



Gimnazija Franca Miklošiča Ljutomer

Prešernova ulica 34

9240 Ljutomer

## **Raziskovalna naloga**

# **Avtomatska identifikacija**

Področje: elektrotehnika, elektronika in robotika

Avtor: Aljaž Utroša, Jan Smolko, Sergej Trstenjak

Mentor: Damjan Erhatic, prof.

Ljutomer, Februar 2022

## **POVZETEK**

V današnjih časih je preverjanje prisotnosti zelo pomembno opravilo. Vsa večja podjetja so zaznala potrebo po identifikaciji oseb ali preverjanju, ali je ta oseba res tista za katero se izdaja. S tem so si zagotovili lastno varnost ter varnost premoženja in lastnine, pa tudi zaščito drugih.

S hitrim razvojem tehnologije in spletnih sistemov se je pojavilo več različnih sistemov za prepoznavanje oziroma identifikacijo oseb, ki nam pomagajo preveriti njihovo prisotnost. Trgovcem pa je posebej pomembno beleženje izdelkov v svoji trgovini, saj morajo vsako leto narediti vsaj eno inventuro. K temu pa so pripomogle različne črtne kode.

Raziskovalno delo smo razdelili na teoretični del in praktični del. V teoretičnem delu so predstavljeni različni sistemi za avtomatsko identifikacijo. V praktičnem delu pa je predstavljen primer avtomatske identifikacije z RFID-značko.

## **Ključne besede**

Identifikacija, varnost, tehnologija, črtne kode, sistem RFID.

## **Zusammenfassung**

In heutigen Zeiten ist das Überprüfen der Anwesenheit eine sehr wichtige Arbeit. Alle großen Unternehmen heben einen Bedarf für die Identifikation von Menschen wahrgenommen und das Überprüfen, ob die Person wirklich die ist, für die sie sich ausgibt. Mit dem Stellen sie eigene Sicherheit, Vermögen und Eigentum und die Sicherheit Anderer.

Mit der schnellen Entwicklung von Technologien und Netzwerken haben sich auch verschiedene Systeme für das Erkennen beziehungsweise die Identifikation von Personen entwickelt, die uns helfen ihre Anwesenheit zu überprüfen. Den Händlern ist es auch besonders wichtig das sie ihre Ware in ihren Geschäften notieren, da sie einmal pro Jahr eine Inventur machen müssen, dabei haben verschiedene Strichcodes entwickelt.

Die Forscherarbeit haben wir in den theoretischen und praktischen Teil unterteilt. In dem theoretischen Teil sind verschiedene Systeme für automatische Identifikation vorgestellt. Im praktischen Teil ist ein Beispiel der automatischen Identifikation mit der RFID Marke vorgestellt.

## **Schlüsselwörter**

Die Identifizierung, die Sicherheit, die Technologie, die Barcodes, das RFID-System.

# Kazalo vsebine

UVOD.....	1
Opredelitev teme raziskovanja in cilji .....	1
Hipoteze .....	1
Metode dela .....	2
BIOMETRIJA.....	3
FIZIKALNE BIOMETRIČNE METODE .....	3
DNA/DNK.....	3
Prstni odtisi.....	4
Šarenica .....	4
Obraz .....	5
VEDENJSKE BIOMETRIČNE METODE .....	6
Glas.....	6
RFID .....	6
Kako deluje RFID.....	7
Uporaba RFID .....	7
Radijski valovi .....	9
Sestava RFID sistema.....	10
RFID značka .....	10
VRSTE RFID ZNAČK .....	11
Pasivne značke .....	11
Aktivne značke.....	11
Semi-pasivne značke .....	11
RFID ČIPI.....	12

