacijskih sustava.

Prvi oblici kontrole pristupa, od kojih neke i danas koristimo, predstavljali su fizičke kontrole pristupa, kao što su ključevi i brave ograničavaju pristup određenim resursima i prostorima.

Skupa sa razvojem računalnih tehnologija i elektronike, počinje ubrzani razvoj kontrole pristupa u drugoj polovici dvadesetog stoljeća. Fizičku kontrolu pristupa, korištenu od davnina, zamjenjuju sve popularniji pristupni kodovi, elektroničke brave i kartični sustavi.

Pojavom i razvojem računalnih sustava u 20. stoljeću, javlja se potreba za kontrolom pristupa digitalnim resursima, te su iz tog razloga razvijeni autentifikacijski mehanizmi, kao što su korisnička imena i lozinke, kako bi pristup podatcima i sustavima bio dozvoljen samo ovlaštenim osobama i entitetima.

Idući korak u razvoju tehnologije kontrole pristupa omogućio je korištenje biometrijski karakteristika kod procesa autentifikacije. Neki od biometrijskih metoda su prepoznavanje otiska prsta, prepoznavanje lica, te skeniranje šarenice oka. Osim šta pružaju zavidnu razinu sigurnosti, ove metode mogu biti izrazito praktične.

U današnjem vremenu složenih sustava izuzetno je važno dodjeljivanje i upravljanje pravima pojedinaca, sustava i aplikacija, kako bi svaki pojedinac koja ima pristup određenim resursima i podacima, mogao tim istim podacima i resursima pristupiti pravovremeno i ciljano. Pod ciljano podrazumijeva se da je potrebno osigurati da pojedinac na određenoj poziciji ima onoliko pristupa koliko mu je potrebno za obavljanje poslovnih zadaća, dok pravovremeno označava pristup podacima za vrijeme radnog vremena, iako se u nekim slučajevima pristup daje na neograničeno vrijeme, neovisno o radnom vremenu pojedinica.

Danas je kontrola pristupa dio informacijske sigurnosti. S vremenom je postalo potrebno razvijanje sigurnosnih standarda kako bi se osigurala odgovarajuća zaštita resursa, podataka i sustava.

2. TEHNOLOGIJA KONTROLE PRISTUPA

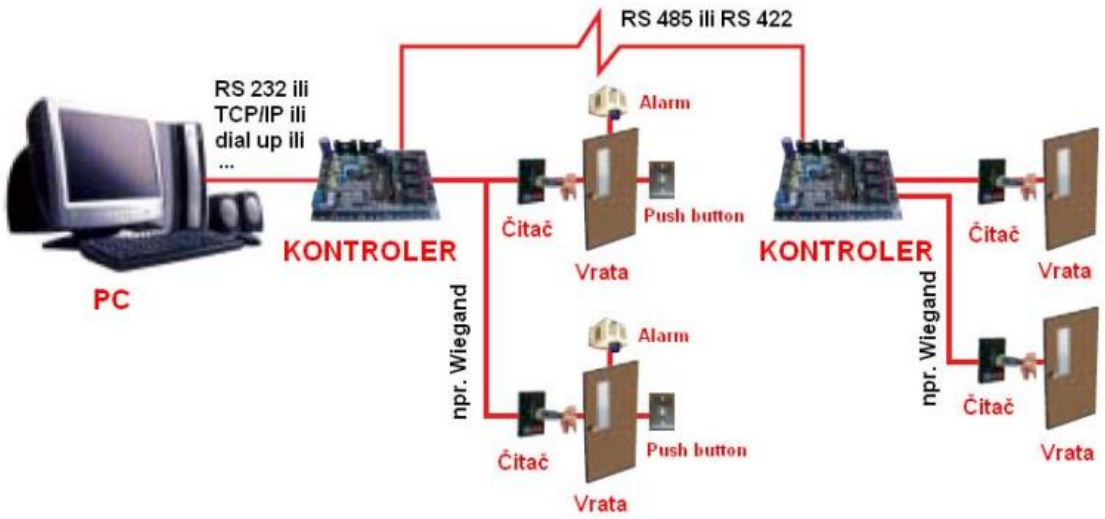
Pojam kontrole pristupa opisuje širok spektar pojmova. Može se koristit za fizičku sigurnost (npr. kontrola pristupa prostorijama ili zgradama), informacijsku sigurnost (npr. pristup podacima i računalnim sustavima) i mrežnu sigurnost (npr. pristup mrežnim resursima).

U slučajevima kada ključevi i brave nisu dovoljno zaštita resursa, podataka i sustava potrebno je koristiti elektroničke sustave kontrole pristupa. Iako su takvi sustavi skuplji u odnosu na jednostavne kontrole pristupa (ključeve i brave), puno su sigurniji i isplativiji, pogotovo za velike sustave, kada jedna osoba mora imati više ključeva, te kada izgubljeni i ukradeni ključevi predstavljaju sigurnosni rizik, odnosno velike troškove. [1]

Kontrola pristupa sadrži sljedeće elemente:

- Identifikacija: Proces prepoznavanja subjekta koji traži pristup podacima, resursima ili sustavu. To se najčešće radi putem korisničkog imena, lozinke, biometrijskih podataka ili nekom drugom identifikacijskom metodom.
- Autentifikacija: Predstavlja proces provjere gdje se utvrđuje dali korisnik ili entitet stvarno onaj korisnik ili entitet koji tvrdi da je. To se najčešće radi unosom lozinke, korištenjem dvofaktorske autentifikacije ili nekom drugom metodom. Kako je korištenje dvofaktorske, odnosno višefaktorske autentifikacije u današnje vrijeme postao standard, ponekad osim korisničkog imena i lozinke, za dodatnu autentifikaciju može se tražiti neki od biometrijskih podataka ili potvrđivanje identiteta putem broja mobilnog uređaja.
- Autorizacija (Ovlaštenje): Nakon autentifikacije subjekta, potrebno je odrediti koja prava subjekt može koristiti. To se radi definiranjem pravila i pristupnih dozvola koja određuju što subjekt može i može raditi, odnosno kojim podacima i resursima može ili ne može pristupiti.
- Nadzor i revizija: Praćenje i zapisivanje svih aktivnosti povezanih s pristupom resursima ili sustavima. To omogućava praćenje i analizu aktivnosti te identifikaciju nepravilnosti ili sigurnosnih prijetnji.
- Enkripcija je ključna komponenta kontrole pristupa. Razvoj jakih enkripcijskih algoritama i metoda zaštite podataka od neovlaštenog pristupa ključni su koraci u povijesti sigurnosti informacija. [2]

Glavne komponente sustava kontrole pristupa su: čitači i tipkovnice, kontroleri, komunikacija, programi, te ostale komponente (REX (eng. request to exit) tipkala i kontroleri, panik bar-ovi, izvršni elementi, mehaničke barijere).



Slika 2.1. Primjer sustava kontrole pristupa za četiri vrata [3]

2.1. Čitači i tipkovnice

Kartični čitači su uređaji koji čitaju informacije s kartica. Te kartice mogu biti magnetne kartice, pametne kartice ili RFID (eng. Radio-Frequency Identification) kartice. Fizička kontrola pristupa često koristi kartične čitače. Najčešća mjesta gdje srećemo kartične čitače su: ulazi u zgrade, prostorije i parkinzi.

Biometrijski čitači na osnovu biometrijskih osobina identificiraju, autentificiraju i autoriziraju korisnika. Biometrijske osobine su otisci prstiju, oblik lica, oblik i boja šarenice, glas. Ovi uređaji pružaju visoku sigurnost i teško su podložni zloupotrebama.

Blizinski (eng. proximity) čitači temelje se na bežičnoj tehnologiji, te imaju mogućnost očitanja kartica koje su na većoj udaljenosti. Ova je tehnologija izrazito praktična jer korisnici ove tehnologije ne moraju dodirivati čitač kao bi ih isti očitao.

Numeričke tipkovnice koriste se za unos osobnih identifikacijskih brojeva - PIN (eng. Personal Identification Number) ili drugih kodova kako bi se autenticirao korisnik. Ovo je često korištena metoda u kombinaciji s kartičnim čitačima.

Kod korištenja PIN-a postoji mogućnost snimanja istog, te kako bi se takva mogućnost smanjila koriste se tipkovnice sa virtualnim brojevima. Na ekranu se prikazuju virtualne tipke s brojevima, koje mogu biti drugačijeg redoslijeda od klasičnog kako bi se otežala moguća zlonamjerna snimanja. Uporaba je ista kao i kod fizičkih tipkovnica, gdje korisnik unosi svoj PIN na virtualnoj tipkovnici.

Kombinacijom tipkovnica za unos lozinki i biometrijskim čitačem osigurava se dvofaktorska autentifikacija. Višefaktorska autentifikacija postiže se dodavanjem dodatnih uređaja za identifikaciju i autentifikaciju korisnika.

Kvaliteta i sigurnost sustava kontrole pristupa ovisi o integraciji čitača i tipkovnica sa ostalim sigurnosnim protokolima, kao što su upravljanje pravima i enkripcija podataka, te je od velike važnosti da pristup ovakvim uređajima bude dobro zaštićen, kako bi se spriječili neovlašteni pristupi i zloupotrebe. [3]

2.1.1. Čitači

Čitači su uređaji koji se koriste za identifikaciju i autentikaciju korisnika ili uređaja kako bi im se omogućio pristup određenim resursima, prostorima ili informacijama. Čitači imaju ključnu ulogu u sustavima kontrole pristupa i sigurnosti jer osiguravaju da samo ovlaštene osobe ili uređaji mogu pristupiti određenim podacima ili resursima. U nastavku ćemo objasniti i opisati neke glavne vrste čitača.

Prva vrsta koju ćemo opisati su kartični čitači. Kartični čitači koriste se za čitanje informacija s različitih vrsta kartica. To mogu biti magnetne kartice, pametne kartice (često s mikročipom), ili RFID (eng. Radio-Frequency Identification) kartice.

Magnetne kartice razvijene su od strane IBM-a, te je 1969. godine prihvaćena kao standard u Sjedinjenim Američkim Državama, dok je u ostatku svijeta kao standard prihvaćena dvije godine kasnije. Razvijena je za potrebe CIA-e (eng. Central Intelligence Agency) u svrhu kontrole pristupa. [4]

Magnetne kartice su česta forma identifikacije i autentikacije u sustavima kontrole pristupa i drugim aplikacijama gdje je potrebna identifikacija korisnika. Dizajn magnetske kartice sastoji se od plastične kartice na koju je montirana magnetna traka sa kodiranim podacima osobe ili entiteta u čijem je vlasništvu kartica. Oblikom i veličinom slične su kreditne karticama.

Magnetska traka izrađena je od tankog feromagnetskog materijala na koju su podaci kodirani magnetizacijom. Podaci se spremaju na karticu kao binarni zapisi.

Magnetne kartice su relativno jeftine za proizvodnju, lako ih je zamijeniti ako se izgube ili oštete, i jednostavne za korištenje. Također se lako čitaju pomoću čitača.

Magnetne kartice su manje sigurne u usporedbi s drugim oblicima autentikacije, poput pametnih kartica ili biometrijskih sustava, jer podaci s trake mogu relativno lako biti kopirani ili presnimljeni. Također su osjetljive na oštećenja magnetskog traga ili magnetskih čestica. [5]

Čitač magnetskih kartica sadrži uređaj koji se zove solenoid, a služi za kontrolu feromagnetskih čestica u magnetskoj traci. Solenoid je zapravo gusto namotana zavojnica, koji proizvodi jako magnetsko polje kada kartica prođe kroz njega. Kada kartica sa magnetskom trakom prođe kroz čitač, napon se inducira u navojima solenoida. Voltaža se tada pojačava, i elektronički snima te ju procesor unutar čitača čita kako bi čitač mogao pristupiti informacijama zapisanim na kartici.

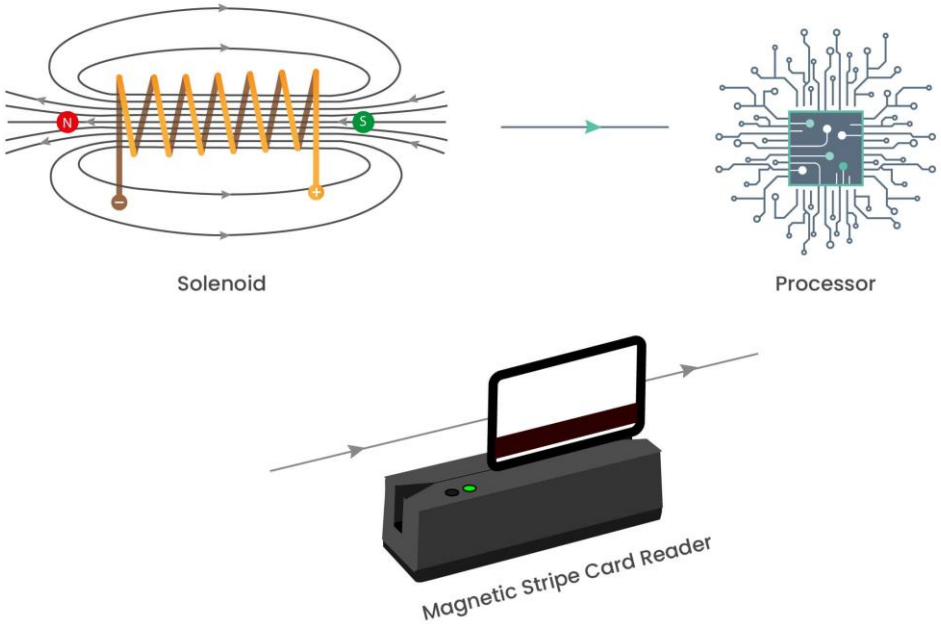
Kako bi se poboljšala sigurnost magnetnih kartica, često se koristi PIN autentikacija. Korisnik mora unijeti odgovarajući PIN kako bi se autenticirao uz karticu, iako je ovakva primjena češća kod kupoprodaje i u bankovnim sustavima, moguća je primjena i kod kontrole pristupa.

Važno je napomenuti da su magnetne kartice sve više zamjenjivane naprednijim tehnologijama, poput pametnih kartica s mikročipom i RFID tehnologijom, koje pružaju višu razinu sigurnosti i funkcionalnosti. Međutim, magnetne kartice i dalje se široko koriste u mnogim aplikacijama diljem svijeta zbog svoje jednostavnosti i niske cijene.

Osim u kontroli pristupa magnetna kartica može se koristiti u bankarstvu, za identifikaciju i u transportu. [6]

Slika 2.2. Magnetna kartica [7]

Slika 2.3. Kartica sa čitačem [8]



Slika 2.4. Princip rada solenoida[8]

Druga vrsta čitača su biometrijski čitači. Biometrijski čitači koriste biometrijske osobina pojedinca za identifikaciju. To uključuje otiske prstiju, skeniranje šarenice, prepoznavanje lica, prepoznavanje glasa, čak i analizu potpisa.

Biometrijski čitači pružaju visoku razinu sigurnosti jer su biometrijske karakteristike jedinstvene za svakog pojedinca.

Problem kod biometrijskih čitača je što zahtijevaju posebnu opremu i softver koji moraju biti u skladu s propisima o zaštiti privatnosti.

Biometrijski čitači bit će detaljnije obrađeni poslije u radu.

Treća vrsta čitača su blizinski čitači. Blizinske čitače ili RFID služe se bežičnom tehnologijom radio valova kako bi čitali podatke sa kartice ili uređaja koji se nalaze na većoj udaljenosti. Koriste radiofrekvenciju (RFID) kako bi čitali tražene informacije.

Velika prednost ovih čitača je što se identifikacija što ne zahtijevaju da se kartica ili neki drugi identifikacijski uređaj prinesu u neposrednu blizinu čitača kako bi se pročitale informacije sa kartice, već se to automatski obavlja prolaskom kartice kroz područje pokriveno radio valovima čitača.

RFID sustav radi na principu da čitač, odnosno antena emitira radiofrekvencijski signal u prostor oko sebe. Signal predstavlja elektromagnetsko polje koje se širi u prostor oko čitača. Kada uređaj ili kartica koji sadrži RFID čip, koji je zapravo zavojnica, koja se inducira prolaskom kroz elektromagnetsko polje, te u trenutku primanja energije kartica emitira signal nazad u čitač, odnosno u antenu. Čip unutar kartice sadrži jedinstveni identifikacijski kod, koji se šalje nazad na čitač (antenu). Kada čitač primi kod od RFID čipa, obrađuje primljeni kod, na način da ga dekodira i provjeri jeli jedinstveni identifikacijski broj valjan. Ako je onda je pristup korisniku RFID kartice odobren.

Gore opisan proces predstavlja proces kod pasivnih RFID sustava, gdje RFID kartice i tagovi nemaju vlastito napajanje.

Slika 2.5. RFID antena [9]

Slika 2.6. RFID tag [10]

Osim pasivnih, postoje i aktivni RFID sustavi. Za razliku od pasivnih, aktivni tagovi i kartice sadrže vlastite baterije ili napajanje, te aktivan komunikacijski sklop. Također sadrže vlastiti odašiljač koji može emitirati signal neovisno o prisutnosti čitača. Aktivno tag može na zahtjev korisnika emitirati radiofrekvencijske signale, koji pobuđuju antenu. Podaci koji su pohranjeni u tagu uključuju jedinstveni identifikacijski kod. Kada antena primi signal koje šalje tag, antena šalje signal tagu, te tek tada tag šalje signal sa informacijama. Signal se dekodira, te provjerava jeli identifikacijski kod taga valjan. Ako je, korisnik je tada autoriziran za prolazak. [11]

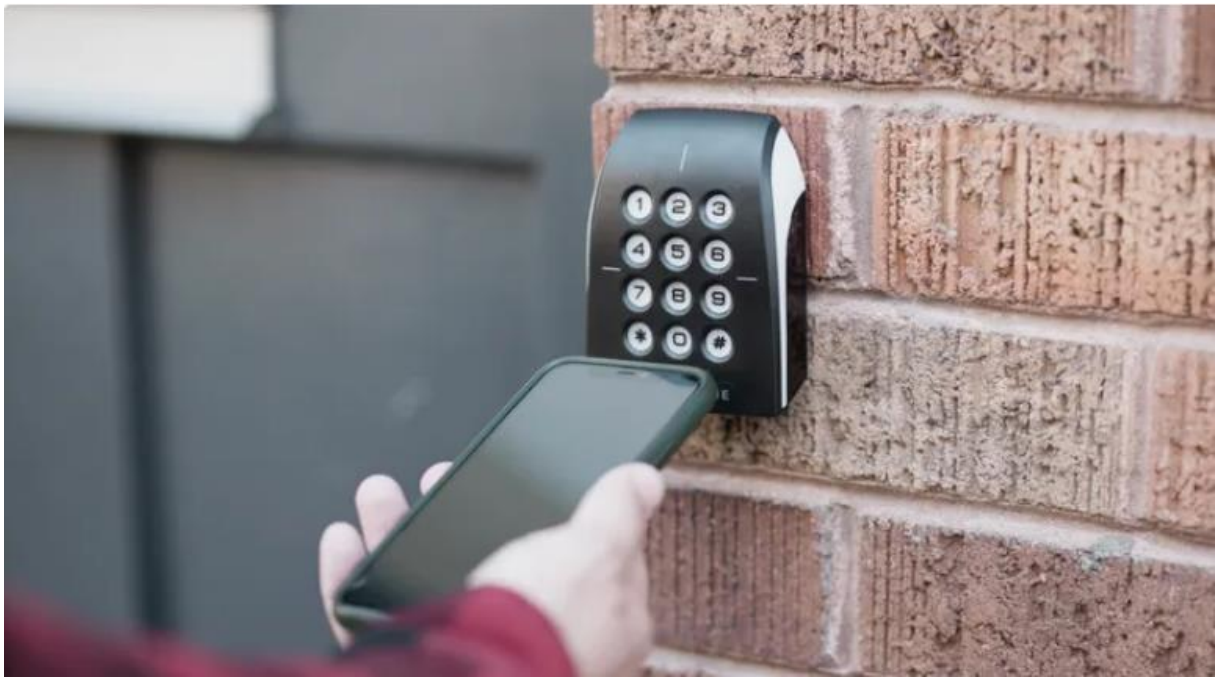
Slika 2.7. Aktivni RFID tag [12]

Razlika između aktivnih i pasivnih RFID sustava je, osim u napajanju, i u samim performansama sustava. Aktivni sustavi omogućuju veću udaljenost na kojoj antena i tag komuniciraju, dok je kod pasivnih sustava ta udaljenost znatno manja. Također, aktivni tagovi imaju autonomnost, koju pasivni nemaju, i to zbog vlastitog napajanja. Aktivni sustavi također su kompleksniji i skuplji u usporedbi sa pasivnom tehnologijom, te omogućuju aktivno praćenje taga u vremenu jer signale emitiraju sami.

Primjena ovakvih sustava osim u kontroli pristupa može biti u slučajevima kada je potrebno pratiti objekte na većoj udaljenosti i u stvarnom vremenu. Također je moguće upravljanje zalihama u opskrbnom lancu, ili praćenje proizvoda u velikim halama. [13]

Četvrta vrsta su smartphone čitači. Smartphone čitači omogućuju da korisnikom pametne mobitele služi kao sredstvo identifikacije i autentifikacije. Na uređaj se preuzima aplikacija proizvođača čiji sustav kontrole pristupa koristimo. Postoje razni načini prepoznavanja dozvoljenog uređaja, te odobravanja pristupa, pa tako pametni mobiteli mogu koristiti NFC (eng. Near Field

Communication), Bluetooth, QR (eng. quick response) kod ili pritiskom na virtualnu tipku unutar same aplikacije kako bi dobili pristup određenom prostoru, resursu ili informaciji. Nakon čitanja informacija sa pametnog telefona, aplikacija informacije obrađuje lokalno ili ih šalje na server, kako bi se napravila provjera autentičnosti korisnika i provjerila prava pristupa. Na temelju rezultata, aplikacija odobrava ili ne odobrava pristup resursima. Osim pametnih mobitela, instalaciju softvera često je moguće napraviti i na osobna računala.



Slika 2.8. NFC čitač [14]

Čitači se koriste u različitim sektorima, uključujući fizičku sigurnost, kontrolu pristupa u zgradama, bankama, zračnim lukama, bolnicama, IT sustavima i mnogim drugim aplikacijama gdje je potrebna sigurna autentikacija. Izbor čitača ovisi o specifičnim potrebama i sigurnosnim zahtjevima organizacije ili sustava. [15]

Tablica 2.1. Tehnologije kartica sa karakteristikama

Tehnologija	**Cijena čitača**	**Cijena kartice**	**Sigurnost**	**Ostale karakteristike**
Magnetska kartica	Niska	Niska	Niska	Česta pogrešna očitanja, mogućnost oštećenja i kopiranja
RF beskontaktne (pasivne i aktivne)	Srednja do Visoka	Srednja do Visoka	Visoka	Lake za korištenje, snižavanjem cijene raste im popularnost, većinom pasivne (neograničen vijek trajanja)
Bežična	Visoka	Visoka	Visoka	Neželjena očitanja, aktivne (ograničen vijek trajanja)
Pametna kartica (npr. Mifare)	Visoka	Visoka	Visoka	Koristi se u slučajevima kad se jedna kartica želi koristiti za više namjena

2.2. Kontroleri

Kontroleri predstavljaju mozak sustava kontrole pristupa, povezujući sofisticiranu programsku logiku, čitače i bravu u koherentnu cjelinu. Iako obično ostaju skriveni, njihova uloga je ključna za uspješno ostvarivanje kontrole pristupa, identifikacije i autentifikacije. Funkcioniraju kao inteligentni posrednici, prikupljajući i analizirajući podatke prikupljene od čitača kako bi donijeli precizne odluke o odobravanju ili odbijanju pristupa korisnicima.

Važno je istaknuti da kontroleri nadziru i usklađuju aktivnosti čitača te uspostavljaju komunikaciju s centralnom bazom podataka gdje se čuvaju informacije o korisnicima i njihovim ovlastima za pristup, iako je moguće da su podaci korisnika spremljeni lokalno na samom kontroleru. To omogućava brzu i pouzdanu identifikaciju i provjeru svakog korisnika pri svakom pristupu, osiguravajući pritom sigurnost i integritet sustava kontrole pristupa.

U suštini, kontroleri omogućavaju složenim sustavima kontrole pristupa da funkcioniraju besprijekorno, štiteći resurse i objekte na učinkovit i pouzdan način. [16]

U nastavku ćemo se baviti vrstama kontrolera.

Slika 2.9. Kontroler u elektroormaru [16]

2.2.1. Kontroleri za n vrata

Ovo je najčešći tip kontrolera, gdje se električna tiskana pločica smješta unutar električnog kućišta. Kućište se obično montira na zid unutar ormara ili na strop iznad vrata. Ovaj pristup nudi niz prednosti koje ga čine izuzetno praktičnim. Kontroleri ove vrste omogućuju upravljanje više od jednih vrata, postoje izvedbe koje podržavaju upravljanje s 32 vrata ili čak više, iako se u praksi često koriste verzije s do četiri vrata.

Jedna od ključnih prednosti ovih kontrolera je njihova sposobnost učinkovitog upravljanja većim brojem vrata. To se postiže putem žičane komunikacije koja ulazi izravno u kućište kontrolera. Ovakve izvedbe s više vrata često zahtijevaju manje kabela, što ih čini ekonomičnijima i lakšima za održavanje i upravljanje.

Važno je napomenuti da je kontroler smješten na sigurnoj strani sustava. Bez obzira na događaje na nesigurnoj strani, kao što su kvarovi ili vandalizam na čitačima, vrata ostaju zaključana i sigurna.