RFID kartice z nizko frekvenčnim čipom .....	12
RFID kartice z visoko frekvenčnim čipom in NFC .....	13
RFID kartice z ultra visoko frekvenco .....	16
ZAPISOVANJE RFID ZNAČK .....	16
ČITALEC RFID ZNAČK .....	17
POTEK DELA.....	17
MOŽNOSTI IZBOLJŠAVE.....	24
Povezava z podatkovno bazo .....	24
Povezava z eAsistentom.....	24
Bluetooth povezava.....	25
Prstni odtis.....	25
UGOTOVITVE IN SKLEPI.....	27
1 Hipoteza .....	27
2 Hipoteza .....	27
3 Hipoteza .....	27
ZAKLJUČEK.....	28
VIRI .....	29
Literatura.....	29
Slike .....	31

#### KAZALO SLIK

<b>Slika 1: DNK analiza [10] .....</b>	<b>3</b>
<b>Slika 2: Prstni odtis [11] .....</b>	<b>4</b>
<b>Slika 3: Šarenica [12] .....</b>	<b>5</b>
<b>Slika 4: Skeniranje obraza [13].....</b>	<b>5</b>
<b>Slika 5: Sonogram [14] .....</b>	<b>6</b>

<b>Slika 6: RFID [15]</b> .....	7
<b>Slika 7: RFID nalepka [16]</b> .....	8
<b>Slika 8: RFID sledenje živali [17]</b> .....	8
<b>Slika 9: RFID smučarske karte [18]</b> .....	8
<b>Slika 10: RFID cestnina [19]</b> .....	9
<b>Slika 11: RFID sistem [20]</b> .....	10
<b>Slika 12: sestava RFID značke [21]</b> .....	11
<b>Slika 13: Vrste značk [22]</b> .....	12
<b>Slika 14: EM4200 [23]</b> .....	13
<b>Slika 15: EM4550 [24]</b> .....	13
<b>Slika 16: MIFARE Classic® 4K [25]</b> .....	14
<b>Slika 17: NFC tehnologija [26]</b> .....	15
<b>Slika 18: NFC branje podatkov [27]</b> .....	15
<b>Slika 19: peer to peer [28]</b> .....	15
<b>Slika 20: RFID UHF [29]</b> .....	16
<b>Slika 21: Čitalec RFID [30]</b> .....	17
<b>Slika 22: Arduino [31]</b> .....	17
<b>Slika 23: ARDUINO UNO plošča [32]</b> .....	18
<b>Slika 24: RFID- RC522 [33]</b> .....	19
<b>Slika 25: Vezava osnovne plošče z RFID- RC522 [34]</b> .....	20
<b>Slika 26: Povezava plošče z čitalnikom [35]</b> .....	20
<b>Slika 27: USB kabel [36]</b> .....	20
<b>Slika 28: Prepoznavna obeska [37]</b> .....	21
<b>Slika 29: Prepoznavna kartice [38]</b> .....	21
<b>Slika 30: Izpis podatkov [39]</b> .....	21
<b>Slika 31: Program [40]</b> .....	22
<b>Slika 32: Program [41]</b> .....	23
<b>Slika 33: PHpMyAdmin [42]</b> .....	24
<b>Slika 34: eAsistent [43]</b> .....	25
<b>Slika 35: Modul bluetooth povezan z ploščo Arduino Uno [44]</b> .....	25
<b>Slika 36: Čitalec prstnih odtisov [45]</b> .....	26



# UVOD

Dandanes ima svetovni splet v življenj zelo pomembno vlogo. Dostopen je že na vsakem koraku ter nam s svojimi neomejenimi možnostmi omogoča najrazličnejše stvari. Sem sodijo iskanja informacij, spremljanja novic, nakupovanje, igranje iger, poslušanje glasbe, gledanje filmov in še več.

Vse te storitve pa zahtevajo določeno stopnjo zaščite in varnosti, s katero bi zabeležili dejanje določene osebnosti, kot na primer kupca v e-trgovini. Podoben namen ima beleženje prisotnosti v podjetju oziroma naš predlog: beleženje prisotnosti učencev pri pouku.