Osim toga, budući da ovaj kontroler upravlja s više vrata, korisnik se može registrirati samo jednom kako bi imao pristup svim vratima kojima kontroler upravlja. Također je moguće prilagoditi pristupna prava korisnika, omogućujući im pristup svim vratima ili samo odabranim. Ova fleksibilnost olakšava prilagodbu sustava sigurnosti specifičnim potrebama.

Osim toga, ovakvi kontroleri mogu biti povezani s centralnim računalom putem mreže, što omogućuje centralizirano upravljanje i registraciju korisnika za sve povezane kontrolere. Ovaj pristup olakšava administraciju i osigurava konzistentnost sigurnosnih postavki na različitim lokacijama. [17]

Slika 2.10. Kontroler za 4 vrata [18]

2.2.2. Samostalni sustavi

Još jedna često primijenjena varijanta kontrole pristupa je kontroler s integriranim čitačem. U ovom aranžmanu, kontroler i čitač nalaze se unutar istog kućišta. Ova konfiguracija često se primjenjuje u manjim sustavima, poput kućnih pristupa. Iako kompaktna i praktična, ovakva izvedba često je ograničena na upravljanje jednim vratima.

Važno je napomenuti da ova izvedba može predstavljati neke sigurnosne izazove jer i kontroler i čitač nalaze se na nesigurnoj strani sustava. Kako bi se osigurala adekvatna sigurnost, često se primjenjuju dodatne sigurnosne mjere, uključujući sigurnosno ožičenje i specifične sigurnosne konektore. Ovakvi sustavi često se koriste u situacijama gdje nije nužno zahtijevati visoki stupanj sigurnosti.

Unatoč tim izazovima, jedna od prednosti ovakvih kontrolera je brzina montaže. Njihova jednostavna konstrukcija omogućuje brzo postavljanje sustava pristupa bez potrebe za kompliciranim instalacijama. [3]

Slika 2.11. Samostalni sustav [19]

2.3. Komunikacija komponenti sustava kontrole pristupa

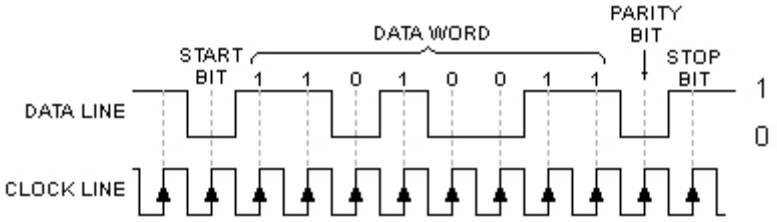
Komponentne kontrole pristupa kao što su kontroleri, čitači, baze podataka i elektroprihvatnici koriste razne protokole za komunikaciju. Koji će protokol biti korišten ovisi o specifičnostima sustava i opreme. U nastavku ćemo obraditi komunikacijske protokole.

2.3.1. RS-232

RS-232 standard predstavljen je 1960. godine, te služi za serijsku komunikaciju. Sastoji se od dvije žice, od kojih jedna služi za slanje, a druga za primanje podataka. RX predstavlja prijemnik, dok TX predstavlja odašiljač, odnosno moguće je istovremeno slanje i primanje podataka. Informacija se prenosi digitalno, putem logičkih nula i jedinica. Logička jedinica odgovara naponskoj razini od -3 do -15 V, dok logička nula odgovara naponskoj razini od 3 do 15 V. Također, postoje dva konektora koja su kompatibilna sa ovim standardom, a to su DB9, koji se češće koristi i DB25, prikazani sa slici 2.19.

Slika 2.12. DB9(lijevo) i DB25(desno) [20]

Signal poslan preko RS-232/422/485 sastoji se od startnog bita,podatkovnih bitova, paritetnog bita i stop bita, kao što je vidljivo na slici 2.14.



Slika 2.13. Raspored bitova [20]

Startni bit predstavlja početak prijenosa, i najčešće je nula. Podatkovni bitovi predstavljaju podatak koji se prenosi, paritetni bit služi za detekciju greški, dok stop bit predstavlja završetak prijenosa.

RS232 podaci se šalju serijski, svaki bit se šalje jedan za drugim jer postoji samo jedna linija podataka u svakom smjeru. Ovaj način prijenosa podataka također zahtijeva da prijamnik zna kada stvarni podaci dolaze kako bi se mogao uskladiti s dolaznim podacima. Da bi se postiglo ovo, logička 0 se šalje kao početni sinkronizacijski bit (startni bit).

Brzina prijenosa podataka ovisi o samoj udaljenosti između uređaja, odnosno o duljini žice. Na duljini žice od 15 metara, brzina prijenosa iznosi 9600 bps, dok na minimalnoj udaljenosti iznosi 115 kbps. [20]

2.3.2. RS-422

RS-422 sučelje slično je RS-232 sučelju. Također dozvoljava istovremeno slanje i primanje podataka koristeći dvije žice, ali za razliku od RS-232 standarda koristi diferencijalne signale. Ovi

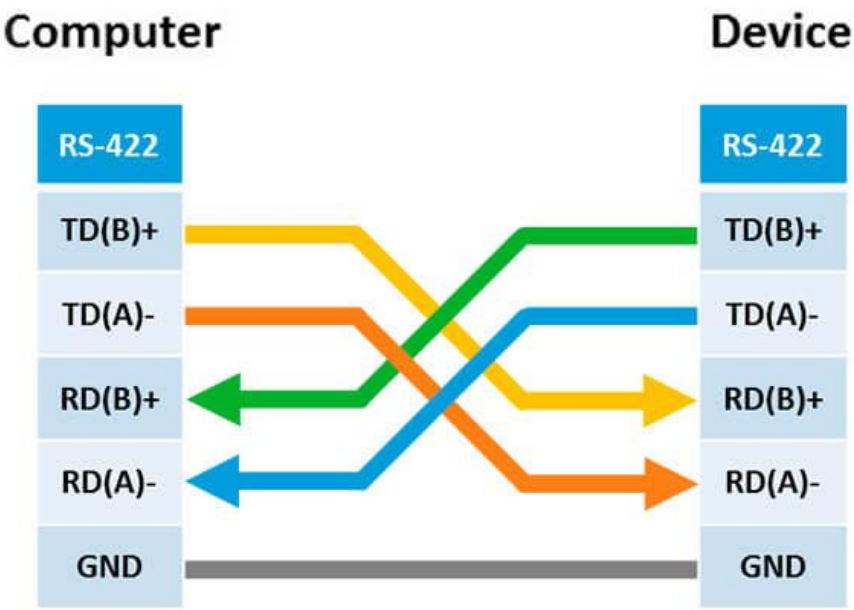
diferencijalni signali, označeni kao 'A' i 'B', čine što se naziva diferencijalnim parom. U ovom paru, jedan signal predstavlja izvorni signal, dok je drugi signal invertiran.

Brzina prijenosa podataka u RS-422 sustavu varira ovisno o udaljenosti i može se kretati u rasponu od 10 kbps na udaljenostima do 1200 metara, sve do 10 Mbps na udaljenostima do 10 metara. U RS-422 mreži dopušten je samo jedan uređaj za slanje podataka, dok se može povezati do 10 uređaja za primanje.

RS-422 linija sastoji se od četiri žice za prijenos podataka, pri čemu svaka parna žica služi za prijenos i primanje podataka, uz dodatnu zajedničku zemljanu žicu za referencu. Ovaj aranžman žica omogućuje efikasno uklanjanje elektromagnetskih smetnji i interferencija, jer obje žice parova reagiraju istovremeno na bilo kakvu vanjsku smetnju, dok se podaci izvlače iz potencijalne razlike između vodiča A i B na istoj liniji.

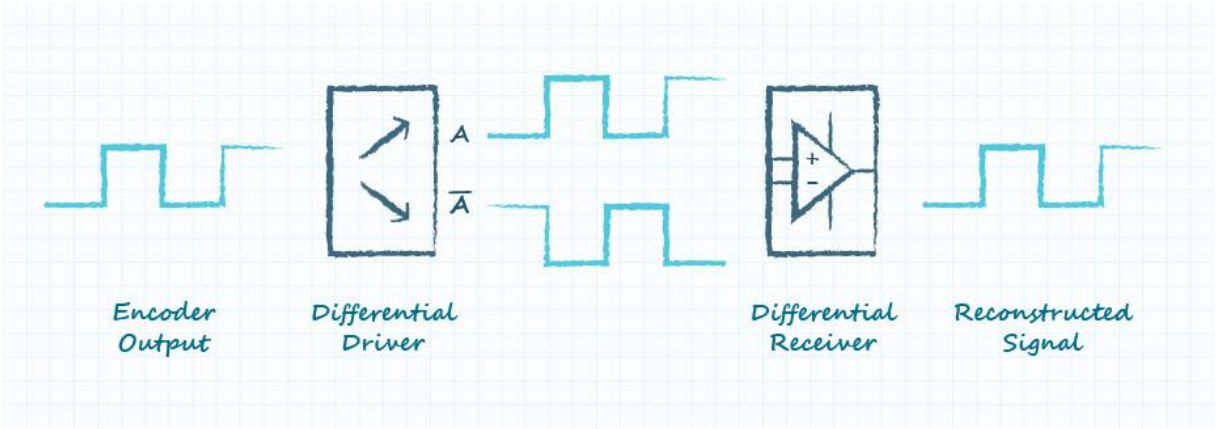
Napon na linijama podataka RS-422 može varirati u rasponu od -6 V do +6 V. Za logičku razliku između A i B potrebno je da bude veća od +0.2 V, dok logička 1 odgovara razlici između A i B manjoj od -0.2 V. RS-422 standard ne specificira određeni tip konektora, ali obično se koristi spojnica s terminalskim blokom ili DB9 konektor. Raspored pinova na RS-422 konektorima može varirati ovisno o proizvođaču uređaja i obično se detaljno opisuje u dokumentaciji za taj uređaj.

Prilikom povezivanja RS-422 uređaja potrebno je izraditi križni spoj između pinova za RX i TX, kao što je prikazano na slici 2.15.



Slika 2.14. Povezivanje RS-422 uređaja [20]

U diferencijalnom pristupu, glavni uređaj generira izvorni signal s jednim krajem, a zatim se signal šalje prema diferencijalnom odašiljaču. Odašiljač stvara diferencijalni par signala koji se prenosi kroz kabel. Kada se koriste dva generirana signala, prijemnik više ne referira naponske razine na zemlju, već uspoređuje ova dva signala međusobno. Prijemnik tako prati razliku između ta dva signala umjesto da uspoređuje s referentnom razinom zemlje. Diferencijalni prijemnik zatim rekonstruira ova dva signala natrag u jedan signal s jednim krajem, koji se može tumačiti od strane glavnog uređaja koristeći odgovarajuće logičke razine potrebne za glavni uređaj. [21]

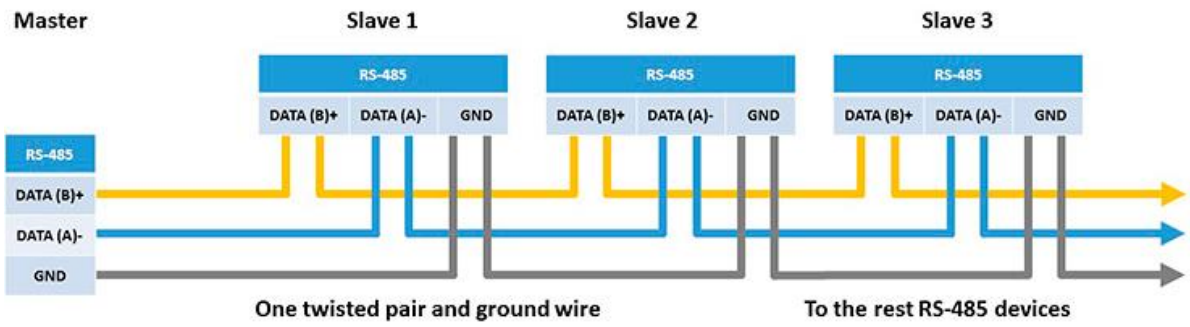


Slika 2.15. Prikaz diferencijalnog pristupa [21]

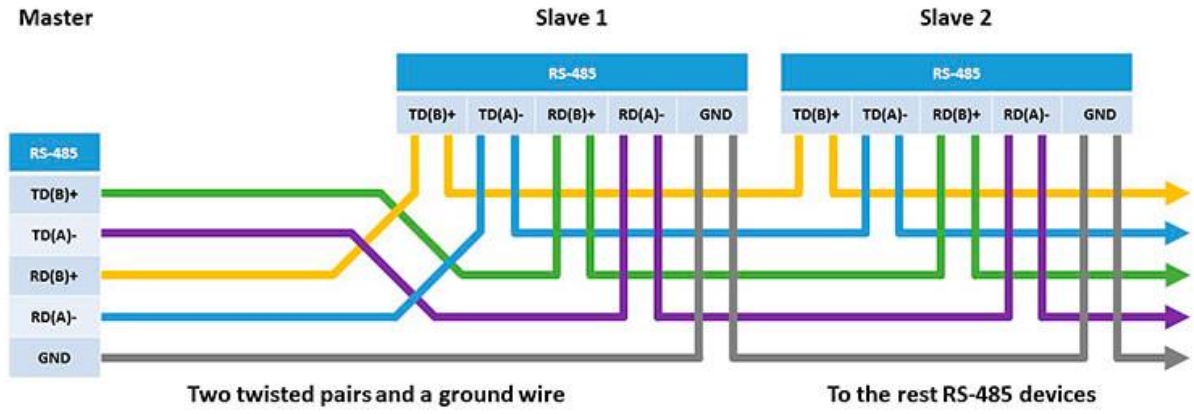
2.3.3. RS485

RS485 je standard napravljen 1998. godine, te se od tada koristi u automatiziranim sustavima. Od tada se često koristi u industrijskim okruženjima, jer omogućuje velike duljine žica i više uređaja na istom vodu. Također ima visok stupanj tolerancije na smetnje, pa je pogodan za primjene u autoindustriji gdje nije sigurno kakve će se sve smetnje naći u krajnjoj primjeni. Upravo ga velike brzine, dugi kabeli i otpornosti na električne smetnje čine dobrim izborom za serijsko spajanje.

RS485 može koristiti dvije linije, koje moraju biti uvrnute, kako bi spomenute dvije linije imale jednaku impedanciju duž svoje duljine. Ovaj se proces naziva balansiranje linija. Osim jednake impedancije duž linija, bitno je da jednake impedancije budu na strani odašiljača, odnosno prijemnika. Za ovu vrstu komunikacije mogu se koristiti različite topologije, ovisno o zahtjevima mreže.



Slika 2.16. Topologija sa dvije žice RS485 linija [20]



Slika 2.17. RS-485 Topologija sa 4 žice [20]

Balansiranje linije prijenosa pruža efikasno rješenje za smanjenje elektromagnetske interferencije kada koristimo diferencijalne signale.

U sučelju s jednim krajem, prijemnik tumači signal s obzirom na referentnu razinu zemlje i odlučuje o stanju signala temeljem unaprijed definiranih naponskih razina, često nazvanih logičkim razinama, koje određuju je li signal u visokom ili niskom logičkom stanju. Međutim, na većim duljinama kabela, gdje napon opada, a brzine promjene signala se usporavaju, često dolazi do pogrešaka u prijenosu signala.

Ovo vrste sučelja također omogućuje različitim uređajima s različitim razinama napona da komuniciraju putem diferencijalnih prijemnika. Sve ovo zajedno pomaže prevladati degradaciju signala koja bi se inače dogodila na dugim duljinama kabela kada se koristi sučelje s jednim krajem.

RS485 ne zahtijeva upotrebu određenog naponskog nivoa, već specificira minimalno potrebni diferencijalni napon (razlika napona signala A i B). RS-485 standard zahtijeva minimalni diferencijalni napon od +/- 200 mV na prijamniku, te će svi RS-485 uređaji imate isti raspon

ulaznih napona, bez obzira na prijenos na različitim naponima. RS-485 podržava napone linije od -7 do 12 V. Također, u jednom segmentu mreže podržava komunikaciju do 32 uređaja.

Mrežni sloj se bavi komunikacijom između uređaja, te u svakom trenutku samo jedan odašiljač smije odašiljati signal. Moguć je sudar signala u slučajevima kada više uređaja pokuša komunicirati istovremeno, što može biti izuzetno štetno za mrežu. Kada dođe do sudara, dolazi do „sukoba“ odašiljača, te svaki na svojoj strani može izazvati kratki spoj. To rezultira povlačenjem velike količine struje iz mreže, što rezultira termalnim gašenjem prijemnika.

Kako bi se izbjegli sudari, glavni uređaj kontrolira protok signala kroz liniju i poziva pojedine uređaje. To se postiže imajući skup naredbi koje prepoznavaju samo određeni uređaji ili imaju specifične adrese za svaki uređaj. Budući da se linija dijeli između više uređaja, svaki će uređaj vidjeti naredbu ili adresu koju šalje glavni uređaj, ali će na naredbu odgovoriti samo uređaj koji je tom naredbom ili adresom aktiviran. [21]

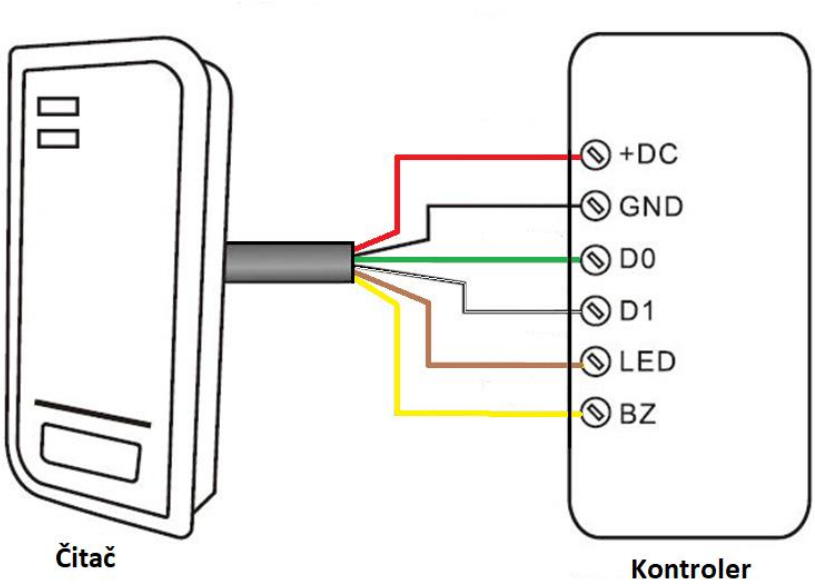
2.3.4. Wiegand

Wiegand je standard za povezivanje čitača kartica sa sustavom za kontrolu pristupa. Postoje popularan 1980-ih i to zbog čitača koji koriste Wiegand efekt. Čitač koji koristi Wiegand standard može biti vezan jedino na kontroler koji također podržava Wiegand standard.

Wiegand efekt ili Wiegand fenomen je fizički fenomen koji je otkrio John R. Wiegand, a promatran je u određenim materijalima i tankim žicama. Opisuje ga nagla promjena magnetskih svojstava tanke žice koja je izložena deformaciji ili mehaničkome stresu. Primjenom mehaničkog stresa ili deformacije žice dolazi do promjene u kristalnoj strukturi žice i moguće je inducirati efekt. Primjenom Wiegand efekta moguće je generirati oštri magnetski impuls, koji je moguće detektirati primjenom odgovarajućih magnetskih senzora. [22]

Sustavi koji koriste Wiegand standard, rade na principu da se u pristupnu karticu ugradi mali dio Wiegand žice, te kada se kartica provuče kroz čitač kartica, primjenjuje se mehanički stres koji na žicu generira karakteristični magnetski impuls, koji detektira senzor u čitaču, te omogućuju ili uskraćuje pristup korisniku kartice.

Wiegand standard za prijenos podataka koristi tri žice, od kojih je jedna zajednička za uzemljenje, jedna se naziva "D0" ili "Data Low", te "D1" ili "Data High". Na slici 2.19. su prikazane "D0", "D1" i "GND" koje koristi Wiegand, te neke dodatne žice koje se koriste za napajanje ("+DC") i dodatne funkcije ("LED" služi za svjetlo obavijesti, dok "BZ" služi za zvuk obavijesti). [23]



Slika 2.18. Način spajanja Wiegand standarda [24]

Kada nema slanja podataka, obje su žice na visokoj razini napona od 5V. Kada se šalje logička nula "D0" se spušta na niski napon dok "D1" ostaje na visokom naponu. Kada se šalje logička jedinica "D1" se spušta na nisku razinu napona, a "D0" ostaje na visokoj razini napona.

U kontroli pristupa za komunikaciju najčešće se koristi 26 bitni Wiegand protokol. Radi na način da je prvi bit bit pariteta, idućih 8 bitova predstavljaju oznaku uređaja, sljedećih 16 bitova služi za ID oznaku, te je završni bit, također bit pariteta. Prvi bit pariteta računa se na temelju prvih dvanaest bitova, a završni bit pariteta računa se na temelju posljednjih 12 bitova. Unatoč ovome, postoje razne implementacije i proširenja ovog osnovnog formata. [25]

2.3.5. OSDP

OSDP (eng. Open Supervised Device Protocol) je standard za komunikaciju između uređaja u kontroli pristupa razvijen od strane SIA-a (eng. Security Industry Association), kako bi ponudio sigurniju komunikaciju između komponenti kontrole pristupa. Standard je odobren 2020. godine od strane Međunarodnog elektrotehničkog povjerenstva, zaduženog za normizaciju električne elektroničke i srodne tehnologije.

Koristi se za povezivanje kontrolera sa perifernim uređajima, kao što su čitači kartica, tipkovnice i biometrijski uređaji. OSDP je otvoreni standardni protokol koji pruža napredne sigurnosne značajke i poboljšanu funkcionalnost u usporedbi sa starijim protokolima kao što je Wiegand.

OSDP omogućuje dvosmjernu komunikaciju, odnosno dozvoljava uređajima primanje i slanje naredbi, što poboljšava fleksibilnost i funkcionalnost samog sustava kontrole pristupa.

Sam standard koristi dvije žice, u kojem je jedna žica zadužena za slanje, a druga za primanje podataka. To je bitno jer za razliku od Wieganda omogućuje potvrde (ACK) i negativne potvrde (NAK) tijekom procesa komunikacije, odnosno osigurava da su poslani podaci uspješno primljeni od strane namjeravanog primatelja.

OSDP pruža visoku razinu sigurnosti koristeći AES-128 enkripciju, koja koristi 128 bitova za enkripciju i dekripciju poslanih poruka, te je time OSDP standard sigurniji od Wieganda. Sam OSDP omogućuje neprestano nadgledanje ožičenje kako bi osigurao da je sustav uvijek online. [26]

2.3.6. TCP/IP

TCP/IP (eng. Transmission Control Protocol/Internet protocol) razvijen je od strane Američkog ministarstva obrane 1960-ih godina. TCP/IP predstavlja niz standardiziranih pravila koja omogućavaju računalu da komuniciraju sa mrežom, kao što je naprimjer internet.

TCP/IP opisuje procese razdvajanja podataka u pakete, njihovo adresiranje, slanje, usmjeravanje i primanje na odredištu. Značajna prednost TCP/IP protokola je što zahtijeva minimalnu središnju kontrolu, a njegova struktura je oblikovana kako bi mrežama pružila iznimnu pouzdanost, uključujući i automatsku obnovu nakon bilo kakvih neuspjeha na mrežnim uređajima.

TCP određuje kako aplikacije mogu uspostaviti komunikacijske kanale preko mreže. Nadalje, on upravlja procesom segmentacije poruka na manje pakete prije nego što ih šalje putem interneta, osiguravajući da se na odredištu ponovno sastave u ispravnom redoslijedu. S druge strane, IP protokol određuje način adresiranja i usmjeravanja svakog paketa kako bi osigurao da svaki stigne do svoje prave odredišne adrese. Na svakom mrežnom prekidaču se prati IP adresa kako bi se odlučilo kamo poslati poruku. Maska podmreže je informacija koja govori računalima i drugim mrežnim uređajima koji dio IP adrese označava mrežu, a koji dio predstavlja domaćine ili druga računala unutar te mreže.

NAT (eng. Network Address Translation) predstavlja virtualizaciju IP adresa i pridonosi većoj sigurnosti i smanjenju potrebne količine IP adresa za organizaciju.

TCP/IP mrežni protokoli uključuje: HTTP (eng. Hypertext Transfer Protocol), odnosno protokol za prijenos hiperteksta upravlja komunikacijom između poslužitelja na webu i preglednika na webu, HTTPS (eng. Hypertext Transfer Protocol Secure) koji osigurava sigurnu komunikaciju između poslužitelja na webu i web preglednika, te FTP (eng. File Transfer Protokol) koji upravlja prijenosom datoteka između računala. [27]

Jedan od osnovnih zadataka TCP/IP-a je razbijanje cijele poruke na manje dijelove, odnosno pakete. Ovi paketi se zatim šalju i sastavljaju na odredištu. Zanimljivo je da svaki paket može krenuti različitim rutama prema svom odredištu, omogućavajući prilagodbe u stvarnom vremenu ako prva ruta nije dostupna ili je pretrpana. TCP/IP također organizira različite aspekte komunikacije u različite slojeve, svaki s vlastitom specifičnom ulogom. Podaci putuju kroz četiri ovakva sloja prije nego što se konačno prime na odredištu. TCP/IP tada prolazi kroz ove slojeve u obrnutom redoslijedu kako bi ponovno sastavio podatke i predstavio ih primatelju. Svrha ovakvog slojevitog pristupa je očuvati standardizaciju, bez obzira na raznolikost hardverskih i softverskih rješenja. Osim toga, ovaj pristup omogućava ažuriranje pojedinih slojeva kako bi se poboljšala izvedba ili sigurnost, bez potrebe za cjelokupnom rekonfiguracijom sustava. [28]

Četiri sloja TCP/IP-a su:

Aplikacijski sloj gdje se pri dizajniranju TCP/IP-a, stvaratelji prepoznali potrebu da protokoli višeg sloja integriraju niz tehničkih aspekata, uključujući pitanja veze, prezentaciju, kodiranje i upravljanje dijalozima. Zbog toga su stvorili jednostavan aplikacijski sloj koji preuzima odgovornost za protokole višeg sloja, kao i za prikaz podataka, njihovo kodiranje i upravljanje komunikacijom. TCP/IP elegantno objedinjuje sve ove aplikacijske izazove u jednom sloju, tj. aplikacijskom sloju, pružajući pravilno pakiranje podataka za daljnje prijenose.

Prijenosni sloj posvećuje se osiguranju visoke kvalitete usluge, problemima pouzdanosti, protoku podataka i ispravljanju eventualnih pogrešaka. Jedan od protokola unutar prijenosnog sloja, TCP, nudi iznimno fleksibilne i pouzdane mehanizme za uspostavljanje stabilnih i gotovo besprijekornih mrežnih komunikacija.

Internet sloj ima zadatak uspješnog slanja paketa iz bilo koje mreže na međumrežje i njihovog sigurnog pristizanja na odredište, Internet sloj obavlja ključnu funkciju.

Sloj mrežnog pristupa - nekada se ovaj sloj opisuje kao "računalo-prema-mreži sloj" (eng. host-to-network layer). Ovaj sloj obuhvaća LAN i WAN protokole, te sve pojedinosti koje su prisutne u fizičkom i podsloju OSI referentnog modela. [29]

2.4. Ostale komponente sustava kontrole pristupa

Električne brave - najčešći su primjer izlaznih uređaja poput električnih brava, elektromagnetskih brava i drugih vrsta elektrificiranog hardvera. Kontroler je uređaj koji tumači ispravno očitanu legitimaciju i primjenjuje logiku za otključavanje vrata. Izlazni signal ili kontakti releja prekidaju napajanje brave, prekidajući "zaključano" stanje hardvera na temelju uspješno očitane legitimacije.

Prekidači položaja vrata - Prekidači položaja vrata, često nazivani i senzorima položaja vrata ili senzorima otvorenosti vrata, su uređaji koji se koriste za otkrivanje ili nadziranje položaja vrata. Oni mogu biti električni ili elektronički uređaji koji se instaliraju na vratima ili oko vrata te omogućuju sustavima za kontrolu pristupa ili sigurnosnim sustavima da znaju je li vrata otvorena, zatvorena ili u nekom drugom položaju. Ovi senzori često igraju ključnu ulogu u sigurnosnim sustavima kako bi osigurali da vrata budu pravilno zatvorena i zaključana kada je to potrebno. [30]

Slika 2.19. Prekidač položaja vrata [30]

REX i sigurnosni senzori - Napajanje elektromagnetske brave, poznate i kao maglock, regulira se putem uređaja za aktivaciju izlaza (REX) koji je montiran ispred vrata, na neosiguranom dijelu. Hodanje ispred REX-a prekida napajanje elektromagnetske brave, omogućujući time otvaranje vrata. Tehnički gledano, mogli biste upotrijebiti bilo koji senzor pokreta kao REX, no posebno dizajnirani REX uređaji obično imaju znatno manje detekcijsko područje, često ograničeno samo na područje neposredno oko vrata.

Uobičajeni senzori pokreta koji se koriste za protuprovalne alarme projektirani su za nadzor cijele prostorije, pa bi u takvom slučaju mogli nehotice aktivirati bravu čak i s veće udaljenosti. REX može biti i fizički gumb koji korisnici pritisnu kako bi omogućili otvaranje vrata. [31]

Slika 2.20. Lijevo senzor, desno REX dugme [17]

3. BIOMETRIJA

Biometrija u suštini predstavlja znanstvenu disciplinu koja se bavi mjerenjem jedinstvenih fizičkih karakteristika pojedinaca, digitalnim prikazom tih osobina, te njihovim sigurnim pohranjivanjem kako bi se omogućilo precizno određivanje identiteta osobe. U svijetu biometrije, najčešće korištene metode uključuju prepoznavanje otiska prsta, prepoznavanje lica i skeniranje mrežnice oka.

Prvi slučaj primjene biometrije je u drugom stoljeću prije Krista, kada je kineski car Ts'In She koristio otisak šape tuljana za prepoznavanje pojedinih jedinki. Otisak prsta prvi put je komercijalno koristio William James Herschel 1858. godine. On je bio zadužen za izgradnju cesti u regiji Bengal, te je koristio otisak prsta kao zamjenu za potpis njegovih radnika. U 19. stoljeću, francuska je policija prva počela koristiti otisak prsta kao sredstvo identifikacije ponovnih prijestupnika. [32]

Biometrija se može podijeliti u tri glavne kategorije: biološka biometrija, morfološka biometrija i bihevioralna biometrija. Biološka biometrija koristi genetske i molekularne karakteristike za jedinstvenu identifikaciju osobe, često kroz analizu DNA koja se dobiva iz uzorka krvi ili drugih tjelesnih tekućina. Morfološka biometrija fokusira se na strukturalne karakteristike tijela, poput otiska prsta, osobina oka i oblika lica.

Bihevioralna biometrija, s druge strane, oslanja se na jedinstvene obrasce ponašanja svake osobe. To uključuje način hodanja, govor, potpis, pa čak i stil pisanja na tipkovnici kao oblike koji se mogu koristiti za identifikaciju, s različitim stupnjem pouzdanosti.

Biometrijske metode predstavljaju jedan od najsigurnijih i najpouzdanijih načina identifikacije, budući da idealna biometrijska karakteristika posjeduje univerzalnost (svaki pojedinac ju ima), jedinstvenost (razlikuje se među pojedincima), trajnost (ne mijenja se tijekom vremena) i prikupljivost (lako se može prikupiti putem senzora i jednostavno kvantificirati).

Bitno je spomenuti dva pojma, a to su: FAR (eng. False acceptance Rate) koji predstavlja učestalost pogrešnih prihvaćanja, te definira se kao postotak osoba koje neovlašteno mogu ući u sustav i FRR (eng. False Rejection Rate) koji predstavlja učestalost pogrešnih odbijanja ,te definira postotak ovlaštenih osoba kojima je odbijen pristup sustavu. [33]

U tablici 3.1. su dane biometrijske metode, te njihove karakteristike.

Tablica 3.1. Karakteristike biometrijskih metoda kontrole pristupa [3]

Metoda	Univerzalnost	Jedinstvenost	Trajnost	Prikupljivost	Sigurnost?
Lice	Velika	Mala	Srednja	Velika	Mala
Otisak prsta	Srednja	Velika	Velika	Srednja	Velika
Geometrija šake	Srednja	Srednja	Srednja	Velika	Srednja
Šarenica oka	Velika	Velika	Velika	Srednja	Velika
Mrežnica oka	Velika	Velika	Srednja	Mala	Velika
Potpis	Mala	Mala	Mala	Velika	Mala
Glas	Srednja	Mala	Mala	Srednja	Mala
Termogram	Velika	Velika	Mala	Velika	Srednja

3.1. Prepoznavanje lica

Tehnologija prepoznavanja lica sposobna je upariti ljudsko lice iz digitalne slike ili videa sa licima u bazi podataka. Tehnologija prepoznavanja lica javlja se 1960.-ih godina, kada Woody Bledsoe, Helen Chan Wolf i Charlie Bisson kreću rad na računalu koje će prepoznavati ljudska lica, međutim bili su bezuspješni. Tadašnja tehnologija još nije bili dovoljno razvijena kako bi mogla nadići, danas jednostavne probleme, kao što su: nagib glave, kut i intenzitet osvjetljenja, izrazi lica i starenje. [34]

Većina sustava se oslanja na 2D tehnologiju kamere, koja stvara dvodimenzionalnu sliku lica i precizno bilježi ključne "čvorne točke" poput oblika i veličine očiju, nosa, jagodica i drugih karakteristika. Nakon toga, sustav izračunava relativan položaj ovih točaka i pretvara ih u numerički kod. Algoritmi za prepoznavanje lica potom pretražuju pohranjenu bazu podataka lica u potrazi za potencijalnim podudaranjima. 2D tehnologija izuzetno dobro funkcionira u stabilnim i dobro osvijetljenim okruženjima, kao što su kontrolne točke na putovnicama ili slični uvjeti. Međutim, njezina učinkovitost opada u tamnijim okruženjima i kada se subjekti kreću. Osim toga, 2D tehnologija je ranjiva na prevaru putem fotografija, što ograničava njezinu pouzdanost u sigurnosnim kontekstima. Ovi se problemi mogu riješiti koristeći se tehnologijom živosti, koja detektira ukoliko je sustav u interakciji sa stvarnom osobom, a ne lažnom ili snimljenom verzijom.

Razvoj neuronskih mreža također omogućava lakše prepoznavanje pokušaja prevara. Ova vrsta strojnog učenja posvećena je otkrivanju uzoraka u slikovnim podacima.

Na primjer, Apple koristi 3D kameru kako bi napajao značajku Face ID temeljenu na toplinskoj infracrvenoj tehnologiji u svom iPhone X uređaju. Termalna infracrvena slika mapira obrasce lica dobivene prvenstveno iz obrasca površinskih krvnih žila ispod kože.Apple također šalje zabilježeni obrazac lica u "sigurni prostor" uređaja. To osigurava da se autentifikacija događa lokalno i da obrasci nisu dostupni Apple-u. [35]

Osim u svrhu otključavanja telefona, tehnologija prepoznavanja lica rade tako što uspoređuje lica prolaznika sa slikama osoba koje su evidentirane na posebnom popisu. Važno je napomenuti da ti popisi mogu uključivati slike bilo koga, a podaci se mogu prikupljati iz različitih izvora, uključujući i naše profile na društvenim mrežama. Sustavi za prepoznavanje lica variraju u svojoj izvedbi, no općenito rade na sljedeći način:

- Detekcija lica – Kamera detektira i pronalazi sliku lica, bilo da je lice samo ili u gužvi. Ova slika može prikazivati osobu koja gleda ravno ili iz profila.
- Analiza lica - Nakon toga se snima slika lica i podvrgava analizi. Većina tehnologija za prepoznavanje lica preferira 2D slike nad 3D slikama jer se 2D slika praktičnije uspoređuje s javnim fotografijama ili onima u bazi podataka. Specijalizirani softver čita geometriju vašeg lica, uzimajući u obzir ključne faktore poput udaljenosti između vaših očiju, dubine vaših očnih šupljina, razmaka od čela do brade, oblika jagodica te kontura usana, ušiju i brade. Osnovni cilj je identificirati značajne točke lica koje su presudne za jedinstvenost i prepoznavanje vašeg lica.
- Pretvaranje slike u podatke - Proces bilježenja lica transformira analogne informacije, poput lica osobe, u digitalni skup podataka temeljen na karakteristikama tog lica. Suština analize lica se zapravo svodi na matematičku formulaciju, rezultirajući numeričkim kodom poznatim kao "otisak lica". Kao što su otisci prstiju jedinstveni za svaku osobu, tako i svaka osoba ima svoj jedinstveni otisak lica.
- Pronalazak podudaranja - Vaš jedinstveni otisak lica potom se uspoređuje s bazom podataka koja sadrži informacije o drugim poznatim licima. Na primjer, FBI ima pristup broju od 650 milijuna fotografija iz različitih državnih baza podataka. Na društvenoj mreži Facebook, svaka fotografija koja je označena s imenom osobe postaje dio Facebookove vlastite baze podataka koja se također može koristiti za prepoznavanje lica. Ako vaš otisak lica pronađe podudarnost s nekom od slika u bazi podataka za prepoznavanje lica, tada se donosi određena odluka.

Među svim biometrijskim metodama, prepoznavanje lica smatra se najprirodnijom. To ima smisla jer obično prepoznajemo sebe i druge osobe upravo promatranjem njihovih lica, a ne fizičkih

otisaka prstiju ili struktura šarenice. Fascinantno je da se više od polovice svjetske populacije redovito susreće s tehnologijom prepoznavanja lica, što svjedoči o širokoj rasprostranjenosti ove tehnologije. [36]

Tehnologija prepoznavanja lica koristi se i u kontroli pristupa, te koristi 2D ili 3D metode, sa svim navedenim manama i prednostima. 2D prepoznavanje lica donosi praktičnost, ali istovremeno zahtijeva odgovarajuće sigurnosne mjere kako bi se spriječila potencijalna zloupotreba, poput korištenja fotografija ili videozapisa osobe kako bi se neovlašteno pristupilo zgradi. Ovi uređaji također moraju osigurati adekvatne svjetlosne uvjete kako bi omogućili precizno prepoznavanje lica u različitim okruženjima.

S druge strane, 3D prepoznavanje lica pokazuje veću otpornost na promjenjive svjetlosne uvjete i može biti usmjereno prema zaštiti privatnosti, s obzirom da ne koristi fotografije osoba u cijelom spektru boja. No, važno je napomenuti da veliki sustavi za prepoznavanje lica temeljeni na 3D tehnologiji još nisu postali popularni zbog nedostatka velikih skupova podataka potrebnih za obuku strojnih modela za ovakve sustave.

Prednosti prepoznavanja lica su mnoge. Prepoznavanje lica potvrđuje vaš identitet na temelju vašeg lica, a ne fizičkih predmeta poput ključnih kartica ili PIN-ova. Zbog toga predstavlja sigurniji način kontrole pristupa. Dodatno, ovaj sustav omogućuje pristup bez potrebe za fizičkim kontaktom. Jednostavno se približite čitaču, a vrata će se automatski otvoriti. Ovo je jedan od najpraktičnijih načina pristupa zgradama, eliminirajući potrebu za traženjem kartica.Važno je napomenuti da je prepoznavanje lica vrlo jednostavno za sve dobne skupine, čak i za one koji nisu vješti s tehnologijom. Nadalje, prepoznavanje lica nije podložno kloniranju kao što su to kartice. Klasične kartice i privjesci mogu se relativno lako kopirati pomoću jeftinih uređaja dostupnih online, dok prepoznavanje lica pruža siguran sustav bez tih rizika. U svijetu fleksibilnog radnog mjesta nakon pandemije, pristup putem prepoznavanja lica može se registrirati udaljeno putem mobilne aplikacije, što dodatno povećava njegovu praktičnost. Konačno, primjena prepoznavanja lica može značajno smanjiti troškove i operativno opterećenje povezane s dodjeljivanjem ključeva i kartica osobama osobno.

Iako donose brojne prednosti, važno je istaknuti nekoliko nedostataka. Terminali za prepoznavanje lica nešto su skuplji u usporedbi s tradicionalnim sustavima kontrole pristupa putem kartica. Također, važno je uzeti u obzir da prepoznavanje lica nije za svakoga. Neki ljudi izražavaju zabrinutost zbog privatnosti i straha od masovnog nadzora. Ova zabrinutost može biti opravdana, s obzirom na lošu upotrebu ove tehnologije u prošlosti. Stoga bi tvrtke koje implementiraju pristup putem prepoznavanja lica trebale razmotriti mogućnost pružanja alternativnih metoda pristupa,

kao što su ključne kartice ili mobilni uređaji, kako bi poštovale osobne izbore svojih korisnika. Također, nedostatak potpune integracije i podrške u sustavima kontrole pristupa može predstavljati izazov. Mnogi sustavi za pristup putem prepoznavanja lica prodaju se kao samostalni terminali koji samo mapiraju lice na broj kartice kako bi se povezali s trećim sustavom. Ovo može rezultirati kompliciranim i frustrirajućim iskustvom za korisnike i administratore sustava. [37]

3.2. Otisak prsta

Otisak prsta je trag koji ostavljaju nabori na krajevima prstiju i palčeva. Otisak prsta predstavlja jedan od primjera biometrije, znanstvenog pristupa koji se koristi za identifikaciju osoba putem njihovih fizičkih ili bioloških karakteristika. Važno je napomenuti da nijedna dva ljudska bića nemaju identične otiske prstiju, čak i u slučaju identičnih blizanaca. Otisci prstiju ostaju konstantni tijekom života osim u rijetkim slučajevima kada je duboki ili "bazalni" sloj oštećen ili namjerno promijenjen kirurškim postupkom. Postoje tri glavna oblika otisaka prstiju poznata kao lukovi, petlje i spirale, vidljivo na slici 3.1. Jedinstvenost svakog otiska prsta proizlazi iz različitih oblika, veličine, broja i rasporeda manjih detalja u ovim oblicima. Praksa korištenja otisaka prstiju kao sredstva identifikacije, nazvana daktiloskopija, neophodna je pomoć modernoj provedbi zakona. [38]

Slika 3.1. Oblici otiska prsta. [39]

Danas smo svakodnevno okruženi tehnologijom prepoznavanja otiska prsta koja je postala nezaobilazan dio naših života. Ona se nalazi u mobilnim telefonima, tabletima, pa čak i prijenosnim računalima kao standardna značajka. Na radnom mjestu, sve više organizacija prepoznaje vrijednost ovog biometrijskog skeniranja za praćenje prisutnosti i upravljanje svojim zaposlenicima, uz sigurnosne prednosti koje pruža. Ova tehnologija zamjenjuje tradicionalne lozinke, ID kartice i ulazne kodove na vratima. Brza, nenametljiva i jednostavna za korištenje, lako je uočiti zašto je tehnologija prepoznavanja otiska prsta postala najnaprednije i najrasprostranjenije sigurnosno rješenje na tržištu.

Softver za prepoznavanje otiska prsta radi pažljivo i precizno, izdvajajući iz otiska prsta značajne karakteristike. Skener registrira atribute kao što su orijentacija, promjene smjera grebena, prisutnost lukova i spirala u otisku. Neki napredniji skeneri čak mogu identificirati i pore na koži. Ove karakteristike potom se pažljivo bilježe i pohranjuju u sustav kako bi se u budućnosti koristile za potvrdu identiteta korisnika. Ova tehnologija omogućava visoku razinu preciznosti i sigurnosti u procesu identifikacije. [40]

Privlačnost skenera otiska prsta temelji se, između ostalog, na njihovoj visokoj razini točnosti. Oni nadmašuju tradicionalne metode sigurnosti poput lozinki i PIN-ova, sa stopom pogreške manjom od 1%. Ovo ih čini iznimno pouzdanim sredstvom za provjeru korisnika. Važno je napomenuti da stopa neuspjeha može varirati ovisno o proizvođačima i kvaliteti korištenih komponenata, a neki skeneri postižu stopu pogreške nižu od 0.1%. Ova visoka razina točnosti osigurava da se identitet korisnika može potvrditi s izuzetnom pouzdanošću, što doprinosi njihovoj privlačnosti i širokoj uporabi.

Skeneri otiska prsta pružaju iznimno olakšanje u postupku prijave, nudeći glatko i brzo rješenje za provjeru identiteta. Korisnici jednostavno trebaju dodirnuti prst na skeneru, a cijeli postupak traje samo nekoliko sekundi - značajno poboljšanje u odnosu na ponovno unošenje lozinki ili PIN-ova više puta tijekom dana. Osim toga, više ne moraju brinuti o tome jesu li slučajno zaboravili svoju karticu ili ključ kod kuće. Ova praktičnost i brzina čine skenere otiska prsta atraktivnim i korisnicima prijateljskim rješenjem za autentikaciju.

Otisak prsta predstavlja neponovljivu i jedinstvenu karakteristiku koja pripada isključivo pojedincu, čineći je izuzetno snažnom zaštitom od sigurnosnih prijetnji. Otisci prstiju, za razliku od lozinki ili PIN-ova, ne mogu se lako replicirati ili pogoditi, čime se osigurava iznimno visoka razina sigurnosti.

Osim visoke sigurnosti koju pružaju, skeneri otiska prsta su i iznimno robusni. Dizajnirani su da izdrže česte upotrebe i pruže pouzdanost tijekom vremena. Njihova je izdržljivost napredovala tijekom posljednjih deset godina, često dolazeći s visokim IP (eng. Ingress Protection) ocjenama koje označavaju otpornost na prašinu i vodu. Mnogi od njih također sadrže ugrađene funkcije protiv vandalizma, čime se osigurava zaštita čak i na mjestima s visokom frekvencijom korištenja gdje je oprema često izložena trošenju i oštećenju.

Nadalje, tijekom godina, skeneri otiska prsta postali su ekonomičniji i dostupniji. Ova ekonomska dostupnost čini ih prihvatljivim izborom ne samo za velike korporacije već i za male i srednje tvrtke koje žele ojačati svoje sigurnosne mjere i zaštiti svoje resurse.

Za razliku od nekih drugih biometrijskih tehnologija, skeneri otiska prsta zahtijevaju fizički kontakt. Ovaj zahtjev može predstavljati izazov za one koji imaju fizička ograničenja ili ozljede koje utječu na njihovu sposobnost korištenja prstiju. Tijekom pandemije postojala je tendencija izbjegavanja skenera otiska prsta, zbog mogućnosti prijenosa zarazne bolesti, međutim danas se skeneri otiska prsta ponovno koriste bez zadrške.

Unatoč tome što je izrazito sigurna metoda autentifikacije, skeneri otiska prsta nisu neprobojni. Visokokvalitetne replike otisaka prstiju pojedinca potencijalno mogu prevariti ove skenere. No, važno je napomenuti da je takav pothvat izazovan i znatno manje čest u usporedbi s drugim oblicima prijevara, kao što je krađa lozinki. U većini situacija gdje bi napadač bio voljan poduzeti takve korake, primjenjivali bi se dodatni slojevi autentifikacije kako bi se stvorilo iznimno sigurno okruženje.

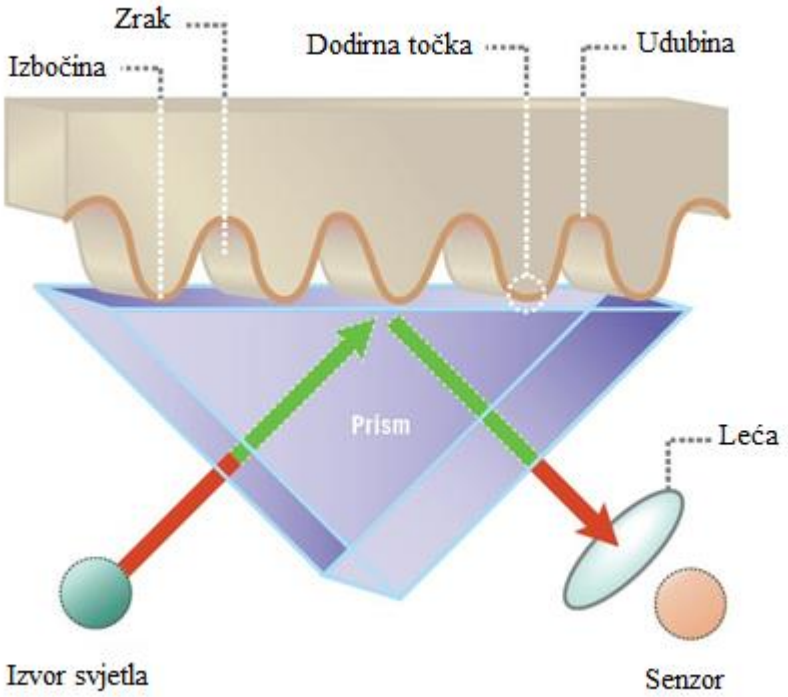
Skeneri otiska prsta mogu imati poteškoća u pouzdanom prepoznavanju otiska prsta korisnika u određenim situacijama. Prljavi, vlažni ili oštećeni otisci prsta mogu uzrokovati neuspjeh skenera, što može izazvati frustraciju i zastoje u procesu autentifikacije. U nekim se sektorima ovakvi izazovi prevladavaju povećanom primjenom različitih biometrijskih tehnologija, poput skenera lica u građevinskoj industriji gdje radnici često suočavaju s problemima degradiranih ili ozlijeđenih otisaka prstiju. Zbog toga je moguće korištenje čitača koji imaju više od jedne mogućnosti autentifikacije, prikazanog na slici 3.2. [41]

Slika 3.2. Uređaj sa više mogućnosti autentifikacije [17]

3.2.1. Optički senzor otiska prsta

Optički skenerima otisaka prsta predstavljaju jednu od najstarijih metoda za snimanje i usporedbu otisaka prsta. Kao što samo ime sugerira, ova tehnika se oslanja na snimanje optičke slike, suštinski stvarajući fotografiju otiska prsta. Nakon toga, koristi složene algoritme kako bi prepoznao jedinstvene obrasce na površini otiska, kao što su brda i žljebovi, analizirajući varijacije u svjetlini i tamnoj boji na slici.

Slično kao kod kamera na pametnim telefonima, i ovi senzori imaju svoju rezoluciju, koja određuje koliko detaljno mogu uhvatiti informacije o otisku prsta, time povećavajući razinu sigurnosti. Da bi precizno snimili te detalje, optički skeneri često koriste visoku gustoću dioda po inču, omogućavajući im da registriraju najmanje nijanse na površini otiska. No, budući da može postati prilično tamno kada prst prekrije skener, uređaji su opremljeni nizom LED dioda ili čak koriste zaslon pametnog telefona kao izvor svjetla kako bi osvijetlili sliku tijekom procesa skeniranja.