## *Opredelitev teme raziskovanja in cilji*

V zgodovini se razvilo zelo veliko različnih mehanizmov, ki skrbijo za varnost in zaščito sistemov in podjetij. To počnejo tako, da preprečujejo vstop nepooblaščenim in beležijo prisotnost zaposlenih.

Cilj naše raziskovalne naloge:

- predstaviti različne sisteme za avtomatsko identifikacijo;
- pojasniti, kako delujejo sistemi za avtomatsko identifikacijo,
- predstaviti idejo o uporabi RFID-značke na šolah.

## *Hipoteze*

- Z uporabo RFID-značk na šoli bi bilo beleženje dijakov hitrejše kot beleženje prisotnosti s strani profesorjev.
- Z uporabo RFID-značk na šoli bi bilo beleženje dijakov natančnejše kot beleženje prisotnosti s strani profesorjev.
- Z uporabo prstnih odtisov, bi bilo beleženje prisotnosti dijakov pristnejše kot z RFID značko.



## *Metode dela*

V teoretičnem delu smo za opis in predstavitev avtomatskih sistemov identifikacije uporabili spletno literaturo. V praktičnem delu pa smo najprej raziskali, kaj vse potrebujemo, da bo avtomatsko preverjanje prisotnosti učencev pri pouku mogoče. Pozanimali se smo delovanje programa Arduino, in napisali program, ki odčita potrebne informacije s kartice. Raziskali smo tudi možnosti za nadgradnjo programa in programske opreme.

# BIOMETRIJA

Biometrija je opredeljena kot študija in uporaba znanstvenih metod za analiziranje človekovih edinstvenih značilnosti. Je ena izmed možnosti, ki se uporablja za avtomatsko identifikacijo. Dejansko mnogi od nas uporabljajo biometrijo v obliki prstnih odtisov in obraza. Namen biometrije je identificirati človeka na podlagi njegovih unikatnih telesnih lastnosti, njegovih kretenj ali dejanj. Nudi enostavno in zanesljivo rešitev pri preverjanju identitete ljudi. Za identifikacijo se uporabljajo različne modalnosti, katerih unikatnost pri ljudeh izkoriščajo biometrične metode. [1, 16]

## FIZIKALNE BIOMETRIČNE METODE

### *DNA/DNK*

DNA oziroma DNK je molekula, v kateri so zapisane genetske informacije v vseh živih organizmih. Glavna vloga molekule DNK je shranjevanje bistvenih bioloških informacij. Zaporedje nukleotidov določa pomen genetske informacije. V vseh živih organizmih (z izjemo nekaterih virusov) ima DNK obliko dvojne vijačnice, pri čemer se dve molekuli DNK ovijeta ena okrog druge. DNK je najnatančnejši način za prepoznavo oziroma identifikacijo človeka, zato se uporablja pri prepoznavanju storilcev, za katere sumijo, da so sodelovali v kaznivem dejanju [5].



Slika 1: DNK analiza [10]

## Prstni odtisi

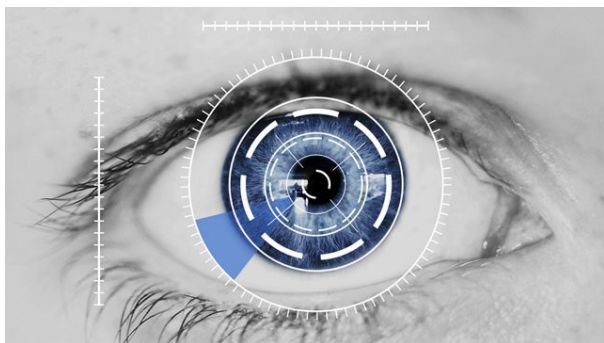
Prstni odtis je konfiguracija grebenov s porami, ki jih delijo doline. Ležijo na ožilju, neposredno pod kožo. Vzorec prstnega odtisa je povezan z določenimi električnimi in toplotnimi značilnostmi kože. To pomeni, da svetlobo, toploto ali električno napetost (ali kombinacijo vseh) lahko uporabimo za zajem podobe prstnega odtisa. Prstni odtis nastane že pri razvoju zarodka in se s starostjo osebe ne spremeni, temveč raste v svoji prvotni obliki in po končani rasti osebe ostane v svoji velikosti nespremenjen. Tudi po poškodbi se obnovi v prvotno obliko. Niti enojajčni dvojčki nimajo enakih prstnih odtisov [7].