Slika 3.3. Princip rada optičkog senzora [42]

Iako su optički skeneri otisaka prsta iznimno praktični, imaju jednu značajnu manu - relativno nisku sigurnost. Ova tehnologija snima samo 2D sliku otiska, što otvara prostor za potencijalne

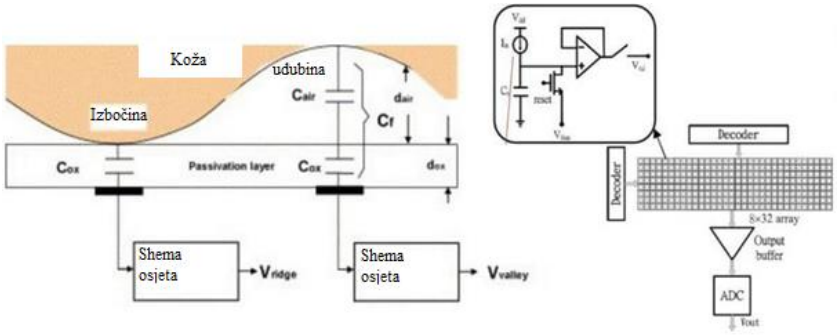
prijevare. Proteze i čak visokokvalitetne fotografije mogu se koristiti za prevaru ovog konkretnog dizajna. Iz tog razloga, ovaj tip skenera često nije dovoljno siguran za zaštitu najosjetljivijih podataka. Kao odgovor na ovu zabrinutost, industrija je razvila sigurnija hibridna rješenja koja kombiniraju više metoda za postizanje više razine sigurnosti. [42]

3.2.2. Kapacitivni senzor otiska prsta

Kapacitivni skeneri otiska prsta postali su sveprisutni, uključujući prednje i stražnje strane pametnih telefona, te najnovije verzije s ugrađenim zaslonima, zbog njihovih dodatnih sigurnosnih prednosti. Ovaj tip skenera, kako naziv sugerira, temelji se na uporabi kondenzatora za prikupljanje podataka o otiscima prstiju. Umjesto stvaranja tradicionalne slike otiska prsta, kapacitivni skeneri koriste mrežu malih kondenzatorskih krugova za prikupljanje podataka. Kondenzatori pohranjuju električni naboj i reagiraju na promjene kada se prst postavi na površinu skenera. Integrirani krug s operacijskim pojačalom koristi se za registraciju tih promjena, koje se zatim pretvaraju u digitalni oblik pomoću analognog-digitalnog pretvarača.

Nakon snimanja digitalnih podataka, analiziraju se kako bi se otkrile karakteristične i jedinstvene osobine otiska prsta, a te informacije se čuvaju za kasniju usporedbu. Ovaj dizajn posebno se ističe zbog svoje izuzetne otpornosti na prijevaru, budući da se rezultati ne mogu reproducirati putem slika, te je gotovo nemoguće prevariti ih protezama, s obzirom na različite materijale i njihove nesigurne promjene u nabojima kondenzatora. Pravi sigurnosni rizici dolaze od mogućeg hakiranja hardvera ili softvera. Stvaranjem dovoljno velikog niza ovih kondenzatora, obično stotina ili čak tisuća u jednom skeneru, postiže se iznimno detaljan prikaz otiska prsta samo pomoću električnih signala. Kao i kod optičkih skenera, više kondenzatora rezultira skenerima veće razlučivosti, čime se povećava razina sigurnosti, iako uz porast troškova proizvodnje.

Iako su kapacitivni skeneri ranije bili skupi zbog većeg broja komponenata u krugu za detekciju, današnji modeli su jednostavni za upotrebu i pružaju visoku sigurnost. Osim čitanja otiska prsta, noviji modeli također nude geste ili podržavaju prepoznavanje sile te omogućuju interakciju s drugim elementima korisničkog sučelja. [43]



Slika 3.4. Princip rada kapacitivnog senzora [43]

3.2.3. Termalni senzor otiska prsta

Ugrađeni u silikonsku ploču, termalni senzori otiska prsta koriste poseban piroelektrični materijal kako bi precizno registrirali varijacije temperature. Ova silikonska ploča opremljena je tranzistorima koji reagiraju na promjene u temperaturi stvarajući digitalni otisak prsta koji je jedinstven i karakterističan za svaku osobu. Osim toga, ova silikonska ploča sadrži vlastiti mikroprocesor koji se brine za obradu podataka tranzistora prije nego što ih pohrani. Termalni senzori dolaze u različitim izvedbama, uključujući pasivne i aktivne. Pasivni senzori koriste prirodne temperaturne razlike između okoline i površine kože kako bi generirali sliku otiska prsta. S druge strane, aktivni senzori koriste unutarnji grijaći element za otkrivanje i bilježenje temperaturnih razlika radi stvaranja slike otiska prsta.

Korištenjem termalne slike, senzor otiska prsta precizno mjeri količinu topline koja se generira kada prst dođe u kontakt s uređajem za skeniranje. Ovo postiže detektiranjem razlika u temperaturi između grebena i dolina vašeg otiska prsta u odnosu na okolnu temperaturu zraka. Taj proces koristi piroelektrični materijal koji, kao odgovor na te termalne promjene, potiče tranzistore da stvore električni naboj. Taj električni naboj zatim oblikuje jedinstveni digitalni predložak koji se koristi u svrhu autentifikacije.

Termalni senzori otiska prsta donose mnoge prednosti, uključujući njihovu iznimnu preciznost i sposobnost upotrebe u različitim uvjetima, bez obzira na to jesu li površine mokre ili suhe. Osim toga, ističu se visokom razinom sigurnosti, budući da je repliciranje ili krivotvorenje termalne slike vašeg otiska prsta gotovo nemoguće. Ipak, važno je napomenuti da su osjetljivi na ekstremne okolišne uvjete, što ih čini manje pouzdanim u područjima s naglim temperaturnim promjenama.

Također, njihov proces obrade otiska prsta može trajati nešto dulje, a njihova nabavna cijena može biti relativno visoka u usporedbi s drugim vrstama skenera. [44]

3.2.4. Ultrazvučni senzor otiska prsta

Koristeći naprednu ultrazvučnu tehnologiju, ovaj senzor precizno i brzo skenira vaš otisak prsta kako bi stvorio detaljnu 3D sliku. Visokofrekventni zvučni valovi prodiru kroz površinu kože, reflektiraju se od donjih slojeva dermisa i bilježe karakteristične značajke, uključujući grebene linije i pore za znojenje. Ovaj jedinstveni proces omogućuje senzoru da čita otiske prsta s visokom preciznošću, čak i u slučaju prljavih ili masnih otisaka. Primjenom pulznog jeke, ultrazvučni skeneri osiguravaju učinkovitu i sigurnu identifikaciju u realnom vremenu.

Ultrazvučni senzori otiska prsta koriste sofisticiranu tehniku sličnu sustavu radara. Oni emitiraju električne impulse pretvorene u ultrazvučne valove, koje usmjeravaju prema površini vašeg prsta. Ovi zvučni valovi prolaze kroz vanjski sloj kože i zatim se reflektiraju od unutarnjih struktura, uključujući karakteristične grebene i pore za znojenje u dermisu. Kada se odjeci od tih unutarnjih struktura vrate i budu uhvaćeni od strane prijemnika, formiraju jedinstveni otisak prsta. Tada se ti odjeci analiziraju i pretvaraju u digitalni format putem mikroprocesora te se pohranjuju kao predložak za buduće usporedbe. Ovaj napredni proces, omogućuje stvaranje trodimenzionalne slike otiska prsta za preciznu usporedbu, čime se olakšava razlikovanje čak i prljavih ili masnih otisaka. [44]

Ultrazvučni senzori otiska prsta ističu se svojom nadmoćnom preciznošću u odnosu na tradicionalne kapacitivne i optičke skenere, budući da bilježe razlike između grebena, a ne samo rubova otiska. Ova unaprijeđena sposobnost čini ih iznimno učinkovitima čak i kada su prsti izloženi vlazi ili nečistoći. Naravno, ova visoka razina preciznosti dolazi s cijenom, ali nudi nevjerojatnu pouzdanost tijekom dugog vremenskog razdoblja. Ultrazvučni senzori otiska prsta donose niz prednosti, no važno je napomenuti i nekoliko nedostataka. Unatoč tome, njihova izvanredna preciznost i otpornost na habanje čine ih idealnim za tvrtke koje postavljaju visoke standarde sigurnosti bez kompromisa u pogledu preciznosti i pouzdanosti. [45]

3.3. Geometrija ruke

Održivi uređaji za prepoznavanje geometrije ruke počeli su se razvijati još u ranim 1970-ima, označavajući time početak široke primjene geometrije ruke u računalnom svijetu. Inovator Robert Miller prepoznao je potencijal karakterističnih značajki veličine i oblika ruke za svrhu identifikacije te je 1971. godine patentirao prvi automatizirani uređaj za prepoznavanje geometrije ruke u Institutu Stanford Research Institute. Ovaj inovativni uređaj koristio je mjerenja ruke i

usklađivao ih s otvorima na korisničkoj identifikacijskoj kartici kako bi aktivirao identifikacijski krug. Važnu ulogu u razvoju uređaja za prepoznavanje geometrije ruke imao je i David Sidlauskas, koji je patentirao Handkey ID3D, prvi uređaj za skeniranje ruke koji je koristio 3D tehnologiju. Ovaj uređaj je integrirao optičku mjernu ploču, kameru i numeričku tipkovnicu za unos osobnog PIN-a, postavši tako značajan korak naprijed u razvoju ove tehnologije. [46]

Primjene biometrije za prepoznavanje geometrije ruke, iako možda nisu tako očite kao u slučaju drugih biometrijskih metoda poput otisaka prstiju ili prepoznavanja lica, ostaju relevantne u različitim kontekstima, posebno kada je riječ o fizičkom pristupu i praćenju radnog vremena. Ova vrsta biometrije se temelji na pretpostavci da je geometrija ruke svake osobe jedinstvena. Iako nema apsolutnih dokaza koji potvrđuju jedinstvenost geometrije ruke s obzirom na moguće varijacije anatomskih struktura unutar različitih pojedinaca, možemo je promatrati kao fiziološku karakteristiku koja se može koristiti za jedinstvenu identifikaciju pojedinca. [47]

Biometrijski sustavi za prepoznavanje geometrije ruke pažljivo uzimaju u obzir karakteristike ne samo prstiju, već i površine same ruke te njezin profil s bočne strane. Snimanje slika obavlja se dok je ruka postavljena dlanom prema dolje na potporu i precizno pozicionirana pomoću vodilica. Tijekom ovog procesa, bilježe se mjere poput duljine, širine, debljine i površine ruke osobe, a iz tih mjerenja izvlače se brojne značajke i detalji. Često se snima više slika iste ruke kako bi se stvorio 3D predložak s dovoljno informacija za svrhe identifikacije. Slike zajedno s pripadajućim podacima zatim se brižno pohranjuju u bazu podataka i koriste za provjeru identiteta osobe koja se ponovno snima. Uspoređuju se s referentnim slikama kako bi se entitet potvrdio ili odbacio, što omogućava preciznu i pouzdanu verifikaciju identiteta. [48]

Prepoznavanje geometrije ruke temelji se na jedinstvenim karakteristikama oblika ruke pojedinca, uključujući površinu, debljinu, duljinu i širinu ruke, kao i dimenzije prstiju, udaljenosti između zglobova i oblik članaka. Ova precizna mjerenja omogućuju stvaranje jedinstvene biometrijske matrice. U pogledu točnosti, sustavi prepoznavanja geometrije ruke su izuzetno precizni, neovisno o jedinstvenim točkama podataka koje se ne koriste kao u drugim biometrijskim sustavima, poput prepoznavanja retine. Geometrija ruke jedinstvena je sama po sebi zbog oblika ruke. Zbog toga se prepoznavanje geometrije ruke primarno koristi za verifikacijske aplikacije, kao što su kontrola fizičkog pristupa i evidencija radnog vremena. Iako većina ljudi ima svoje jedinstvene značajke na rukama, te karakteristike nisu tako bogate informacijama kao što su šarenica ili retina oka. Sustavi za prepoznavanje ruke su dizajnirani za precizno bilježenje i mapiranje oblika ruke, pa čak i za prilagodbu manjim promjenama u obliku ruke uzrokovanim fluktuacijama tjelesne težine. Danas, čitači geometrije ruke mogu pohranjivati biometrijske podatke za više od 40 000 subjekata i i dalje pružati izvanrednu učinkovitost i preciznost. [46]

Slika 3.5. Uređaj za skeniranje geometrije ruke [46]

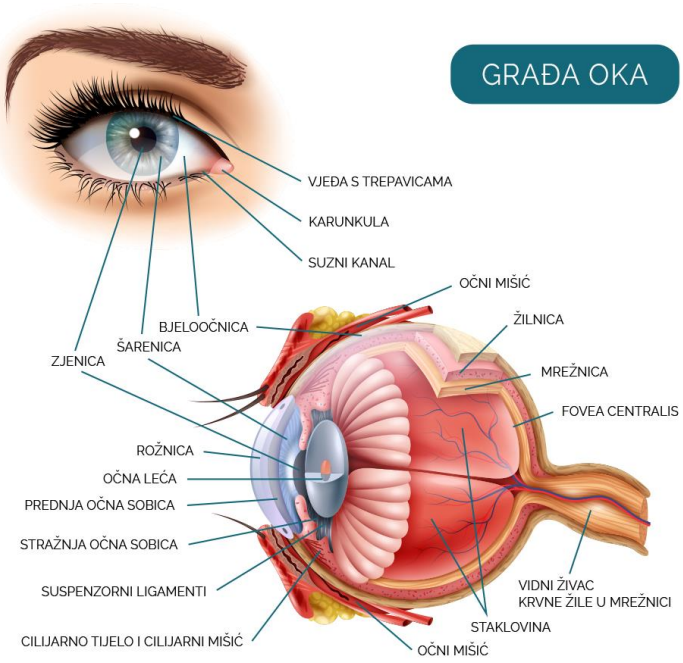
Univerzalnost je jedna od glavnih prednosti ove metode. Većina ljudi može koristiti ovu tehnologiju jer svatko ima barem jednu ruku s jedinstvenim karakteristikama, a tehnologija je čak toliko napredovala da se čak i fizičke deformacije (do određenog stupnja) mogu uzeti u obzir.. Tehnologija je čak prilagodljiva za ljevoruke osobe, čineći je vrlo pristupačnom. Većina ljudi ima neke jedinstvene značajke na svojim rukama, no one nisu tako bogate podacima kao što je, na primjer, retinalne skeniranje. Nedostatak ove metode je njena osjetljivost na vanjske utjecaje. Ruka, kao vanjski dio tijela, može biti podložna promjenama uzrokovanim ozljedama, varijacijama tjelesne težine i drugim faktorima kao što su bolesti poput reumatizma. Sirove slike ruku nisu podložne površinskim nedostacima kože poput prljavštine i ožiljci. Iako nema mnogo podataka, preciznost prepoznavanja geometrije ruke je visoka, što rezultira malom pogreškom. Međutim, uređaji mogu biti veliki, što može utjecati na njihovu percepciju i prihvaćanje od strane korisnika. Većina ljudi širom svijeta dobro prihvaća prepoznavanje geometrije ruke jer se smatra neinvazivnim. Jedini potencijalni problem je briga o higijeni površine na koju se stavlja ruka, jer zahtijeva izravan kontakt s korisnikom. Teško je varati prepoznavanje geometrije ruke jer zahtijeva stvaranje 3D fizičkog modela ruke, što je izazovno. [48]

3.4. Prepoznavanje šarenice

Prepoznavanje šarenice predstavlja automatiziranu metodu biometrijske identifikacije koja koristi matematičke tehnike za analizu vizualnih slika jedne ili obje šarenice u očima pojedinca. Ove šarenice karakteriziraju složeni i jedinstveni obrasci, stabilni u vremenu, te mogu biti promatrani s određene udaljenosti. Učinkovitost svih biometrijskih tehnologija oslanja se na količinu informacijske raznolikosti koju mogu prikupiti i iskoristiti za usporedbu. Prepoznavanje šarenice izuzetno je uspješno u ovom smislu, sprječavajući "kolizije" ili lažna podudaranja čak i u usporedbama među masovnim populacijama. Njegovo glavno ograničenje leži u zahtjevu za blizinom kamere prilikom snimanja slika, obično unutar metra ili dva. Međutim, razvoj tehnologije omogućava sve veće udaljenosti snimanja, čak i do 10 metara, te primjenu u stvarnom vremenu putem video prijenosa.

Iako je John Daugman patentirao prve algoritme za prepoznavanje šarenice u 1990-ima, ovaj koncept ima dugu povijest i danas ga prate mnogi znanstveni istraživači. Već 1953. godine, F.H. Adler je prepoznao potencijal šarenice kao sredstva identifikacije i citirao J.H. Doggarta, oftalmologa iz 1949. godine, koji je opisao raznolikost šareničnih oblika kao potencijalno beskrajne. Slijedeći taj put, američki oftalmolozi L. Flom i Aran Safir patentirali su sličnu pretpostavku, ali nisu imali konkretni algoritam za implementaciju. Tijekom godina, Daugman je razvio algoritme za prepoznavanje šarenice koji su postali temelj za mnoge implementacije. Ovi algoritmi su pružili izvanredne rezultate i korišteni su u mnogim tvrtkama. [49]

Šarenica je obojeni, krugolik dio oka koji se nalazi iza rožnice i oko zjenice. Oblik šarenice svake osobe je jedinstven i ostaje konstantan tijekom cijelog života. Dodatno, budući da je prekrivena rožnicom, šarenica je pouzdano zaštićena od oštećenja, što je čini idealnim dijelom tijela za provođenje biometrijske autentifikacije. [50]



Slika 3.6. Građa oka [51]

Tehnologija skeniranja šarenice vrši jedinstveno mjerenje u obojenim krugovima očiju ljudi. Biometrijski skenerima za prepoznavanje šarenica koriste nevidljivu infracrvenu svjetlost za osvjetljavanje šarenice kako bi uhvatili jedinstvene obrasce koji inače nisu vidljivi golim okom. Ovi uređaji za prepoznavanje šarenica uklanjaju trepavice, kapke i spekularne refleksije koje obično zaklanjaju šarenicu, rezultirajući skupom piksela koji precizno predstavlja šarenicu. Nakon toga, uzorak linija i boja oka se analizira kako bi se izdvojio ključni obrazac koji sadrži informacije o šarenici. Ovaj ključni obrazac se digitalizira i uspoređuje s pohranjenim šablonama u bazi podataka kako bi se postigla verifikacija (jedan-na-jedan usporedba) ili identifikacija (jedan-na-mnogo usporedba). Kamere za prepoznavanje šarenica mogu biti postavljene na fiksnim mjestima, kao što su zidovi, ili biti prenosive i prijenosne.

Skenere za šarenicu prikupljaju oko 240 biometrijskih karakteristika, čija kombinacija je ekskluzivna za svako oko. Ovi uređaji potom stvaraju digitalnu reprezentaciju ovih podataka, precizno bilježeći informacije dobivene iz šarenice. Ova numerička reprezentacija tih izdvojenih informacija iz slike šarenice se pohranjuje u računalnoj bazi podataka. [52]

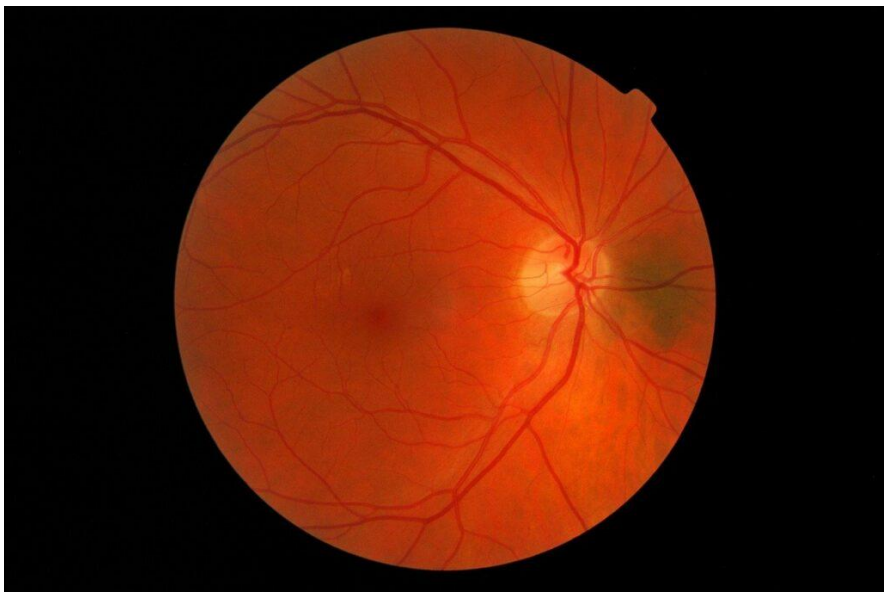
Slika 3.7. Uređaj za prepoznavanje šarenice oka [53]

Raspoznavanje šarenice odlikuje se iznimnom preciznošću među raznim biometrijskim tehnologijama. Bitno je napomenuti da se oblik šarenice u pravilu ne mijenja tijekom života, iako se to ne može smatrati apsolutnom garancijom. Osim toga, s obzirom na različite uzorke šarenica u lijevom i desnom oku, moguće je provesti odvojeno prepoznavanje za svako oko, čime se omogućava razlikovanje blizanaca. Ova tehnologija funkcionira čak i kada osoba nosi šešir, masku, naočale ili rukavice, pod uvjetom da su oči vidljive, što doprinosi njezinoj praktičnoj primjeni. Koristeći infracrvene kamere, moguće je izvoditi prepoznavanje šarenice čak i noću ili u potpunom mraku, proširujući njezinu upotrebu na različite uvjete osvjetljenja. Dodatno, beskontaktna autentikacija omogućuje upotrebu tehnologije bez potrebe za dodirivanjem uređaja, što čini ovu metodu higijenski prihvatljivom. [54]

3.5. Skeniranje mrežnice

Retina, nježan sloj živčanog tkiva koji prekriva unutarnje područje dvije trećine očne jabučice, predstavlja mjesto gdje se svjetlosna stimulacija pretvara u osjećaj vida. Fascinantno je da je retina, u stvarnosti, produžetak samog mozga, formirana u embrionalnom razvoju od živčanog tkiva i povezana s glavnim mozgom putem optičkog živca. Zbog kompleksne strukture kapilara koje opskrbljuju mrežnicu krvlju, svaka osoba ima jedinstvenu mrežnicu. Mreža krvnih žila u mrežnici toliko je složena da čak ni identični blizanci nemaju sličan uzorak. [55]

Koncept identifikacije mrežnice prvi put je osmišljen od strane Carletona Simona i Isadorea Goldsteina, te je prvi put predstavljen u časopisu New York State Journal of Medicine 1935. godine. Ova ideja bila je napredna za svoje vrijeme, no kako se tehnologija razvijala, koncept uređaja za skeniranje mrežnice počeo je postajati stvarnost u 1975. godini. U 1976. godini, Robert "Buzz" Hill osnovao je tvrtku nazvanu EyeDentify, Inc., i posvetio se daljnjem istraživanju i razvoju ovog uređaja. Patenti su pridruženi ovom konceptu 1978. godine, označavajući korak prema ostvarenju ovog sustava. Uz kontinuirani napredak, komercijalni model uređaja za skeniranje mrežnice postao je dostupan 1981. godine. [56]



Slika 3.8. Mrežnica [57]

Biometrijska metoda poznata kao skeniranje mrežnice koristi se za precizno mapiranje jedinstvenih uzoraka mrežnice osobe. Krvne žile unutar mrežnice imaju sposobnost apsorbirati svjetlost više nego okolno tkivo, što omogućava njihovu preciznu identifikaciju uz odgovarajuće osvjetljenje. Proces retinalnog skeniranja provodi se suptilno, pri čemu se nevidljiva niska infracrvena svjetlost usmjerava u oko osobe dok promatra kroz okular skenera. Ova zraka svjetla putuje prema standardiziranoj putanji preko površine mrežnice. Zbog posebne osjetljivosti retinalnih krvnih žila na to svjetlo, količina refleksije varira tijekom skeniranja, stvarajući jedinstveni uzorak za svaku osobu.

Varijacije u obrascima pretvaraju se u računalne kodove i pažljivo pohranjuju u bazu podataka. Vrijedno je napomenuti da retinalno skeniranje također ima važne medicinske primjene. Naime, različite bolesti, poput infektivnih bolesti kao što su AIDS, sifilis, malarija, ili vodene kozice, kao i nasljedne bolesti kao što su leukemija, limfom, i anemija srpasta stanica, često ostavljaju tragove

na očima. Također, retinalno skeniranje može otkriti indikatore kroničnih zdravstvenih problema kao što su zatajenje srca, ateroskleroza i povišeni kolesterol, često prije nego što se simptomi manifestiraju na drugim dijelovima tijela. [58]

Prepoznavanje mrežnice predstavlja precizan proces koji uključuje pažljivo skeniranje mrežnice oka i usporedbu dobivenih podataka s jedinstvenim značajkama mrežnice. Ova metoda izdvaja se kao jedna od najizvanrednijih tehnika biometrijske identifikacije dostupnih. Prilikom točnog skeniranja mrežnice, prikupi se impresivan niz od čak 400 jedinstvenih podataka za analizu. To je značajna razlika u odnosu na otprilike četrdeset jedinstvenih podataka koji se prikupljaju kod skeniranja otisaka prsta.

Procedura snimanja i verifikacije retinalnog skeniranja slijedi iste principe kao i druge biometrijske tehnologije, no ovaj proces se odvija kroz tri ključna koraka.

Prvi korak obuhvaća pažljivo snimanje slike mrežnice i njezinu transformaciju u digitalni format koji će se kasnije uspoređivati s bazom podataka. Inicijalna faza akvizicije i obrade slike zahtijeva najviše pažnje. Brzina i učinkovitost ovog koraka znatno ovise o suradnji korisnika. Da bi se izvršilo skeniranje, korisnik mora precizno pozicionirati svoje oko blizu uređaja i ostati potpuno miran kako bi osigurao jasnu sliku. Korisnici, dok promatraju skener, percipiraju zelenu svjetlost na pozadini bijelog svjetla. Nakon što se skener aktivira, zelena svjetlost putuje u potpuni krug (360 stupnjeva), obuhvaćajući cijelu površinu oka. Nakon završetka ovog procesa, uzorak krvnih žila u mrežnici bilježi se u svoj svojoj cjelovitosti. Ovisno o razini suradnje korisnika, faza snimanja može potrajati i do jedne minute, što je u usporedbi s drugim tehnikama biometrijske identifikacije prilično precizno. Uobičajeno je snimiti tri do pet slika kako bi se osigurala sveobuhvatna usporedba i maksimalno pouzdanje.

U drugoj fazi koristi se specijaliziran program za usporedbu slike mrežnice. Taj program traži točno podudaranje s bazom podataka kako bi identificirao korisnika. S obzirom na to da genetski čimbenici ne utječu na obrazac krvnih žila u retini, svaka slika mrežnice sadrži različite, jedinstvene značajke. Kao što smo već naglasili, slika retine može sadržavati čak do 400 jedinstvenih podataka koji čine osnovu za usporedbu.

Jedinstvene značajke mrežnice prikazuju se kao biometrijski predložak. Tijekom treće i završne faze ovog procesa, jedinstveni uzorak mrežnice transformira se u digitalni predložak za pohranu. Ovaj predložak retine zauzima iznimno malen prostor, veličine svega 96 bajtova, čime predstavlja jedan od najmanjih biometrijskih predložaka u upotrebi. [57]

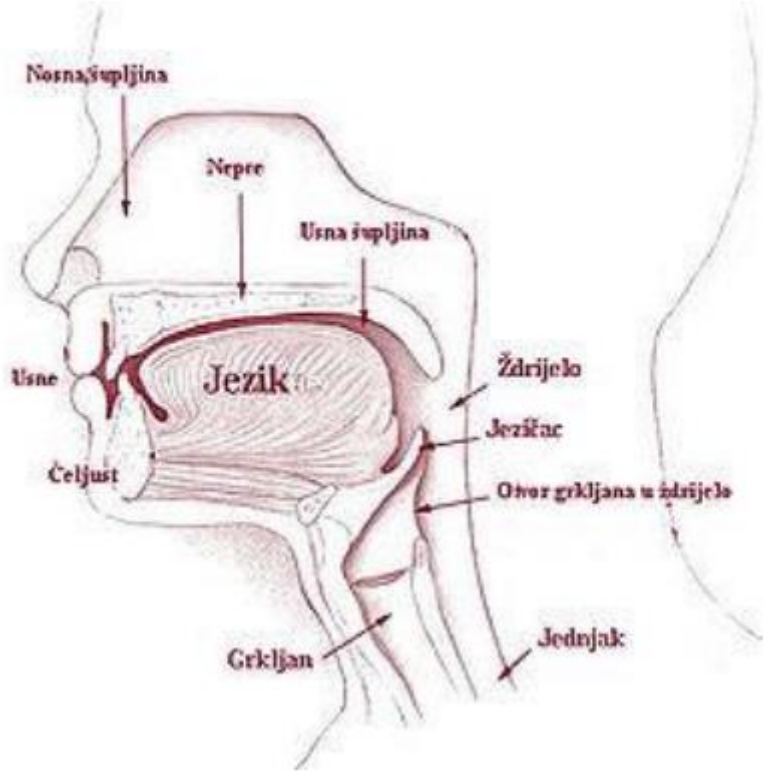
Mrežnica, koja se rijetko mijenja tijekom života pojedinca, uistinu zauzima poseban položaj kao jedna od najstabilnijih i pouzdanijih biometrijskih tehnologija dostupnih na tržištu danas. Njena prednost dalje dolazi do izražaja kroz brzinu i efikasnost sustava. Zahvaljujući kompaktnim datotekama predložaka za prepoznavanje mrežnice, verifikacija identiteta pojedinca odvija se u trenu, često za manje od dvije sekunde. S obzirom na obilje jedinstvenih podataka koje posjeduje, retina gotovo izbjegava greške u identifikaciji; kad sustav prepoznavanja mrežnice potvrdi identitet osobe, možemo biti iznimno sigurni da se radi o toj osobi. Drugim riječima, statistička vjerojatnost da bi sustav pogrešno prihvatio lažnjaka gotovo je zanemariva. Važno je napomenuti da mrežnica, koja se nalazi duboko unutar strukture oka, nije izložena vanjskim utjecajima i okolini, za razliku od drugih biometrijskih tehnologija poput prepoznavanja geometrije ruke ili otisaka prsta.

Općenito, postoji vrlo negativan odnos prema korištenju prepoznavanja mrežnice. Na primjer, zbog same nametljivosti s kojom je povezano, mnogi ljudi smatraju da to predstavlja ozbiljan rizik za zdravlje oka, iako to nije slučaj. Postoji vrlo snažna nelagoda u vezi s tim da je potrebno staviti oko u prijemnik i usmjeriti infracrveni svjetlosni snop izravno na njega. U usporedbi s drugim biometrijskim modalitetima, prepoznavanje retine zahtijeva najvišu razinu suradnje i motivacije od strane krajnjeg korisnika kako bi se dobile visokokvalitetne sirove slike. Kao rezultat toga, sposobnost za provjeru metrike može biti niska, čak i 85% (dok su drugi načini biometrike do 99% ili čak 100%). Zbog pažnje koja se traži od krajnjeg korisnika, može biti potrebno više pokušaja i puno vremena da se dobiju potrebni rezultati. Kao rezultat toga, ako postupak nije izveden ispravno, može doći do velikog postotka lažnih odbijanja.

Univerzalnost ove tehnologije proizlazi iz činjenice da gotovo svaka osoba, osim u slučajevima ozbiljnih problema s vidom, ima mrežnicu, što otvara mogućnost za primjenu retinalnog skeniranja. Osim genetskog niza (DNK), mrežnica sadrži najveći broj jedinstvenih podataka u čitavom ljudskom tijelu, a njezina postojanost, osim u iznimnim medicinskim situacijama, čini je pouzdanim biometrijskim rješenjem koje se rijetko mijenja tijekom života pojedinca. Međutim, prikupljanje visokokvalitetnih slika mrežnice može biti izazovno, budući da je područje skeniranja ograničeno. Performanse prepoznavanja retine nadmašuju mnoge druge tehnike s iznimno visokom razinom točnosti, dosežući stope pogreške koje se mogu spustiti i do jedan prema jedan milijun. Unatoč ovim prednostima, prihvaćenost retinalnog skeniranja među općom populacijom ostaje niska. Uz to, stabilnost i bogatstvo podataka mrežnice čine je izuzetno otpornom na prijevare. Zbog tih karakteristika, primjene na tržištu za prepoznavanje mrežnice su izrazito ograničene i često se koristi tamo gdje su potrebni najviši standardi sigurnosti, kao što su vojne instalacije, nuklearni objekti, te napredni istraživački laboratoriji. [59]

3.6. Prepoznavanje glasa

Proučavanje ljudskog glasa ima duboko ukorijenjenu povijest u znanosti, budući da nam omogućava bolje razumijevanje načina na koji ljudi uspostavljaju međusobnu komunikaciju i društvenu interakciju. Tradicionalno se smatra da se glas sastoji od dva međusobno povezana procesa: stvaranja početnog zvuka i njegove modifikacije. Grkljan generira zvuk s raznovrsnim frekvencijama, a taj spektar se mijenja tijekom vremena uz pomoć jezika, zubi, nepca i drugih elemenata. Ljudski glas ima različite izvore. Obično, energija za stvaranje zvuka dolazi od zraka koji izlazi iz pluća i putuje prema grkljanu gdje utječe na glasnice. U govoru, glasnice, odnosno glasne žice, počinju vibrirati, a zrak koji prolazi kroz njih stvara zvučne valove. To možete jednostavno osjetiti stavljajući prste na Adamovu jabučicu dok govorite. Na slici 3.9. prikazani su anatomski organi u ljudskoj glavi koji igraju ključnu ulogu u procesu stvaranja ljudskog glasa, uključujući pluća, grkljan i glasnice, ždrijelo, usnu i nosnu šupljinu te jezik, zube, usne, nepce i čeljust koji oblikuju zvučne valove. [60]



Slika 3.9. Organi potrebni za stvaranje glasa [60]

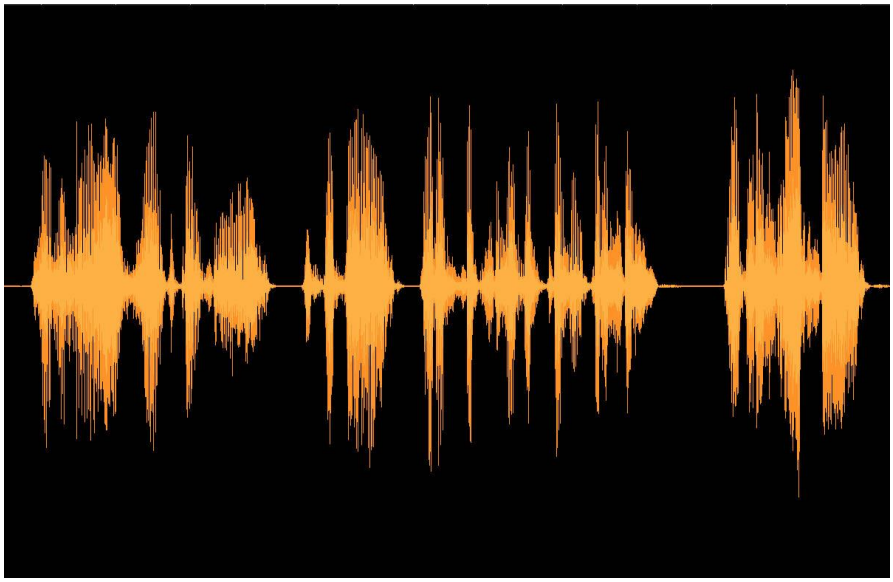
Biometrija glasa se fokusira na prepoznavanje specifičnih karakteristika i osobina govornika, neovisno o sadržaju izgovorenih riječi. Svaki naš glas ima prepoznatljive karakteristike koje proizlaze iz naše anatomije, kao što su oblik i veličina usta, grla i jezika, te različiti obrasci govora,

uključujući brzinu izgovaranja. Te osobine oblikuju jedinstvenu glasovnu identifikaciju svakog pojedinca.

Tehnologija biometrije glasa ima ključnu ulogu u verifikaciji govornika. Kombinirajući je s drugim sigurnosnim faktorima poput identifikacijskih oznaka, lozinki ili PIN-ova, biometrija glasa pruža dvostruku autentifikaciju za siguran pristup web-lokacijama, zgradama i materijalima. Znanstvenici su čak koristili biometriju glasa kako bi identificirali vukove u Nacionalnom parku Yellowstone prema njihovim jedinstvenim zavijanjima. [61]

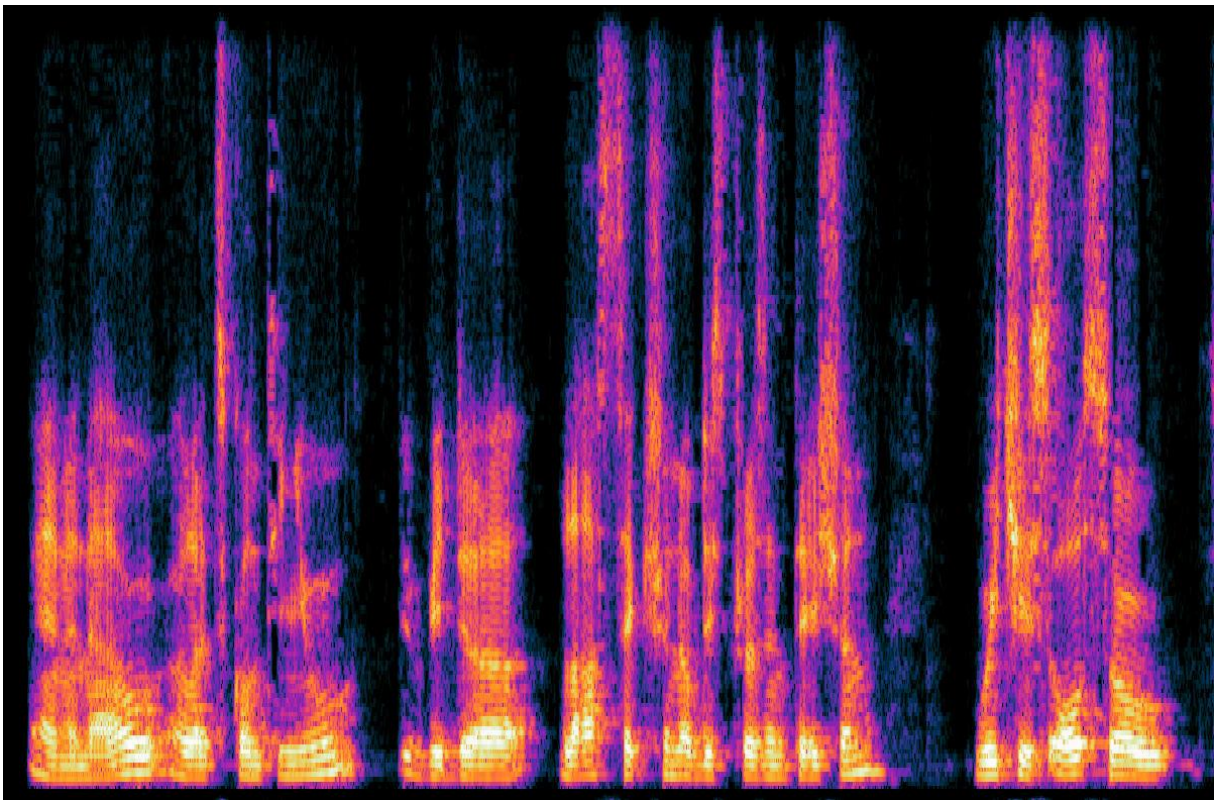
Proces biometrijske identifikacije glasom podijeljen je na dva glavna koraka. Prvi korak obuhvaća izdvajanje glasovnog uzorka, u kojem sustav za biometriju glasa analizira i stvara matematički model glasovnih karakteristika osobe, poznat kao zvučni otisak. Ovaj postupak može se nazvati i upisivanje glasa ako se analizira glas neke osobe po prvi put. Drugi korak uključuje usporedbu izdvojenog zvučnog otiska s pohranjenim zvučnim otiscima u svrhu pronalaženja odgovarajuće podudarnosti, što je ključno za uspješno potvrđivanje ili identifikaciju govornika. Važno je napomenuti da izdvajanje zvučnog otiska obično zahtijeva više vremena i resursa, dok je faza usporedbe zvučnih otisaka izrazito brza i može provesti milijune usporedbi u svega nekoliko sekundi. Ova metoda se može usporediti s otiskom prsta, budući da je svaki glas jednako jedinstven kao i svaki otisak prsta.

Zvuk može biti prikazan u obliku valova, kao na slici 3.10.



Slika 3.10. Zvučni valovi [62]

Ili u obliku spektograma, kao na slici 3.11.



Slika 3.11. Spektogram zvuka [62]

Spektrogram pruža dublju analizu zvučnog vala, gdje okomita os predstavlja frekvenciju, vodoravna os označava vrijeme, a svjetlina predstavlja amplitudu zvučnog vala. Iz te analize spektrograma, sustav za biometriju glasa istražuje karakteristike i dinamiku akustičnog vala generiranog glasom osobe, oblikujući matematički model koji sadrži jedinstvene glasovne karakteristike (obično predstavljene skupom brojeva s pomičnim zarezom). Da bi pronašao odgovarajući skup brojeva koji zastupaju anatomiju i pokrete vokalnih organa osobe, koriste se statistički i pristup umjetnom inteligencijom.

Prilikom prvog stvaranja zvučnog otiska (proces poznat kao "upisivanje glasa"), često je potrebno nekoliko desetaka sekundi govora osobe kako bi se stvorio čvrst i precizan zvučni otisak za buduće usporedbe zvučnih otisaka. Postupak izdvajanja zvučnih otisaka može biti aktivan ili pasivan. Aktivno izdvajanje zvučnih otisaka podrazumijeva da osoba svjesno sudjeluje u postupku, obično ponavljajući određenu frazu ili niz riječi koje pruža sustav. S druge strane, pasivno izdvajanje zvučnih otisaka obavlja se bez izravnog sudjelovanja osobe, odnosno snimanjem normalnog razgovora.

Nakon izdvajanja, zvučni otisci se pohranjuju u bazi podataka zvučnih otisaka u specifičnom formatu koji je jedinstven za svaku tvrtku koja koristi biometriju glasa. Iz tog razloga, zvučni otisci nisu međusobno kompatibilni s različitim sustavima za biometriju glasa od različitih pružatelja usluga.

Važno je napomenuti da iz zvučnog otiska nije moguće rekonstruirati izvorni govor osobe, čime se osigurava anonimnost sadržaja govora.

Zvučne otiske možete uspoređivati u odnosu jedan prema jednom (1:1) za verifikaciju govornika i forenzičku analizu glasa, jedan prema mnogo (1:N) za identifikaciju govornika, pretragu govornika i praćenje govornika, te mnogo prema mnogo (N:M) za grupiranje govornika (kao i za identifikaciju govornika, pretragu govornika i praćenje govornika).

U postupku biometrijske autentifikacije glasom, dvije vrste pogrešaka su relevantne - lažno prihvaćanje (eng. false acceptance) i lažno odbijanje (eng. false rejection). S obzirom na namjenu, sustav za biometrijsku autentifikaciju glasom može prilagoditi prag rezultata, odnosno može se prilagoditi vrijednost iznad koje osoba prolazi verifikaciju ili identifikaciju, kako bi postigao različite razine sigurnosti. To može rezultirati većom sigurnošću s nižom stopom lažnih prihvaćanja - FAR (eng. false acceptance rate) ili većom pragmatičnošću s nižom stopom lažnih odbijanja - FRR (eng. false rejection rate). Povećanjem praga za prihvaćanje smanjuje se FAR, ali raste FRR. Smanjenje praga ima suprotan učinak, povećavajući FAR, ali smanjujući FRR. Stoga se pragovi odabiru ovisno o potrebama, kao što su visoka sigurnost ili otkrivanje važnih kriminalaca.

Suvremeni sustavi za prepoznavanje govornika temeljeni na dubokim neuronskim mrežama također pružaju iznimno visoku točnost. Dodatno, prilagodbom kroz kalibracije koje uzimaju u obzir sigurnosne zahtjeve i jedinstvene karakteristike glasa i jezika, preciznost rješenja za biometrijsku autentifikaciju glasom može se dalje poboljšati.

Za moderne metode biometrijske verifikacije glasom, posebno one koje kontinuirano prate karakteristike glasa tijekom cijelog razgovora, važno je napomenuti da su neovisne o jeziku i riječima koje se izgovaraju. Dodatno, u skladu s Općom uredbom o zaštiti podataka Europske unije (eng. GDPR), važno je napomenuti da se zvučni otisak smatra osjetljivim osobnim podacima i podliježe strogim sigurnosnim mjerama pri obradi. Ova praksa je široko prihvaćena, čak i izvan EU.

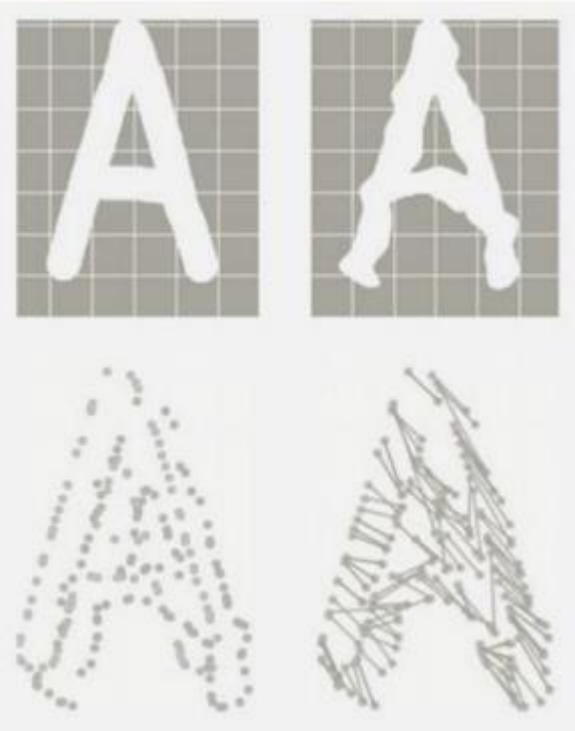
Postupak generiranja zvučnih otisaka prirodno se usklađuje s pravilima sigurnosti podataka navedenima u GDPR-u i drugim sličnim politikama o zaštiti podataka. Biometrijska autentifikacija glasom predstavlja siguran način autentifikacije koji istovremeno poboljšava razinu sigurnosti i korisničko iskustvo. [63]

4. PROJEKT

U ovom poglavlju biti će napravljen projekt kontrole pristupa koji osim standardne identifikacije korisnika karticama dodatno koristi kamere sa funkcijom prepoznavanja registarskih oznaka vozila, inače poznate kao LPR kamere (eng. Licence Plate Recognition).

4.1. LPR kamera

Prepoznavanje registarskih oznaka ili LPR/ANPR (eng. License plate recognition/Automatic Number Plate Recognition) tehnologije su koje omogućuju automatsko prepoznavanje registarskih oznaka na vozilima. U tu svrhu koristi se kombinacija računalnog vida, optičkog čitanja i strojnog učenja kako bi se automatski detektirale registracije vozila te izdvojili alfanumerički znakovi s pločice. Računalni vid područje je u umjetnoj inteligenciji za prepoznavanje dvodimenzionalnih ili trodimenzionalnih predmeta, dok je optičko čitanje ili OCR (eng. Optical Character Recognition) tehnika koja koristi optičke senzore i računalne algoritme kako bi interpretirala vizualne podatke i prevela ih u digitalni oblik razumljiv računalu. LPR/ANPR se sastoji od dvije osnovne faze, pronalaženja tablice i čitanja znakova. Scene videonadzora mogu sadržavati brojne znakove, uključujući reklame, izloge, nazive tvrtki na vozilima itd., zbog kojih sustav prvo mora ograničiti čitanje znakova samo s registarske oznake vozila. Nakon što se pločica pronađe, izvršava se čitanje znakove s pločice koje često zna biti otežano zbog kuta gledanja kamere, veličine i fonta znakova, slika na registraciji (grb ili naljepnica), svjetline, prljavštine, vremenskih nepogoda itd. Tradicionalni OCR uzima pojedini znak s tablice kao ulazni signal te ga uspoređuje sa svim znakovima u sustavu ili ga rastavlja na dijelove i uspoređuje te dijelove s pripadajućim uzorcima. Na slici 4.1. prikazano je slovo A.



Slika 4.1. Detekcija slova "A" [64]

Putem analize oblika i rubova na registarskoj oznaci, OCR sustav donosi zaključak o prisutnosti znakova na pločici, odnosno je li riječ o slovu 'A'. Najveći stupanj preciznosti postiže se u slučajevima gdje su znakovi ravnomjerno raspoređeni, jasno definirani i različiti, te su slične veličine. Međutim, izazovi se pojavljuju kad kamera bilježi registarsku oznaku pod određenim kutom ili kad su znakovi djelomično prekriveni ili oštećeni.

Jedan od glavnih izazova u primjeni OCR tehnike leži u poteškoćama u razlikovanju znakova koji su slični, na primjer, slova 'O' i 'Q', broja '0' i slova 'I', te slova 'B' i broja '8'. Ovo svojstvo znatno komplicira automatsko prepoznavanje registarskih oznaka. Iako se temeljna istina na registarskim oznakama koje su uspješno prepoznate relativno lako može potvrditi, poteškoće se javljaju u slučajevima kada registarske oznake nisu prepoznate, prenapregnute ili nedetektirane, čime se potencijalno gubi korisna informacija.

Iz tih razloga, neki algoritmi za prepoznavanje registarskih oznaka implementiraju posebne strategije ekvivalencije kako bi se smanjila tzv. "fuzzy" detekcija, odnosno slučajevi djelomičnih podudaranja. Međutim, takvi prilagođeni pristupi često rezultiraju povećanom stopom lažno pozitivnih identifikacija, što može biti problem u kontekstu sigurnosti i upravljanja parkiralištima. Na primjer, vozilima s ekvivalentnim registarskim oznakama može se neopravdano omogućiti pristup područjima koja im nisu namijenjena.