Slika 2: Prstni odtis [11]

## Šarenica

Poznamo več načinov, namenjenih za prepoznavo šarenice. Signalno usmerjene metode prepoznajo vzorec šarenice na podlagi informacije signalov. Informacija signala je neodvisna od jakosti barve in svetlosti. John Daugman je leta 1994 prvi implementiral in predstavil komercialni sistem na podlagi signalov. Wild je predstavil metodo za prepoznavanje vzorca šarenice na podlagi teksture. Za delovanje je potrebna slika visoke kvalitete. Za lokalizacijo šarenice se uporablja Houghova transformacija, ki poišče dva kroga, ki tvorita notranji in zunanji rob. Za spodnjo in zgornjo veko pa se uporabita krivulji. Za vzorec se uporablja Laplacov filter, iz katerega se sestavi Laplacova piramida [17].



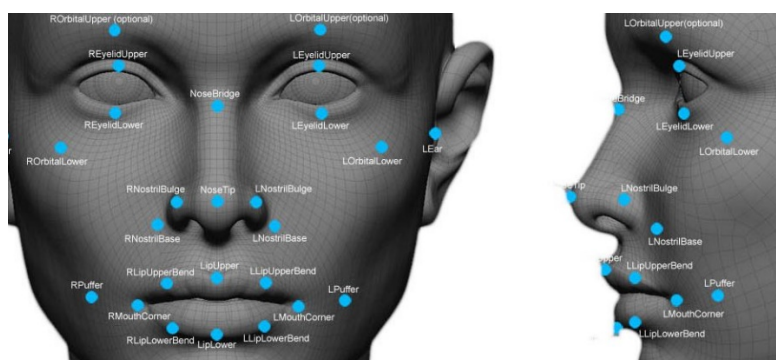
Slika 3: Šarenica [12]

## Obraz

Prepoznavanje obraza je se uporablja v različne namene, vendar najpogosteje zaradi za zagotavljanje varnosti in ugotavljanje kazenskega pregona. Letališča uporabljajo programsko opremo za prepoznavanje obrazov na več različnih načinov, kot je skeniranje obrazov potnikov za iskanje posameznikov, ki so osumljeni kaznivih ali terorističnih dejanj. Tehnologija, ki se uporablja za prepoznavanje obraza, vključuje obrazne skenerje in programe za ujemanje obraza. Sistemi uporabljajo številne meritve in tehnologije za optično branje obrazov, vključno s termičnim slikanjem in določanjem geometrijskih razmerij obraznih lastnosti. Ko sistemi prepoznavajo obraze in opravljajo različne meritve, nastopijo omejitve, ki otežijo ali celo preprečijo prepoznavo obraza [8, 16].

To so:

- slaba ločljivost slike in slaba osvetlitev, ki zmanjšata natančnost rezultatov;
- različni koti in izrazi obraza, tudi preprost nasmeh, ki lahko predstavljajo izzive;
- nepovezanost skeniranega obraza s profilom; optično branje namreč ne bo učinkovito, če v bazi podatkov ni dostopnih fotografij.



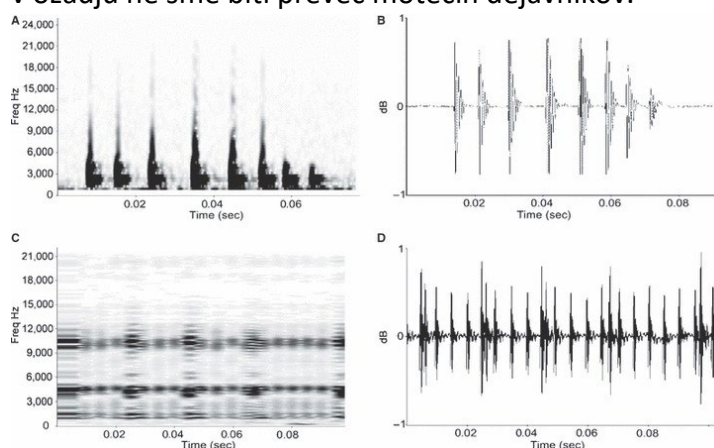
Slika 4: Skeniranje obraza [13]

# VEDENJSKE BIOMETRIČNE METODE

## Glas

Pri prepoznavi glasu govorimo o glasovnem oziroma zvočnem spektrogramu, ki nam prikazuje amplitudo in frekvenco zvoka. Področje ki se ukvarja z glasovno primerjavo oziroma glasovno identifikacijo, imenujemo sonoskopija. Če izraz prevedemo iz grščine, pomeni »gledanje glasu«, torej vizualizacijo glasu. S sonografom se s pomočjo računalniške tehnologije slišani glas pretvori v računalniku razumljivo digitalno obliko, ta pa jo nato prerise na papir. Ta izdelek imenujemo sonogram. Z njega lahko razberemo frekvenco in jakost glasu. Za natančno prepoznavo glasu pa morajo biti izpolnjeni določeni pogoji [18]:

- govor mora biti dovolj dolg, pri tem ni priporočljivo branje;
- uporaba istega slenga oziroma narečja;
- v ozadju ne sme biti preveč motečih dejavnikov.



Slika 5: Sonogram [14]

## RFID

RFID je radiofrekvenčna identifikacija. Je tehnologija ki jo uporabljamo pri identificiranju s pomočjo elektromagnetnega valovanja na področju radijskih frekvenc. Uporaba nam je prinesla hitrejšo, zanesljivejšo, varnejšo in bolj sledljivo označevanje, ki ga črtne kode ne omogočajo. RFID ima korenine v vojski in sicer od leta 1948, ko so prvič objavili članek o uporabi odbijajočih se radijskih signalov za identifikacijo premikajočih objektov [1, 3, 10].

## Kako deluje RFID

Ko je RFID-odzivnik v dosegu RFID-čitalnika, ta preko ustreznih anten s pomočjo radijskih frekvenc razbere podatke, ki so zapisani v odzivniku. Vanj se lahko vpišejo tudi novi željeno podatki. Čitalnik lahko v 1 sekundi identificira več kot 100 odzivnikov. Odzivniki so sestavljeni iz majhnih integriranih elektronskih vezij (čipov) in RF-antene, lahko vsebujejo tudi baterijo. Takrat govorimo o aktivnih odzivnikih, sicer pa so pasivni. Poznamo različne oblike RFID [1, 3, 10]:

- etiketa oziroma pametne nalepke,
- kartice,
- obeske,
- ploščice,
- čipe.



Slika 6: RFID [15]

## Uporaba RFID

Ker je sistem RFID v zelo kratkem času zmožen razbrati veliko odzivnikov, njegova uporaba narašča, aktualna je predvsem pri izvajanju inventure ali sprejemu enot v skladišče. Uporablja pa se tudi za [1, 2, 4]:

- avtomatsko plačevanje cestnine (aktivni RFID, odčitavanje na 10 m),
- spremljanje pošiljk,
- izposojo knjig,
- sledenje in označevanje živali,
- registracijo delovnega časa,
- smučarske karte,
- merjenje časa v športu.