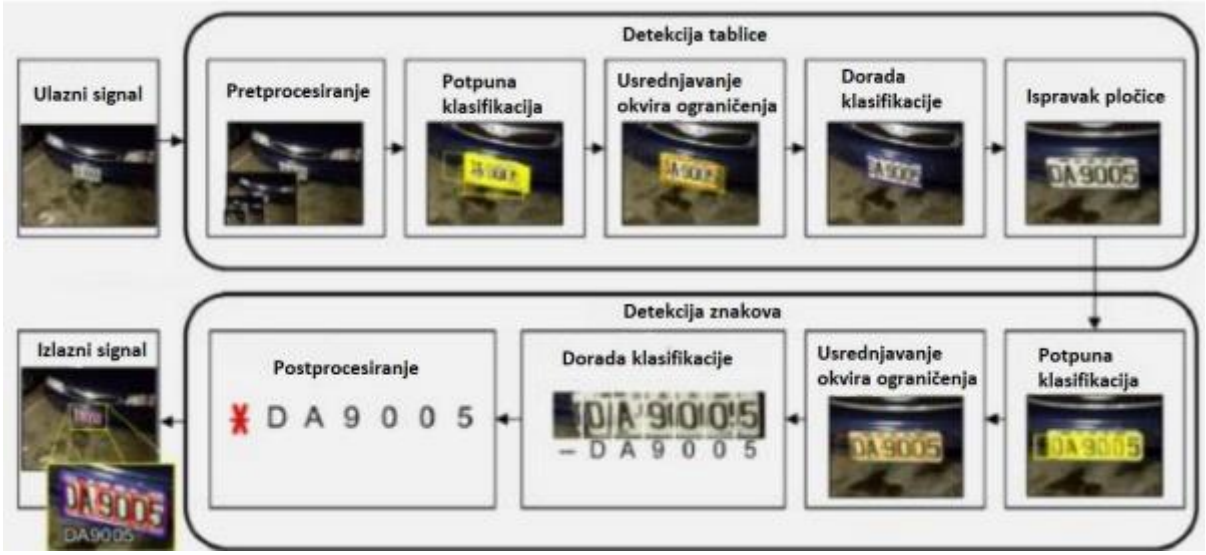
Zahtjevi za prepoznavanje registarskih oznaka u pogledu gustoće piksela variraju znatno, ali često zahtijevaju 30-90 piksela po metru, što je znatno više u usporedbi s detekcijom osoba ili vozila.

Proizvođači obično preciziraju te zahtjeve u pikselima temeljenim na visini ili širini registarskih oznaka i/ili pojedinačnih znakova. Veličina registarskih oznaka i brzina vozila značajno utječu na pikselne zahtjeve.

Tehnologija za prepoznavanje registarskih oznaka (LPR) zadnjih je nekoliko godina doživjela značajan napredak. Dok se ranije oslanjala isključivo na tehnike optičkog prepoznavanja znakova, danas su se razvili napredniji pristupi temeljeni na dubokom učenju. Uobičajena praksa sada je kombinacija različitih tehnika, uključujući klasične metode strojnog učenja i duboko učenje zajedno s optičkim prepoznavanjem znakova (OCR).

Sustavi koji se oslanjaju isključivo na duboko učenje koriste specijalno obučene neuronske mreže za obavljanje zadataka LPR-a. S druge strane, hibridni algoritmi koriste duboko učenje za identifikaciju registarskih oznaka, prilagodbu njihova položaja prema kutu i osvjetljenju, a zatim koriste OCR tehnologiju za precizno čitanje znakova.

Ovoj naprednoj metodi detekcije registarskih oznaka pomoću neuronske mreže dan je praktičan primjer na slici 4.2. Ovaj pristup omogućava visoku točnost i učinkovitost u prepoznavanju registarskih oznaka vozila.



Slika 4.2. Proces detekcije tablice putem dubokog učenja [64]

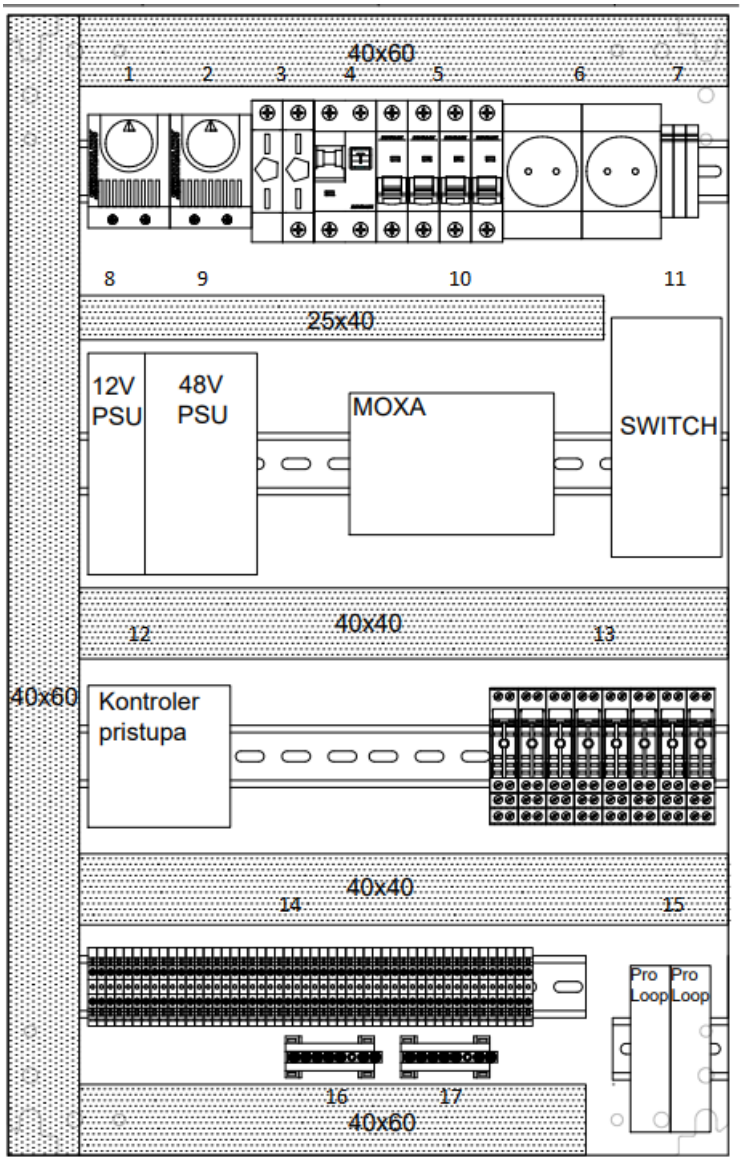
Duboko učenje predstavlja napredniju metodu koja pruža veću preciznost i otpornost na različite izazove, uključujući mrlje, prljavštinu, varijacije u osvjetljenju te različite kuteve gledanja. Ova tehnika omogućava vrhunsku učinkovitost u prepoznavanju registarskih oznaka vozila. Međutim, važno je napomenuti da je uporaba dubokog učenja zahtjevnija i skuplja u usporedbi s klasičnim optičkim prepoznavanjem znakova (OCR).

Treniranje sustava za prepoznavanje registarskih oznaka (LPR) pomoću dubokog učenja zahtijeva specifične skupove podataka s registarskim oznakama vozila. U mnogim zemljama, ovi skupovi podataka zahtijevaju kontinuirano ažuriranje i održavanje, što može predstavljati izazov prilikom treniranja i primjene takvih sustava.

Kada je riječ o brzini kadrova, za LPR sustave iznimno je važno postići visoku brzinu prikazivanja s minimalno 25 kadrova u sekundi kako bi se učinkovito očitavale registarske oznake vozila u pokretu. U usporedbi s drugim vrstama tehnologija, LPR je dokazano zrelija tehnika koja se koristi već mnogo godina i široko se primjenjuje u kontekstima kao što su provođenje zakona, upravljanje parkiralištima te osiguranje na cestama i granicama. [64]

4.2. Opis elemenata korištenih u električnom ormaru

Na slici 4.3. vidimo shemu električnog ormara.



Slika 4.3. Shema električnog ormara [Izrada autora]

Pod brojevi 1 i 2 na slici 4.3. vidimo termostate. Oni služe za nadziranje temperature. Kada se temperatura spusti ispod neke zadane vrijednosti šalju signal koji potom uključuju grijač, zadužen za grijanje samog električnog ormara. Također ako temperatura naraste iznad neke zadane vrijednosti, drugi termostat šalje signal koji uključuje ventilator zadužen za hlađenje električnog ormara.

Slika 4.4. Termostat [65]

Ispod broja 3 na slici 4.3. nalazi se prenaponska zaštita. Prenaponska zaštita štiti niže naponske krugove od oštećenja uslijed porasta napona iznad nazivne vrijednosti, odnosno prati vrijednost napona iz vanjskog izvora napajanja. Sami prenaponi mogu nastati na razne načine, a najopasniji su oni od udara groma. Stoga je potrebno zaštiti elektroničku opremu u tim slučajevima. Najjednostavniji način izvedbe prenaponske zaštite je s pomoću Zenerove diode. [67]

Slika 4.5. Prenaponska zaštita [66]

Ispod broja 4 na slici 4.3. nalazi se FID sklopka (eng. RCS – residual current device), koja je jedna od glavnih zaštita za ljude, ali i općenito od kratkog spoja. FID sklopka radi na principu da mjeri ravnotežu struje koja uđe i izađe kroz nju. Ako razlika struje na ulazu i izlazu iz FID sklopke nije unutar zadane vrijednosti, onda on prekida napajanje. [68]

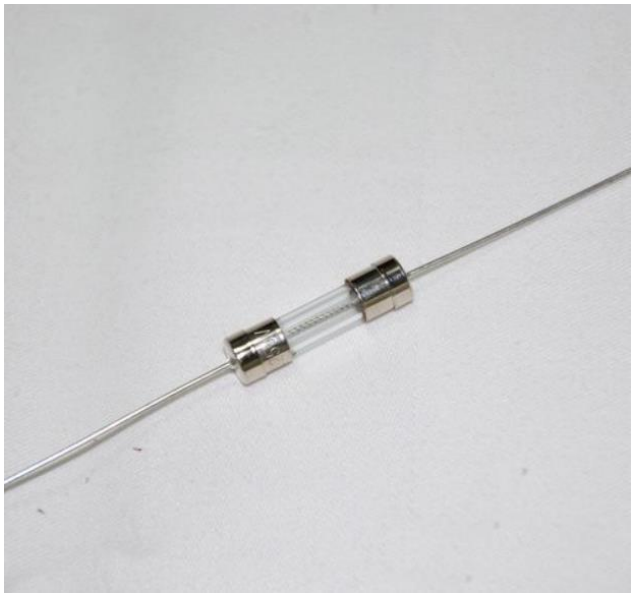
Slika 4.6. FID SKLOPKA [69]

Ispod broja 5 na slici 4.3. nalaze se osigurači. Osigurači su električni uređaji koji štite ostale električne uređaje u slučajevima prevelikog strujnog opterećenja. Kada dođe do takvog slučaja, osigurač prekida strujni krug. Danas općenito, i u ovom projektu koristit će se automatski osigurač, koji koristi elektromagnet koji isključuje ugrađenu sklopku kada struja pređe nazivnu vrijednost osigurača. Nakon ispadanja osigurača, potrebno je vratiti polugu na osiguraču u prvotni položaj, čime se sklopka ponovno uključuje. [70]

Slika 4.7. Osigurač [71]

Ispod broja 6 na slici 4.3. nalaze se utičnice za dodatne električne uređaje, kao na primjer za napajanje prijenosnog računala za vrijeme podešavanja kontrole pristupa ili žarulje.

Ispod broja 7 na slici 4.3. nalaze se stakleni osigurači. Za razliku od prije spomenutih osigurača, ovi se koriste za zaštitu točno određenog uređaja, te kada prevelika struja prođe kroz njega dolazi do pucanja istog, te ga je potrebno zamijeniti. [72]



Slika 4.8. Stakleni osigurač [72]

Ispod broja 8 na slici 4.3. nalazi se napajanje koje služi za pretvorbu izmjenične električne energije napona 230 V u istosmjernu električnu energiju napona 12 V.

Slika 4.9. Napajanje napona 12 V [73]

Ispod broja 9 na slici 4.3.nalazi se napajanje koje služi za pretvorbu izmjenične električne energije napona 230 V u istosmjernu električnu energiju napona 48 V.

Slika 4.10. Napajanje napona 48 V [74]

Ispod broja 10 na slici 4.3. nalazi se ulazno/izlazni uređaj koji služi za skupljanje podataka sa uređaja koji su spojeni na ulaze i upravljanje uređajima koji su spojeni na izlaze.

Slika 4.11. Ulazno/izlazni uređaj [75]

Ispod broja 11 na slici 4.3. nalazi se mrežni preklopnik koji služi za spajanje vanjskih uređaja, kao što su kamere putem TCP/IP protokola.

Slika 4.12. Mrežni preklopnik [76]

Ispod broja 12 na slici 4.3. nalazi se kontroler pristupa, koji je već viđen u radu na slici 2.11.

Ispod broja 13 na slici 4.3 nalaze se releji. Relej je električni upravljan prekidač, koji se aktivira strujom, odnosno signalom jednog električnog kruga, kako bi uklopio ili isklopio drugi električni krug. Relej koji koristi elektromagnet naziva se elektromagnetski relej, a u našem slučaju obavlja ulogu električnog prekidača. [77]

Slika 4.13. Relej za din šinu [78]

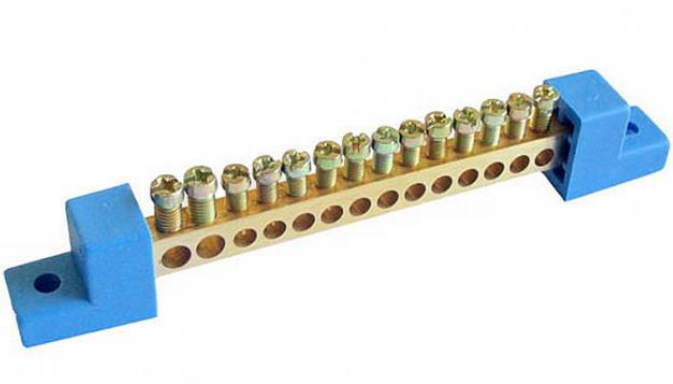
Ispod broja 14 na slici 4.3. nalaze se stezaljke.

Slika 4.14 Stezaljke [79]

Ispod broja 15 na slici 4.3. nalazi se kontroler petlje. Jedan kontroler petlje predstavlja najavnu a drugi odjavnu petlju. Sam kontroler petlje radi na način da prepoznaje promjenu u induktivitetu zavojnice, koja se nalazi zakopana ispod asfalta, kada iznad nje dođe vozilo. U slučaju najavne petlje, najavni kontroler petlje detektira kada je vozilo došlo na poziciju za snimanje registarske oznake vozila, a u slučaju odjavne petlje detektira kada je vozilo prošlo rampu, te istu može spustiti.

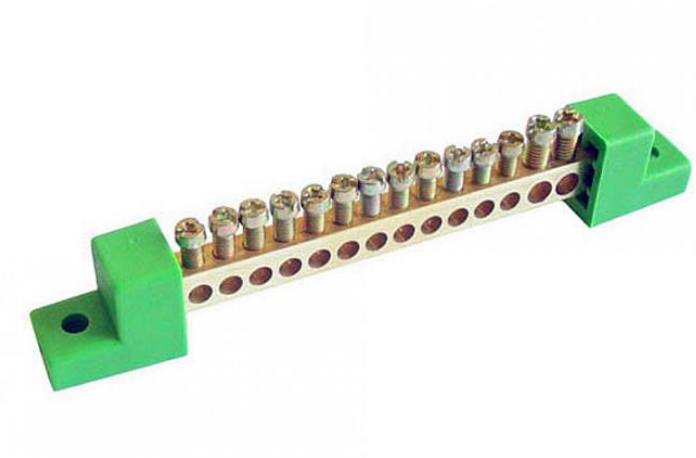
Slika 4.15 Kontroler petlje [80]

Iznad broja 16 na slici 4.3. nalazi se sabirnica za nulu faze.



Slika 4.16. Sabirnice nule faze [81]

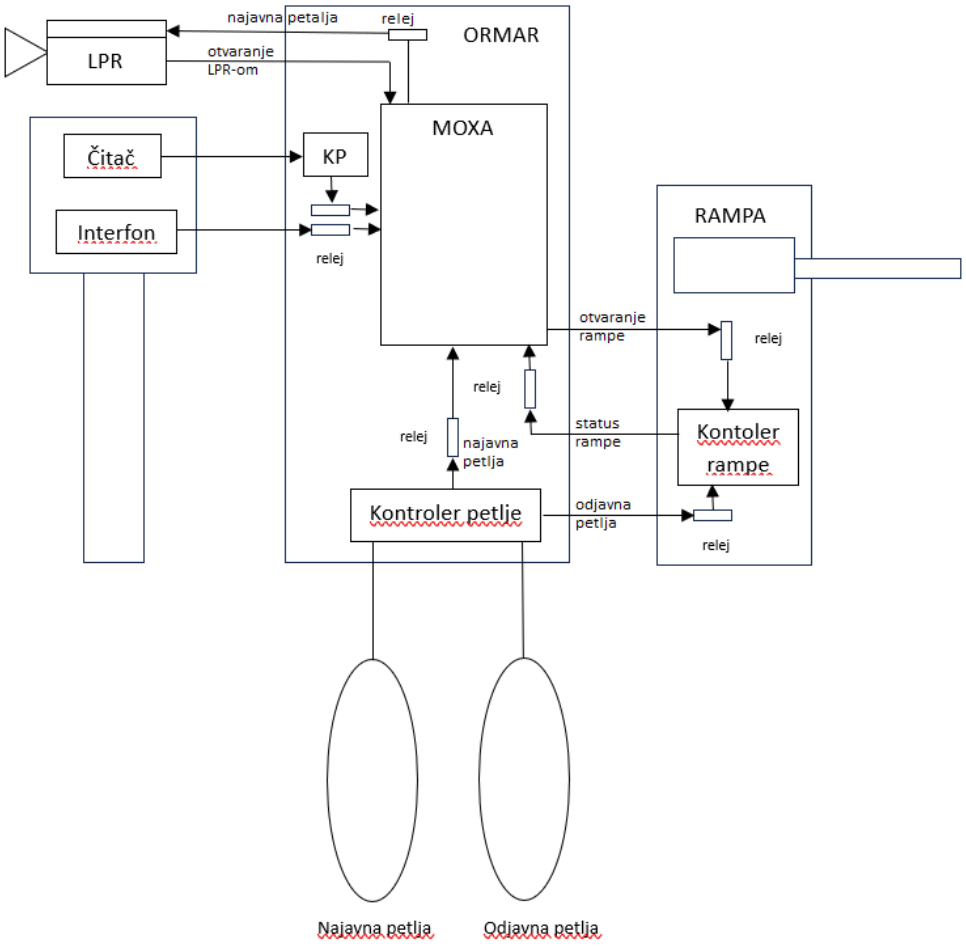
Iznad broja 17 na slici 4.3. nalazi se sabirnica za uzemljenje.



Slika 4.17 Sabirnica uzemljenja [82]

4.3. Idejno rješenje projekta

Na slici 4.18 prikazana je shema koja će služiti kao idejno rješenje i prema kojoj će se projekt realizirati.



Slika 4.18. Idejno rješenje [Izrada autora]

Ideja ovog rješenja je da vozilo dođe iznad najavne petlje. Dolaskom metalnog objekta, odnosno vozila, iznad najavne petlje, dolazi do promjene u induktivitetu same petlje, te kontroler petlje detektira tu promjenu. Šalje signal na na relej, koji taj signal prosljeđuje na ulazno/izlazni. Ona šalje signal za slikanje LPR kameri. Nakon slikanje registarske oznake vozila, LPR kamera šalje podatke o registraciji korisničkom računalu na kojem se nalazi softver za kontrolu pristupa. Softver tada pretražuje ako postoji podudaranje tablice u bazi podataka. Ukoliko bude podudaranja i tablica vozila se nalazi u bazi podataka kojima je dopušten pristup, softver šalje signal za otvaranje na ulazno/izlazni uređaj, koja taj signal prosljeđuje na relej kontrolera rampe, te relej šalje signal za podizanje na rampu. Vozilo prolazi rampu, te dolazi na odjavnu petlju. Kada vozilo dođe iznad odjavne petlje, dolazi do promjene induktiviteta u odjavnoj petlji, te kontroler petlje detektira tu

promjenu. U tom trenutku kontroler petlje šalje odjavni signal, odnosno signal za zatvaranje, na relej kontrolera rampe, te se rampa spušta.

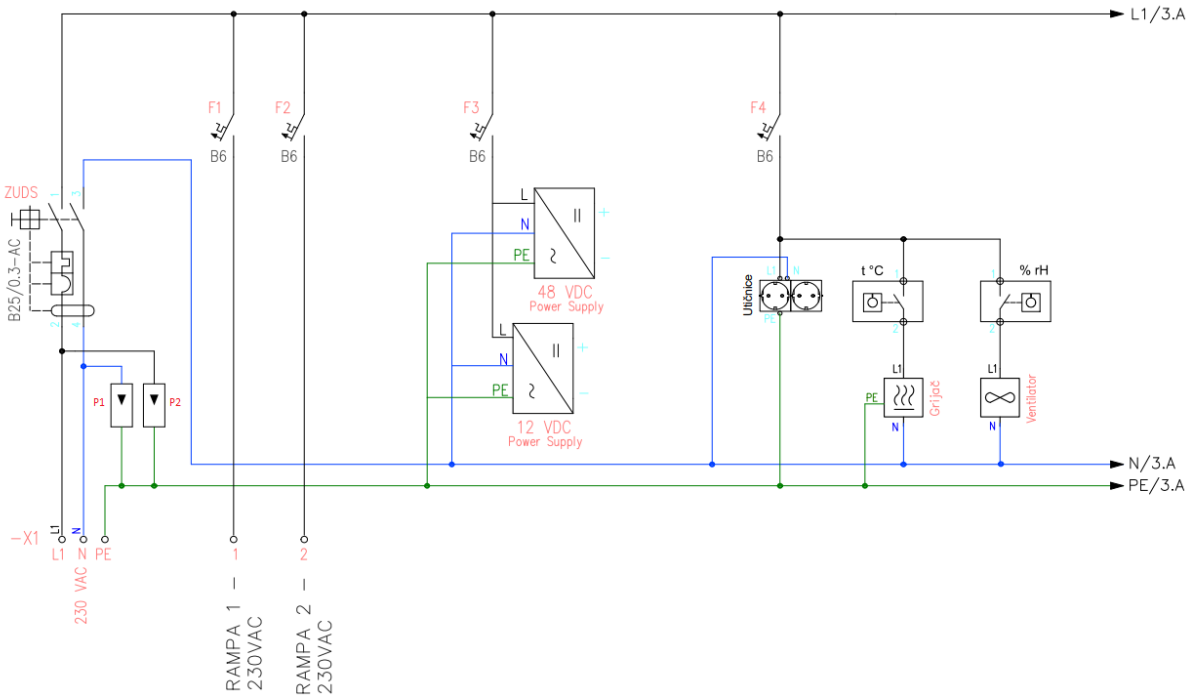
Osim dizanja rampe pomoću LPR-a, rampu je moguće podignuti i pristupnom karticom i pomoću portafona, te tada ulazak mora odobriti ovlaštena osoba sa sigurne strane. Ako LPR kamera ne pronađe registarsku oznaku vozila u svojoj bazi podataka, neće poslati ni signal za otvaranje. Kada se to dogodi moguće je podići rampu uz pomoć kartice. Čitač kartice očitava podatke sa kartice, te ih šalje pomoću Wiegand protokola na kontroler pristupa smješten unutar električnog ormara. Ukoliko kontroler pristupa prepozna karticu kao onu kojoj je dopušten prolazak, šalje signal na relej, koji taj signal prosljeđuje ulazno/izlaznom uređaju. Ulazno/izlazni uređaj taj signal dalje šalje na relej kontrolera rampe, koji će rampu podignuti. Kada vozilo dođe iznad odjavne petlje, kontroler petlje detektira promjenu induktiviteta u odjavnoj petlji, te šalje signal na relej kontrolera rampe, koji će rampu i spustiti.

Treći oblik ulaska na danom sustavu je pomoću portafona kojim se poziva ovlaštena osoba na sigurnoj rampe. Ako ovlaštena osoba dozvoli ulazak, pritiskom na gump, bilo virtualni ili fizički, šalje signal na portafon, koji taj signal prosljeđuje na relej, te ga dalje šalje na ulazno/izlazni uređaj. Ulazno/izlazni uređaj signal šalje na relej kontrolera rampe, koji potom podiže rampu. Kada vozilo dođe na odjavnu petlju, kontroler petlje detektira promjenu induktiviteta na odjavnoj petlji te preko releja kontrolera rampe šalje signal za spuštanje rampe. Rampa se nakon toga spušta.

Bitno je napomenuti da u našem slučaju imamo dvije rampe, jednu za ulaz u ograđeni prostor, drugu za izlaz iz ograđenog prostora, što znači da u sustavu imamo dva portafona, dvije LPR kamere, dvije rampe i dva čitača kartica, što će biti prikazano prikazano u nastavku rada.