Slika 7: RFID nalepka [16]



Slika 8: RFID sledenje živali [17]



Slika 9: RFID smučarske karte [18]



Slika 10: RFID cestnina [19]

## *Radijski valovi*

Sistem RFID za delovanje uporablja radijske valove, ki so elektromagnetno valovanje. Značilnost elektromagnetnega valovanja je, da se lahko razširja skozi fizične ovire ali vakuum, v katerih se razširja s svetlobno hitrostjo. Spekter elektromagnetnega valovanja za radiofrekvenčno komunikacijo razdelimo na nizkofrekvenčne radijske pasove in visokofrekvenčne radijske valove [1, 3, 14].

Nizkofrekvenčni radijski valovi:

- ovire niso moteče in grede čeznje, dolg doseg valov;
- moč z razdaljo od vira pada.

Visokofrekvenčni radijski valovi:

- širijo se v ravnih linijah;
- od ovir se odbijajo, njihov doseg je krajši;
- za branje potrebna vidnost med RFID-značko in čitalcem.

Da je delovanje radijskih valov nemoteno, je potrebno opredeliti frekvenčna območja. Države po svetu imajo dodeljena radiofrekvenčna območja za delovanje posameznih naprav, tudi RFID-značk, vendar s tem zavirajo razvoj univerzalnega globalnega standarda za preskrbovalne prodajne RFID-verige [1].

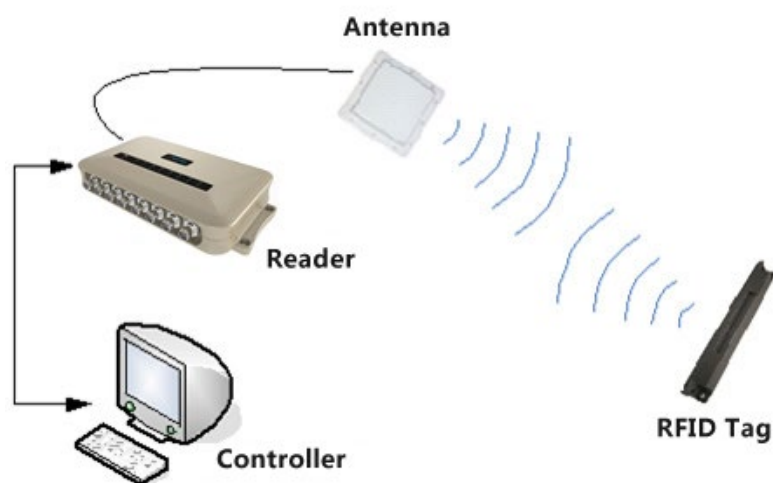


Naprave v Evropi na primer uporabljajo frekvenčno območje 50 MHz, v ZDA pa uporabljajo območje 10 MHz, ker so bili sprejeti takšni standardi. Naprava, ki je uporabna v Evropi, s sistemi v ZDA ni kompatibilna in obratno [1].

## Sestava RFID sistema

RFID-sistem vsebuje [1]

- značko (tag ali priponko);
- zapisovalnik – z njim zapišemo podatke na značko;
- čitalnik – razbere podatke z značke;
- računalnik – kjer je, se odloči za naslednjo dejanje.



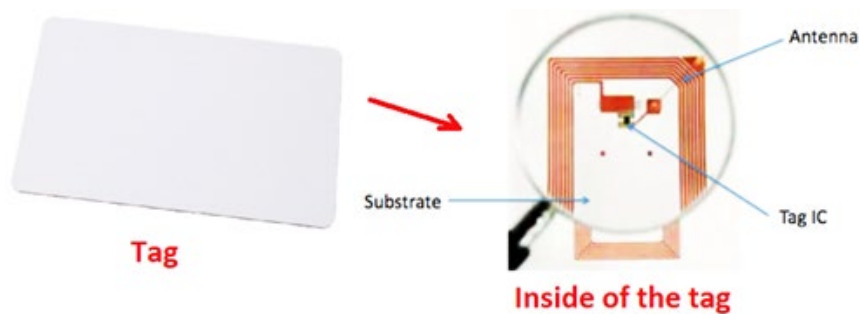
Slika 11: RFID sistem [20]

## RFID značka

RFID-značka se nahaja v plastičnem ohišju oziroma materialu, ki ne moti frekvenc (kovine).