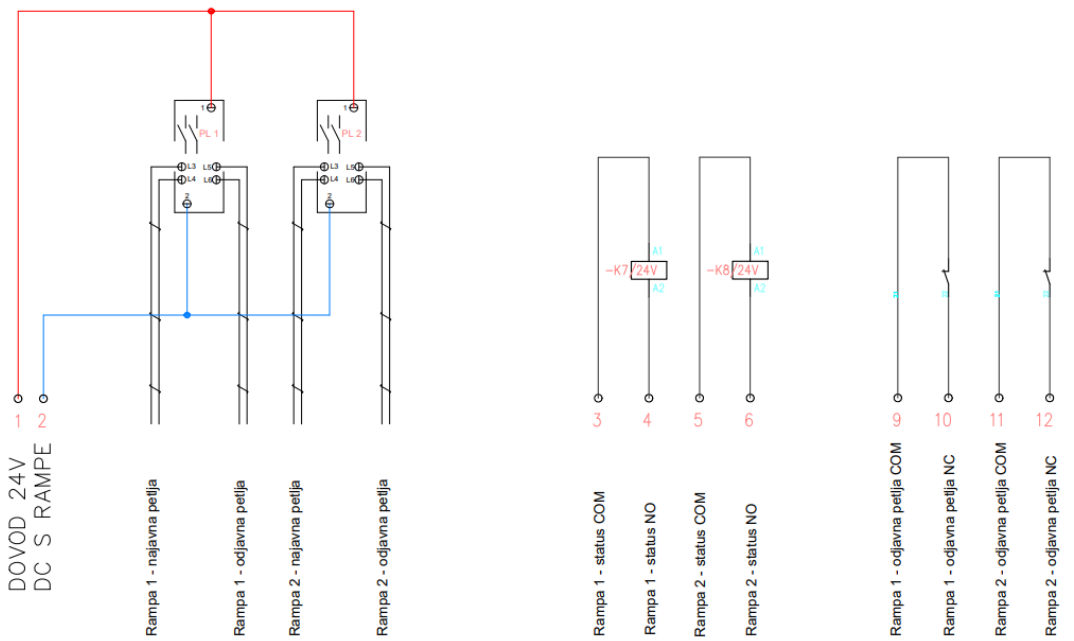
4.4. Izrada projekta

U programskom paket AutoCad radimo nacrt samog električnog ormara. Na slici 4.19. vidimo dovod faze L1 izmjeničnog napona 230V, nule faze N, i uzemljenja PE. Paralelno na fazu L1 i nulu faze N spajaju se prenaponske zaštite P1 i P2, te se serijski spaja FID sklopka oznake ZUDS. Dalje po liniji faze L1 imamo F1 osigurač, čija linija služi za napajanje rampe 1, te osigurač F2 čija linija služi na napajanje rampe 2. Slijedi nam osigurač F3, na koji su međusobno paralelno spojeni izvori napajanja 48 VDC i 12 VDC. Na osigurač F4 paralelno su spojene utičnice i dva termostata. Na jedan termostat spojen je grijač, a na drugi ventilator.



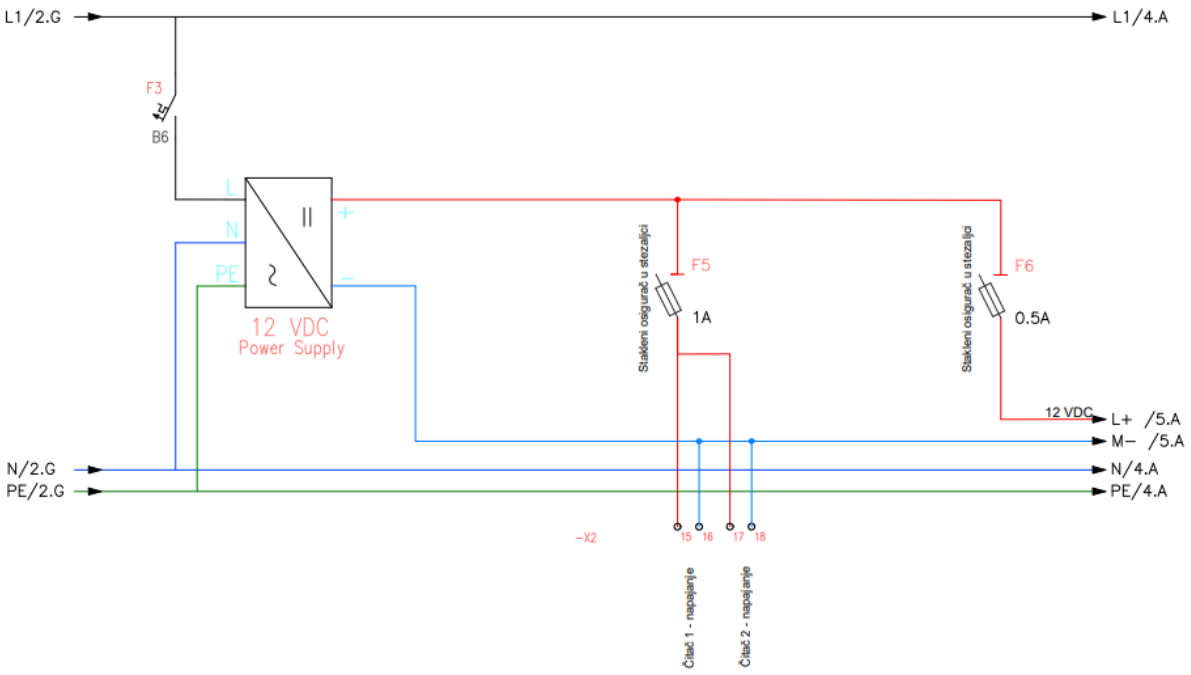
Slika 4.19. Shema glavnih elemenata [Izrada autora]

Na slici 4.20. vidimo kontrolere petlje rampe 1 i rampe 2 sa pripadajućim petljama. Kao što je pokazano na slici 4.19 na rampe odvodimo 230 VAC, no u rampi postoji napajanje koje na ulazu ima spomenutih 230 VAC, a na izlazu 24 VDC iz kojeg se napajaju elementi rampe. Kontroleri petlje jedini su elementi u elektroormaru koji zahtijevaju 24 VDC, pa spomenuti napon do elektroormara dovodimo pomoću žica sa rampi. Kontroler petlje uklapa 24VDC relej u elektroormaru koji šalje signal ulazno/izlaznom uređaju o statusu rampe (u obliku logičke nule ako je rampa spuštena, odnosno logičke jedinice ako je podignuta). Status rampe je informacija koja služi kako LPR kamera ne bi stalno slikala tablicu vozila. Relej odjavne petlje s kontrolera petlje prosljeđujemo na kontroler rampe kako bi pri prolasku vozila rampa otišla u spuštanje.



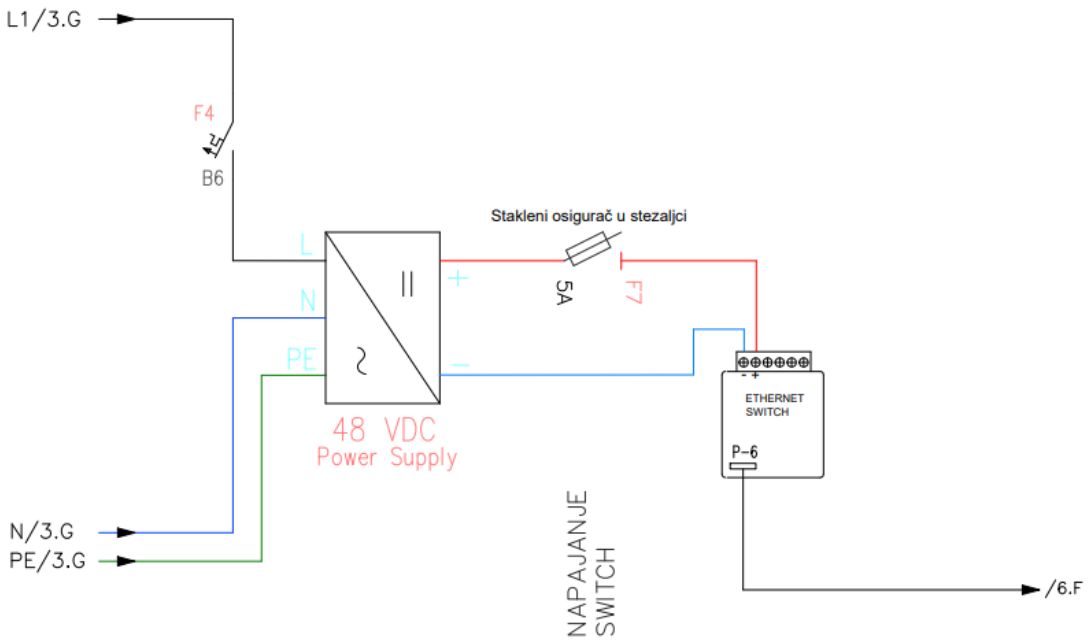
Slika 4.20. Spajanje kontrolera petlje [Izrada autora]

Na slici 4.21. vidimo kako je spojeno napajanje 12 VDC, te što se na njega spaja. Na ulazu u napajanje imamo izmjenični napon od 230 V, dok na izlazu imamo istosmjerni napon od 12 V. Preko osigurača F3 na fazi L1 spojeno je napajanje. Na napajanje je su spojena dva staklena osigurača. Na stakleni osigurač F5 spojena su dva čitača kartica, dok je na osigurač F6 spojen ulazno/izlazni uređaj. Točan način spajanja bit će naknadno objašnjen.



Slika 4.21. Shema spajanja napajanja 12 VDC [Izrada autora]

Na slici 4.22. vidimo kako je preko osigurača F4 na liniji L1 spojeno napajanje 48 VDC. Na ulazu u napajanje imamo izmjenični napon 230 V, dok na izlazu iz napajanja imamo istosmjerno napon 48 V. Na pozitivnu stezaljku izlaza napajanja spojen je stakleni osigurač koji vodi na pozitivnu stezaljku mrežnog preklopnika, dok je negativna stezaljka spojena direktno na negativnu stezaljku mrežnog preklopnika. Na mrežni preklopnik je spojena LPR kamera, te je mrežni preklopnik spojen u mrežu, kako bi preko mreže LPR kamera mogla poslati softveru podatke o skeniranoj tablici.

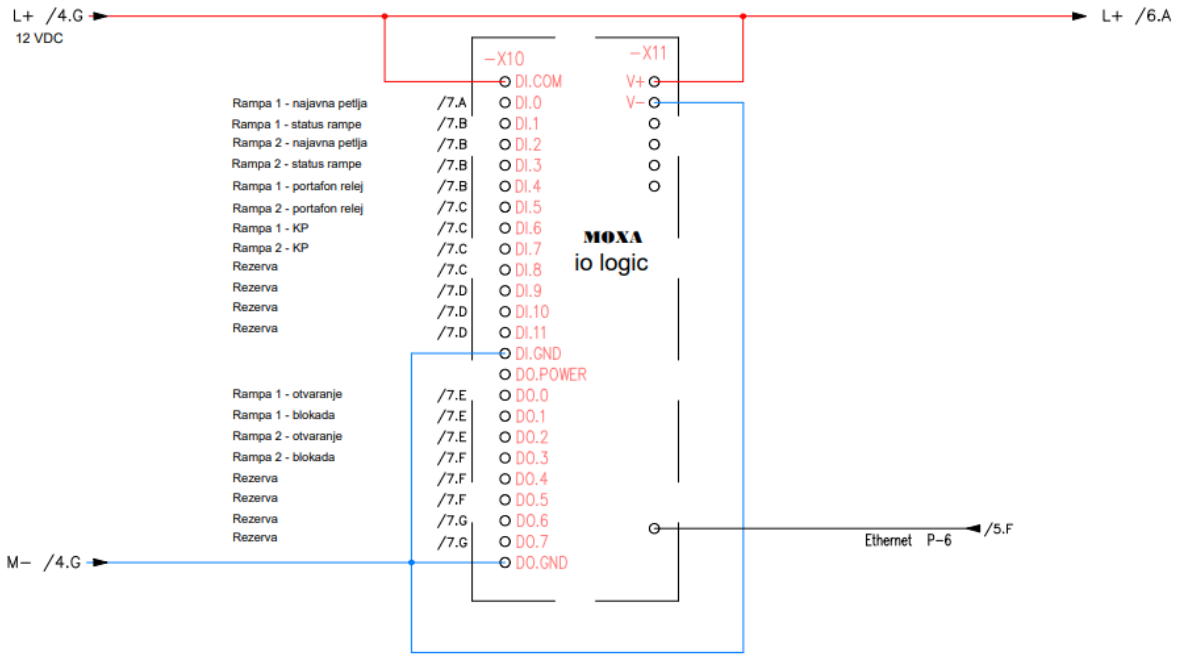


Slika 4.22. Shema spajanja napajanja 48 VDC [Izrada autora]

Na slici 4.23. nam je prikazan ulazno/izlazni uređaj, te način spajanja tog uređaja.

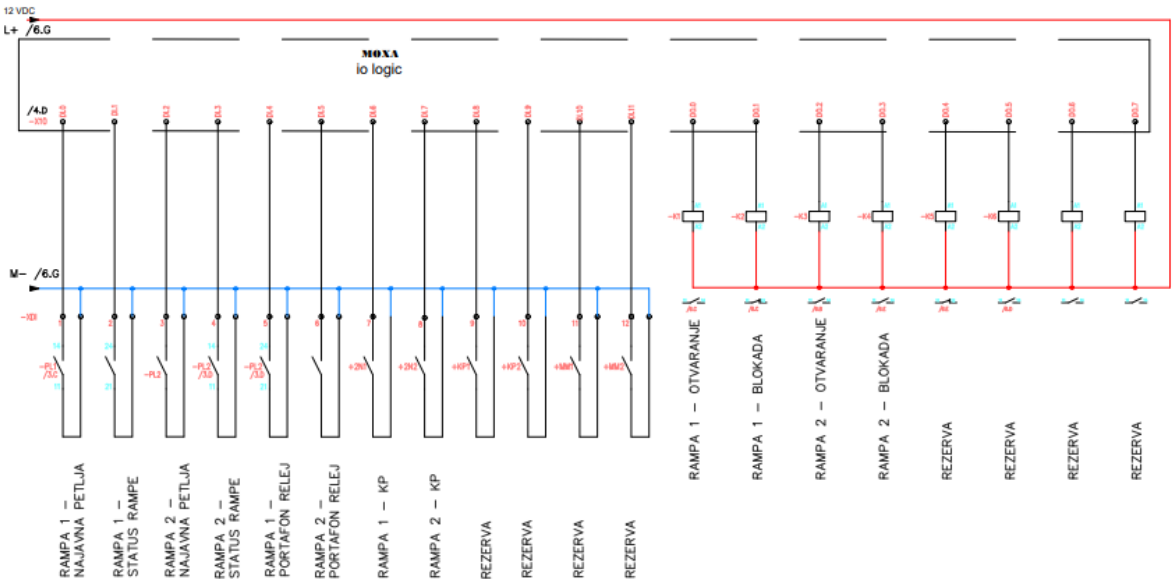
Na slici 4.23. je prikazano spajanje 12 VDC napajanja za ulazno/izlazni uređaj, te raspored ulaznih i izlaznih signala. Pozitivna stezaljka sa izvora napajanja 12 VDC spojena je na stezaljku DI.COM i V+ ulazno/izlaznog uređaja, dok je negativna stezaljka napajanja spojena na stezaljke DI.GND, D0.GND i V-. Ulazno/izlazni uređaj također je spojen na mrežni preklopnik, a samim time i u mrežu. Najavna petlja rampe 1 spojena je na stezaljku DI.0, status rampe 1 spojen je na stezaljku DI.1, najavna petlja rampe 2 spojena je na stezaljku DI.2, status rampe 2 spojen je na stezaljku DI.3, relej portafona 1 spojen je na stezaljku DI.4, relej portafona 2 spojen je na stezaljku DI.5, te je kontroler pristupa spojen na stezaljke DI.6 i DI.7, dok ostatak ulaznih stezaljki nije spojen. Izlaznom stezaljkom DO.0 šalje se signal za otvaranje rampe 1, izlaznom stezaljkom DO.1 šalje se signal za blokiranje rampe 1, stezaljkom DO.2 šalje se signal za otvaranje rampe 1, stezaljkom

DO.3 šalje se signal za blokiranje rampe 2. Signal za blokiranje služi za zadržavanje rampe u položaju u kojem je zatečena u tom trenutku.



Slika 4.23. Shema spajanja ulazno/izlaznog uređaja [Izrada autora]

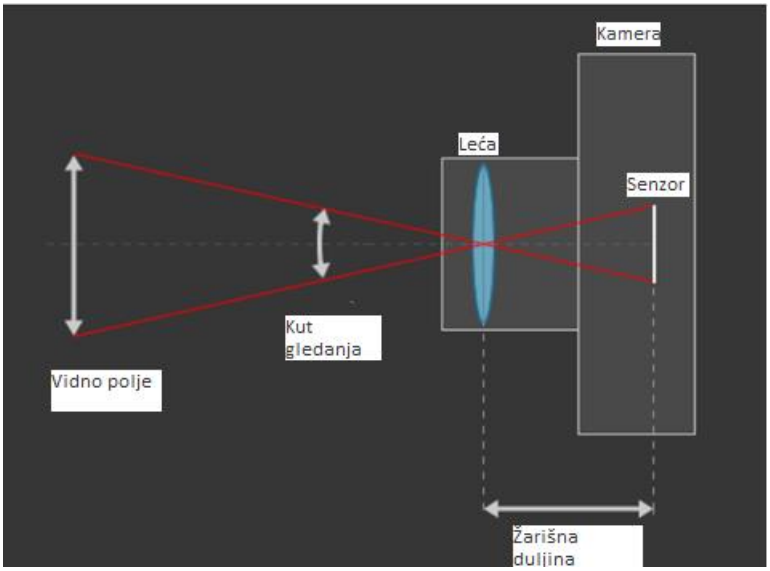
Bitno je napomenuti da periferni uređaji nisu direktno spojeni na ulazno/izlazni uređaj, već preko releja. Ulazno/izlazni uređaj ima svoje unutarnje krugove koji se zatvaraju kada dođe signal na neki od ulaza. Na slici 4.24. je prikazano kako su spojeni releji pojedinih perifernih uređaja.



Slika 4.24. Način spajanja releja na ulazno/izlazni uređaj [Izrada Autora]

4.5. Podešavanje LPR kamere

Žarišna duljina je duljina između leće i digitalnog senzora kamere kada je objekt snimanja u fokusu. Žarišna duljina izražava se u milimetrima (mm) i kod kamera se označava raspon (minimalna i maksimalna) žarišnih duljina koje se mogu postaviti, npr. Vivotek IB9387 f = 2.7 - 13.5mm, Vivotek FE9382 f = 1.245mm.



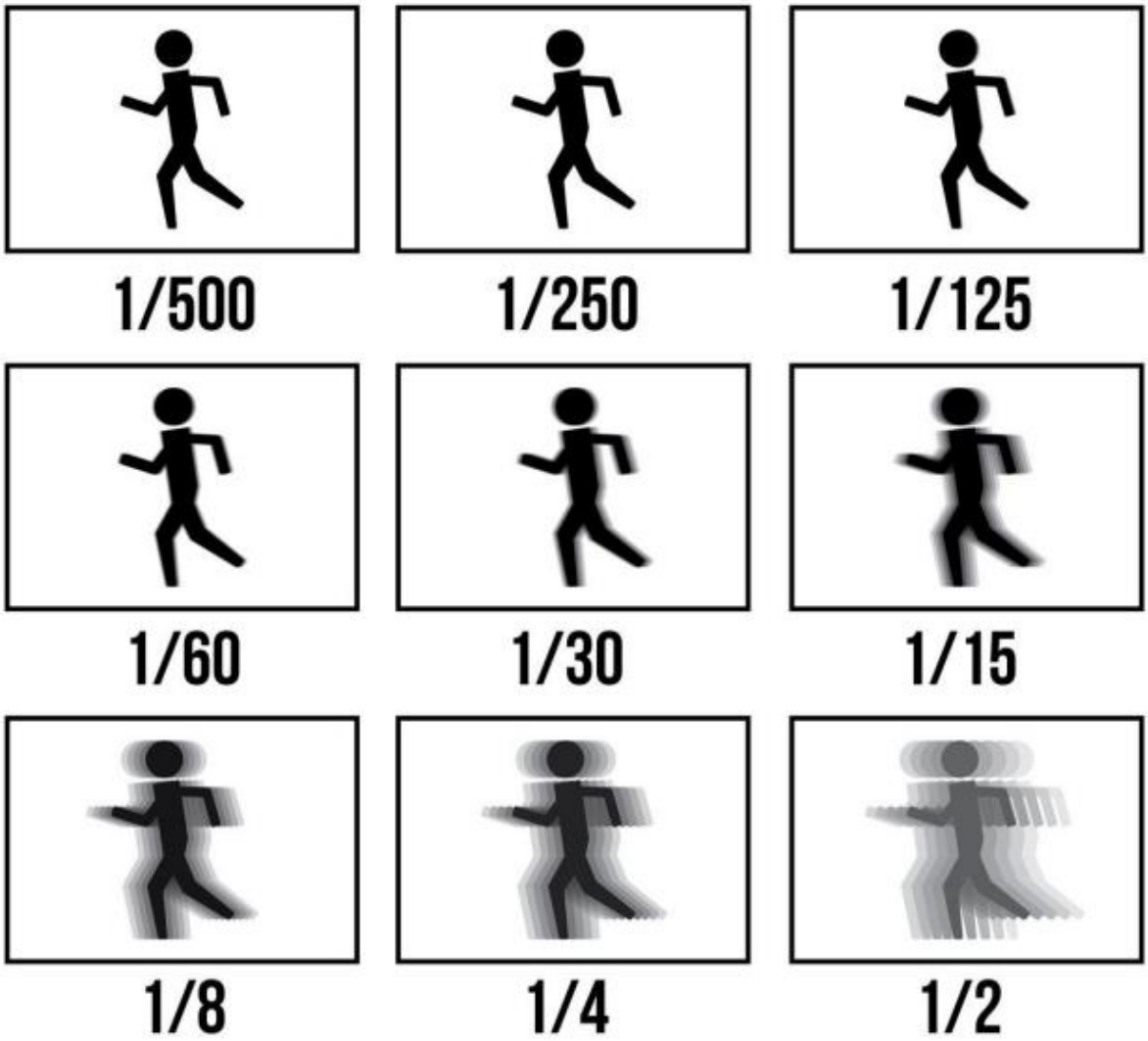
Slika 4.25. Žarišna duljina [83]

Žarišna duljina određuje kut gledanja , odnosno koliko scene će se obuhvatiti, i povećanje (eng. zoom). Što je žarišna duljina duža to je kut gledanja uži, a zoom veći, i obrnuto, što je žarišna duljina kraća to je kut gledanja širi, a zoom manji. [84]

Apertura je otvor kroz koji svjetlost upada u kameru. Veličinu otvora kontrolira blenda (iris). Ovisno o veličini otvora mijenja se dubina polja (eng. depth of field) i količina svjetlosti koja upada u kameru, tj. slika će biti svjetlija ili tamnija. Kod većeg otvora blende imamo svjetliju sliku i manju dubinu polja, a kod manjeg otvora imamo tamniju sliku i veću dubinu polja. [85]

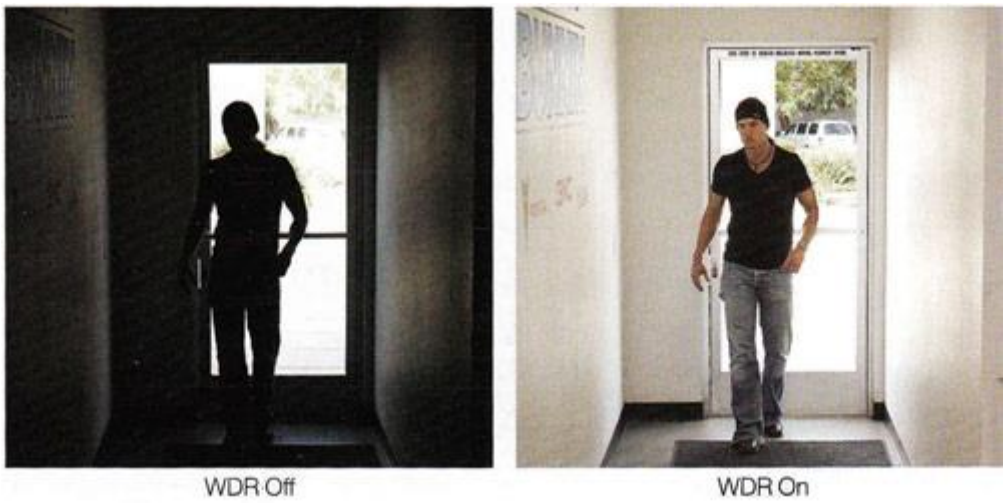
Slika 4.26. Apertura [86]

Vrijeme ekspozicije je vrijeme koje je senzor kamere izložen svjetlosti i mjeri se u sekundama (primjeri: 1, 1/2, 1/4, 1/125, 1/1000) . Kod veće brzine zatvarača, vrijeme izloženosti senzora svjetlu je manje, odnosno kod manje brzine zatvarača, vrijeme izloženosti je veće. Vrijeme ekspozicije nam je bitno kod predmeta u pokretu, manje vrijeme ekspozicije nam daje oštriju sliku predmeta u pokretu. [87]



Slika 4.27. Vrijeme ekspozicije [88]

WDR (eng. Wide Dynamic Range) tehnologija poboljšava kvalitetu slike pod kontrastnim svjetlosnim uvjetima gdje postoje slabo i jako osvjetljeni dijelovi u vidnom polju. WDR omogućuje kameri da jasno snimi i slabo i jako osvjetljeno područje tako da istovremeno snimi dvije do tri slike s različitim razinama ekspozicije te ih spoji u jednu sliku snimke. [89]



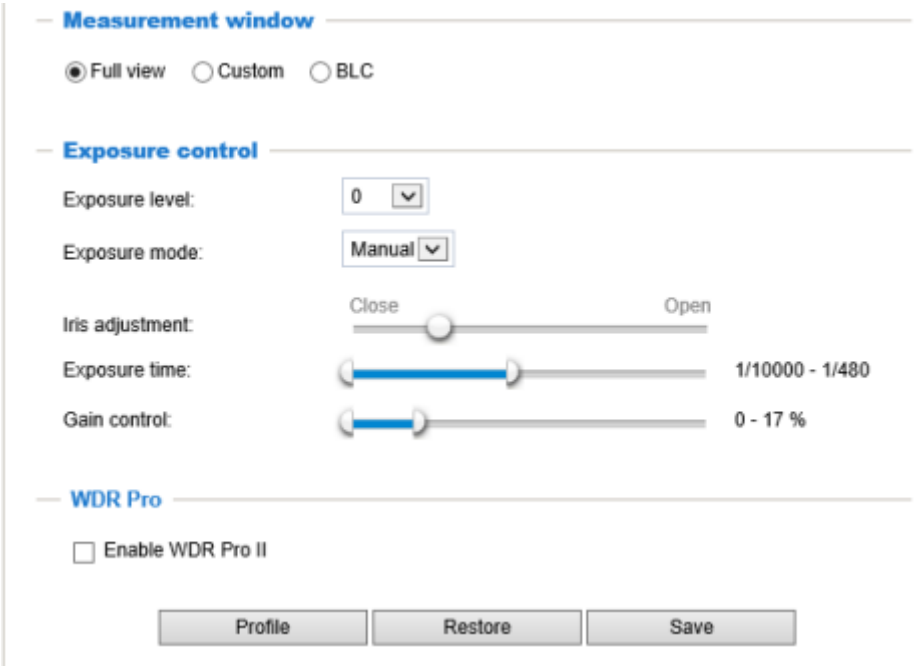
Slika 4.28. WDR [90]

Postavke kamere vrše se internet sučelju same kamere, te se na nju spajamo pomoću njene IP adrese.

U našem slučaju podešavamo kameru na način da je iris što više zatvoren kako bi dobili veću dubinu polja, odnosno imali više fokusiranog područja u kojem možemo očitati tablicu, te iris postavljamo na 20-40% otvorenosti.

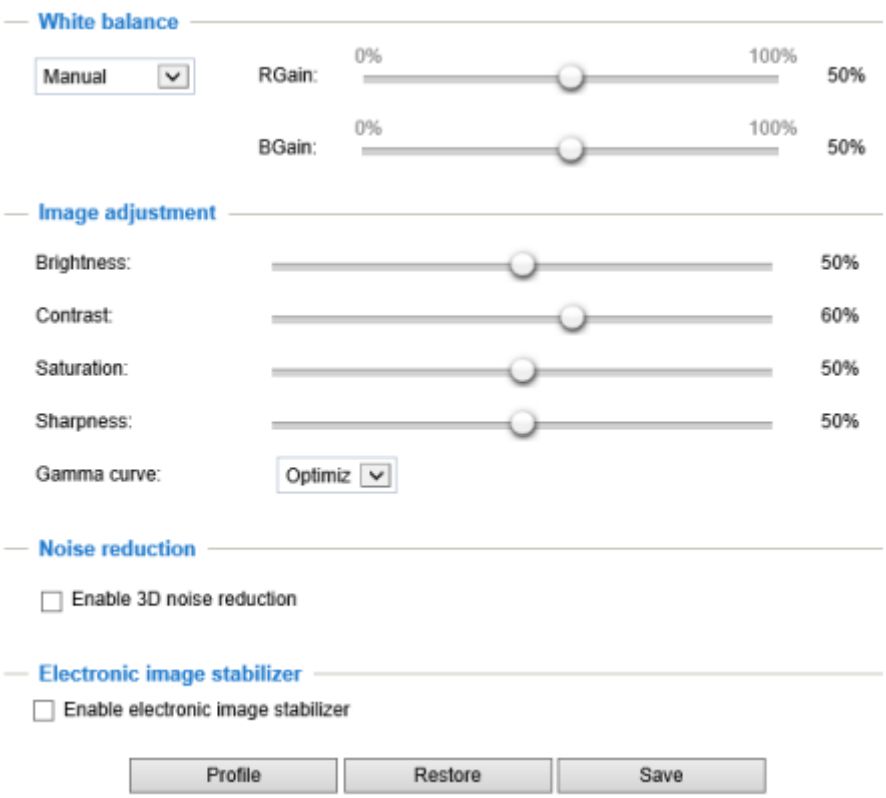
Vrijeme ekspozicije treba biti malo kako bi dobili što oštriju sliku vozila u pokretu. Ako se vozilo zaustavlja na rampi dovoljno je da vrijeme ekspozicije bude 1/250 s ili 1/500 s, a ako samo usporava bez zaustavljanja potrebno je da bude 1/1000 s ili čak manje.

Pojačanje povećava svjetlinu, ali dodaje šum slici koji može utjecati na čitanje tablice, te je u našem slučaju podešen na 17%. Primjer spomenutih postavki vidimo na slici 4.29.



Slika 4.29. Postavke vremena ekspozicije i pojačanja [Izrada Autora]

Kontrast slike potrebno je malo povećati, na otprilike 60%, kako bi se olakšalo čitanje tablice, dok svjetlinu (eng. brightness), zasićenost (eng. saturation) i oštrinu (eng. sharpness) ostavljamo na zadanoj vrijednosti od 50%, kao što je prikazano na slici 4.30.



Slika 4.30. Postavke svjetline, kontrasta, zasićenosti i oštrine [Izrada Autora]

WDR koji spaja dva ili više sličica u jednu, u slučaju kod čitanja tablica može rezultirati preklapajućim znakovima na tablicu, pa tu opciju isključujemo.

Također, poželjno je forsirati crnobijeli, odnosno noćni režim rada kamere tijekom cijelog dana, pošto nas pri očitanju tablica ne zanima boja.

Pri ugradnji LPR kamere treba voditi računa pod kojim kutom vozilo dolazi na mjesto očitanja. Preporučeni kutovi za optimalan rad LPR kamere su: vertikalni kut do 35°i horizontalni kut do 35°.

Na slici 4.31. vidimo kako to izgleda u softveru, te vidimo da se vozilo sa slike nalazi na popisu vozila kojem je dozvoljen pristup ograničenom području.

Slika 4.31. Prikaz u softveru [Izrada autora]

5. ZAKLJUČAK

Kontrola pristupa sigurnosni je koncept koji služi za upravljanje pristupom objektima, dobrima i informacijama. Na taj se način osigurava da samo ovlaštene osobe imaju pristup spomenutim objektima, dobrima i informacijama. Glavni cilj kontrole pristupa je zaštititi sustave, dobra i informacije od zloupotrebe, uništenja i oštećenja. Postavljanjem određenih pravila i ograničenja ograničavam tko i u kojim uvjetima može pristupiti dobrima, informacijama i sustavima.Razvoj kontrole pristupa bitan je za današnje društvo koje se sve češće susreće sa sigurnosnim problemima. Integracija sustava kontrole pristupa s drugim tehnologijama, kao što su videonadzor dovode do ostvarivanja punog potencijala takvih sustava. Ako je potrebna razina sigurnosti visoka koristit ćemo sigurnije metode, kao što su skeniranje mrežnice ili skeniranje rožnice. U takvim slučajevima često se koristi i dvofaktorska autentifikacija, odnosno uz jednu metodu autentifikacije koristi se i druga kako bi se povećala sigurnost. Za slučajeve gdje velika razina sigurnosti nije potrebna koristi se neka od manje sigurnih metoda. Na primjeru projekta koristi se više metoda autentifikacije, međutim nisu korištene kao dvofaktorska autentifikacija, već je potrebna jedna od ponuđenih metoda za pristup, što znači da za pristup ograđenom prostoru nije potrebna velika razina sigurnosti. Korištene metode pristupa u projektu su pristup uz pomoć LPR kamere, kartični pristup i pristup pozivanjem ovlaštene osobe putem portafona.

6. LITERATURA

[1] Stamp M.:"Information Security: Principles and Practice", 2005

[2] Ballad B., Ballad T., Banks E.: "Access Control, Authentication, and Public Key Infrastructure", 2010

[3] Dončević R.: "Uvod u kontrolu pristupa i evidenciju radnog vremena", 2007

[4] Internetska stranica (pristupljeno 15.08.2023): https://www.investopedia.com/terms/m/magnetic-stripe-card.asp

[5] Internetska stranica (pristupljeno 15.08.2023): https://www.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/

[6] Internetska stranica (pristupljeno 18.08.2023): https://thesecurepass.com/blog/magentic-strip-card-reader-access-control-system

[7] Internetska stranica (pristupljeno 18.08.2023): https://www.enciklopedija.hr/natuknica.aspx?id=68066

[8] Internetska stranica (pristupljeno 18.08.2023): https://thesecurepass.com/blog/magentic-strip-card-reader-access-control-system

[9] Internetska stranica (pristupljeno 18.08.2023): https://www.zebra.com/us/en/products/rfid/rfid-reader-antennas/an5x-an7x-series.html

[10] Internetska stranica (pristupljeno 18.08.2023): https://www.atlasrfidstore.com/zebra-technologies/

[11] Finkenzeller K.: " RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication", 2010

[12] Internetska stranica (pristupljeno 18.08.2023): https://www.indiamart.com/proddetail/active-uhf-rfid-tags-22301326891.html

[13] Sweeney II P.J.: "RFID For Dummies", 2005

[14] Internetska stranica (pristupljeno 22.08.2023): https://www.swiftlane.com/blog/mobile-access-control-readers/

[15] Internetska stranica (pristupljeno 22.08.2023): https://www.getkisi.com/guides/mobile-access-control-guide]

[16] Internetska stranica (pristupljeno 10.09.2023): https://dicsan.com/access_control/access_control_controller/

[17] Internetska stranica (pristupljeno 10.09.2023): IPVM [Access control book]

[18] Internetska stranica (pristupljeno 10.09.2023): https://kamir.hr/populus-p-4-b

[19] Internetska stranica (pristupljeno 10.09.2023: https://www.zudsec.com/products/Standalone_Access_Controller_Touch_Panel_242.html

[20] Internetska stranica (pristupljeno 15.09.2023): https://ipc2u.com/articles/knowledge-base/the-main-differences-between-rs-232-rs-422-and-rs-485/

[21] Internetska stranica (pristupljeno 15.09.2023): https://www.cuidevices.com/blog/rs-485-serial-interface-explained

[22] Internetska stranica (pristupljeno 15.09.2023: https://en.wikipedia.org/wiki/Wiegand_effect

[23] Internetska stranica (pristupljeno 15.09.2023): https://en.wikipedia.org/wiki/Wiegand_interface

[24] Internetska stranica (pristupljeno 15.09.2023): https://www.s4a-access.com/wiegand-reader-access-rfid-card-reader-e-h-mifare_p371.html

[25] Internetska stranica (pristupljeno 15.09.2023): https://getsafeandsound.com/blog/26-bit-wiegand-format/

[26] Internetska stranica (pristupljeno 15.09.2023): https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/

[27] Internetska stranica (pristupljeno 15.09.2023): https://www.techtarget.com/searchnetworking/definition/TCP-IP

[28] Internetska stranica (pristupljeno 15.09.2023): https://www.avast.com/c-what-is-tcp-ip

[29] Internetska stranica (pristupljeno 15.09.2023): https://www.geeksforgeeks.org/tcp-ip-model/

[30] Internetska stranica (pristupljeno 18.09.2023): https://ipvm.com/reports/door-pos-tut

[31] Internetska stranica (pristupljeno 18.09.2023): https://blog.midches.com/blog/what-is-a-request-to-exit-rex-sensor-bosch-ds150i-and-ds160-overview

[32] Internetska stranica (pristupljeno 18.09.2023): https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[33] Internetska stranica (pristupljeno 18.09.2023): https://www.kaspersky.com/resource-center/definitions/biometrics

[34] Internetska stranica (pristupljeno 18.09.2023): https://en.wikipedia.org/wiki/Facial_recognition_system#Anti-facial_recognition_systems

[35] Internetska stranica (pristupljeno 18.09.2023): https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition

[36] Internetska stranica (pristupljeno 18.09.2023): https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition

[37] Internetska stranica (pristupljeno 18.09.2023): https://www.swiftlane.com/blog/face-recognition-door-access-control/

[38] Internetska stranica (pristupljeno 25.09.2023): https://www.interpol.int/How-we-work/Forensics/Fingerprints

[39] Internetska stranica (pristupljeno 25.09.2023): https://www.researchgate.net/figure/Basic-fingerprint-patterns-a-the-arch-is-the-simplest-of-all-the-configurations-b_fig1_11673949

[40] Internetska stranica (pristupljeno 25.09.2023): https://www.nec.co.nz/market-leadership/publications-media/advantages-and-disadvantages-of-fingerprint-recognition/

[41] Internetska stranica (pristupljeno 25.09.2023): https://almas-industries.com/blog/advantages-and-disadvantages-of-a-fingerprint-scanner/

[42] Internetska stranica (pristupljeno 25.09.2023): https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

[43] Internetska stranica (pristupljeno 25.09.2023): https://www.arrow.com/en/research-and-events/articles/how-fingerprint-sensors-work

[44] Internetska stranica (pristupljeno 25.09.2023): https://www.aratek.co/news/the-4-fingerprint-sensor-types

[45] Internetska stranica (pristupljeno 25.09.2023): https://www.trustedreviews.com/explainer/what-is-an-ultrasonic-fingerprint-sensor-4241284

[46] Internetska stranica (pristupljeno 25.09.2023): https://en.wikipedia.org/wiki/Hand_geometry

[47] Internetska stranica (pristupljeno 25.09.2023): https://www.bayometric.com/hand-geometry-recognition-biometrics/

[48] Internetska stranica (pristupljeno 25.09.2023): https://www.biometricsinstitute.org/types-of-biometrics-hand-geometry/

[49] Internetska stranica (pristupljeno 25.09.2023): https://en.wikipedia.org/wiki/Iris_recognition

[50] Internetska stranica (pristupljeno 05.10.2023): https://www.britannica.com/science/iris-eye

[51] Internetska stranica (pristupljeno 05.10.2023): https://www.mojeoko.hr/savjeti-za-zdrave-oci/njega-oka/gradja-oka

[52] Internetska stranica (pristupljeno 05.10.2023): https://www.eff.org/pages/iris-recognition

[53] Internetska stranica (pristupljeno 05.10.2023): https://www.mantratec.com/products/Integrated-IRIS-Devices

[54] Internetska stranica (pristupljeno 05.10.2023): https://www.nec.com/en/global/solutions/biometrics/iris/index.html

[55] Internetska stranica (pristupljeno 05.10.2023): https://www.britannica.com/science/retina

[56] Internetska stranica (pristupljeno 05.10.2023): https://en.wikipedia.org/wiki/Retinal_scan

[57] Internetska stranica (pristupljeno 05.10.2023): https://www.rootstrap.com/blog/retinal-recognition-the-ultimate-biometric

[58] Internetska stranica (pristupljeno 05.10.2023): https://www.rightpatient.com/biometric-patient-identification-system-custom-reference-and-resource-center-iris-vs-retina/

[59] Internetska stranica (pristupljeno 05.10.2023): https://platform.keesingtechnologies.com/retinal-recognition-pros-and-cons/

[60] Internetska stranica (pristupljeno 10.10.2023): http://newt.phys.unsw.edu.au/jw/voice.html

[61] Internetska stranica (pristupljeno 10.10.2023): https://www.plumvoice.com/resources/blog/voice-biometrics/

[62] Internetska stranica (pristupljeno 10.10.2023): https://www.phonexia.com/knowledge-base/voice-biometrics-essential-guide/

[63] Internetska stranica (pristupljeno 10.10.2023): https://www.phonexia.com/knowledge-base/voice-biometrics-essential-guide/

[64] IPVM: "2023 Video Analytics"

[65] Internetska stranica (pristupljeno 10.10.2023): https://www.schrack.hr/trgovina/termostat-za-ventilator-1-radni-kontakt-plavi-iuk08566.html

[66] Internetska stranica (pristupljeno 10.10.2023): https://www.schrack.hr/trgovina/odvodnik-prenapona-klase-c-tt-tn-s-255v-20ka-set-is111310.html

[67] Internetska stranica (pristupljeno 10.10.2023): https://www.sunpower-uk.com/glossary/what-is-over-voltage-protection/

[68] Internetska stranica (pristupljeno 10.10.2023): https://www.automatika.rs/baza-znanja/obrada-signala/fid-sklopka-zastitni-uredaj-diferencijalne-struje.html

[69] Internetska stranica (pristupljeno 10.10.2023): https://elcon.hr/fid-sklopka/

[70] Internetska stranica (pristupljeno 10.10.2023): https://hr.wikipedia.org/wiki/Osigura%C4%8D

[71] Internetska stranica (pristupljeno 15.10.2023): https://www.elektromaterijal.hr/osigurac-ex9bn-1p-b25-6ka-100010-noark/58765/product/

[72] Internetska stranica (pristupljeno 15.10.2023): https://www.quarktwin.com/blogs/fuse/glass-tube-fuses-role-and-main-parameters?id=170

[73] Internetska stranica (pristupljeno 15.10.2023): https://www.damencnc.com/en/ndr-120-12-12vdc-120w-din-rail-powersupply/a2338

[74] Internetska stranica (pristupljeno 15.10.2023): https://in.element14.com/mean-well/ndr-240-48/power-supply-ac-dc-48v-5a/dp/2815651

[75] Internetska stranica (pristupljeno 15.10.2023): https://www.moxa.com/en/products/industrial-edge-connectivity/controllers-and-ios/universal-controllers-and-i-os/iologik-e2200-series

[76] Internetska stranica (pristupljeno 15.10.2023): https://www.edimax.com/edimax/merchandise/merchandise_detail/data/edimax/global/smb_switches_industrial/igs-1005/

[77] Internetska stranica (pristupljeno 15.10.2023): https://en.wikipedia.org/wiki/Relay

[78] Internetska stranica (pristupljeno 15.10.2023): https://www.switchtec.com/ProductGrp/din-rail-mount-electrical-latching-relay

[79] Internetska stranica (pristupljeno 15.10.2023): https://www.elektromaterijal.hr/stezaljka-redna-10-zelena-cts-10-un-gn/61012/product/

[80] Internetska stranica (pristupljeno 19.10.2023): https://www.in2access.co.uk/products/proloop-2-loop-detector-2-relays

[81] Internetska stranica (pristupljeno 19.10.2023): https://www.ellabo.hr/sabirnica-2-12-plava-2x16mm2-12x10mm2-1-e-e

[82] Internetska stranica (pristupljeno 19.10.2023): https://www.ellabo.hr/sabirnica-2-12-zelena-2x16mm2-12x10mm2-1-e-e

[83] Internetska stranica (pristupljeno 19.10.2023): https://fotoprofessor.wordpress.com/angle-of-view-assignment/

[84] Internetska stranica (pristupljeno 19.10.2023): https://hr.wikipedia.org/wiki/%C5%BDari%C5%A1na_duljina

[85] Internetska stranica (pristupljeno 19.10.2023): https://hr.wikipedia.org/wiki/Apertura_(razdvojba)

[86] Internetska stranica (pristupljeno 19.10.2023): https://willardsharpphotography.com/2021/03/extreme-weather-photography-aperture-settings/

[87] Internetska stranica (pristupljeno 19.10.2023): https://en.wikipedia.org/wiki/Shutter_speed

[88] Internetska stranica (pristupljeno 19.10.2023): https://www.wildnessphotos.com/visual-reference-guides.html

[89] Internetska stranica (pristupljeno 19.10.2023): https://www.vivotek.com/learning/feature-article/22/wdr

[90] Internetska stranica (pristupljeno 19.10.2023): https://elinetechnology.com/definition/wdr-wide-dynamic-range/

POPIS SLIKA

Slika 2.1. Primjer sustava kontrole pristupa za četiri vrata [3] *4*
Slika 2.2. Magnetna kartica [7] *6*
Slika 2.3. Kartica sa čitačem [8] *7*
Slika 2.4. Princip rada solenoida[8] *7*
Slika 2.5. RFID antena [9] *9*
Slika 2.2.6. RFID tag [10] *9*
Slika 2.7. Aktivni RFID tag [12] *10*
Slika 2.8. NFC čitač [14] *11*
Slika 2.9. Kontroler u elektroormaru [16] *13*
Slika 2.10. Kontroler za 4 vrata [18] *14*
Slika 2.11. Samostalni sustav [19] *15*
Slika 2.12. DB9(lijevo) i DB25(desno) [20] *16*
Slika 2.13. Raspored bitova [20] *16*
Slika 2.14. Povezivanje RS-422 uređaja [20] *17*
Slika 2.15. Prikaz diferencijalnog pristupa [21] *18*
Slika 2.16. Topologija sa dvije žice RS485 linija [20] *19*
Slika 2.17. RS-485 Topologija sa 4 žice [20] *19*
Slika 2.18. Način spajanja Wiegand standarda [24] *21*
Slika 2.19. Prekidač položaja vrata [30] *24*
Slika 2.20. Lijevo senzor, desno REX dugme [17] *25*
Slika 3.1 Oblici otiska prsta. [39] *30*
Slika 3.2. Uređaj sa više mogućnosti autentifikacije [17] *32*
Slika 3.3. Princip rada optičkog senzora [42] *33*
Slika 3.4. Princip rada kapacitivnog senzora [43] *35*
Slika 3.5. Uređaj za skeniranje geometrije ruke [46] *38*
Slika 3.6. Građa oka [51] *40*
Slika 3.7. Uređaj za prepoznavanje šarenice oka [53] *41*
Slika 3.8. Mrežnica [57] *42*
Slika 3.9. Organi potrebni za stvaranje glasa [60] *45*
Slika 3.10. Zvučni valovi [62] *46*
Slika 3.11. Spektogram zvuka [62] *47*
Slika 4.1. Detekcija slova "A" [64] *51*
Slika 4.2. Proces detekcije tablice putem dubokog učenja [64] *52*
Slika 4.3. Shema električnog ormara [Izrada autora] *54*
Slika 4.4. Termostat [65] *55*
Slika 4.5. Prenaponska zaštita [66] *55*
Slika 4.6. FID SKLOPKA [69] *56*
Slika 4.7. Osigurač (71) *57*
Slika 4.8. Stakleni osigurač [72] *57*
Slika 4.9. Napajanje napona 12 V [73] *58*
Slika 4.10. Napajanje napona 48 V [74] *58*
Slika 4.11. Ulazno/izlazni uređaj [75] *58*
Slika 4.12. Mrežni switch [76] *59*
Slika 4.13. Relej za din šinu [78] *59*
Slika 4.14 Stezaljke [79] *60*
Slika 4.15 Kontroler petlje [80] *60*

Slika 4.16. Sabirnice nule faze [81] *61*
Slika 4.17 Sabirnica uzemljenja [82] *61*
Slika 4.18. Idejno rješenje [Izrada autora] *62*
Slika 4.19. Shema glavnih elemenata [Izrada autora] *64*
Slika 4.20. Spajanje kontrolera petlje [Izrada autora] *65*
Slika 4.21. Shema spajanja napajanja 12 VDC [Izrada autora] *65*
Slika 4.22. Shema spajanja napajanja 48 VDC [Izrada autora] *66*
Slika 4.23. Shema spajanja ulazno/izlaznog uređaja [Izrada autora] *67*
Slika 4.24. Način spajanja releja na ulazno/izlazni uređaj [Izrada Autora] *67*
Slika 4.25. Žarišna duljina [83] *68*
Slika 4.26. Apertura [86] *69*
Slika 4.27. Vrijeme ekspozicije [88] *70*
Slika 4.28. WDR [90] *71*
Slika 4.29. Postavke vremena ekspozicije i pojačanja [Izrada Autora] *72*
Slika 4.30. Postavke svjetline, kontrasta, zasićenosti i oštrine [Izrada Autora] *73*
Slika 4.31. Prikaz u softveru [Izrada autora] *74*

SAŽETAK I KLJUČNE RIJEČ

U prvom poglavlju upoznajemo se osnovnim elementima i uređajima sustava kontrole pristupa. Osim uređaja pružamo uvid u načine komunikacije između uređaja, te su predstavljene kontrole pristupa koje koriste kartice i tagove. U drugom poglavlju predstavljene su biometrijske metode kontrole pristupa, a to su: prepoznavanje lica, prepoznavanje otiska prsta, prepoznavanje šarenice, prepoznavanje mrežnice i prepoznavanje glasa. Opisane su prednosti i mane tih metoda, opće karakteristike, te su opisani slučajevi u kojima se koriste. U posljednjem poglavlju obrađen je projekt izrade kontrole pristupa koji koristi LPR kamere, kartične čitače i portafon. Prikazana je i objašnjena detaljna shema spajanja električnog ormara i pripadnih uređaja.

Ključne riječi: Sustav kontrole pristupa, komunikacija, biometrija, prepoznavanje lica, otisak prsta, prepoznavanje šarenice, prepoznavanje mrežnice, LPR

ABSTRACT AND KEYWORDS

In the first chapter, we familiarize ourselves with the basic elements and devices of the access control system. In addition to devices, we provide insights into the ways of communication between devices, and we introduce access controls that utilize cards and tags. The second chapter presents biometric access control methods, which include: facial recognition, fingerprint recognition, iris recognition, retinal recognition, and voice recognition. We describe the advantages and disadvantages of these methods, their general characteristics, and provide examples of scenarios in which they are used. In the final chapter, we discuss a project for implementing access control using license plate recognition cameras, card readers, and an intercom system. A detailed diagram of the electrical cabinet connection and associated devices is shown and explained.

Keywords: Access control system, communication, biometrics, facial recognition, fingerprint recognition, iris recognition, retina recognition, LPR (License Plate Recognition)