Sestavljajo jo [1]:

- mikročip – miniaturno integrirano vezje;
- antena:
  1. različnih dimenzij, s katero sprejema in oddaja elektromagnetno valovanje;
  2. narejena je lahko iz srebra, aluminija ali bakra;
  3. geometrija, velikost in material določata frekvenco branja značke;
- baterija – vsebujejo jo aktivne in semipasivne značke.



Slika 12: sestava RFID značke [21]

## VRSTE RFID ZNAČK

### *Pasivne značke*

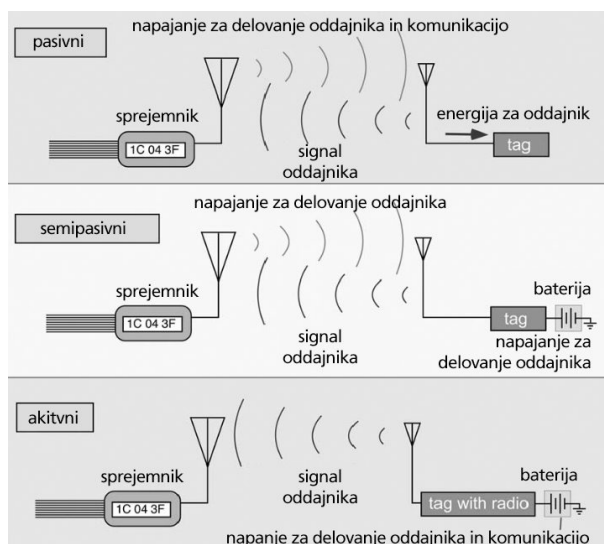
Nimajo baterije, ampak uporabljajo čitalnik. Elektromagnetni valovi inducirajo tok v anteni značke, ta pa nato čitalcu posreduje svoje podatke. V primerjavi z aktivnimi značkami so manjše, imajo daljšo življenjsko dobo in manjše področje delovanja. Uporabljajo se kot vozovnice (Urbana) in za registracijo delovnega časa [1, 3, 19].

### *Aktivne značke*

Delujejo z lastnim napajanjem oziroma imajo dodatno baterijo. Zato oddajajo in sprejemajo signale na več kot 100 metrov. Primerne so predvsem aplikacije, ki jih vgradimo permanentno in jih redno vzdržujemo (menjava baterij). Uporabljajo se pri sledenju avtomobilov in ladijskega tovora [1, 3, 19].

### *Semi-pasivne značke*

Po lastnostih so podobne pasivnim, vendar imajo dodano lastno napajanje in možnost, da delujejo podobno kot aktivne. Uporabljajo se za zabojnike in palete [1, 3, 19].



Slika 13: Vrste značk [22]

## RFID ČIPI

RFID-čipe, ki se nahajajo v plastičnih značkah, delimo po frekvenčnih območjih, v katerih delujejo. Razdelimo jih na [11]:

- LF – Low Frequency
- HF – High Frequency
- UHF – Ultra High Frequency

Čipi se potem razlikujejo še glede na količino spomina, razdaljo branja podatkov in dodatno varnost podatkov.

### *RFID kartice z nizko frekvenčnim čipom*

Kartice komunicirajo na nizki frekvenci oziroma na frekvenci 125 kHz. To frekvenčno območje deluje na kratek bralni doseg, običajno 1 do 10 cm, počasnejša je tudi hitrost branja. Kartice, ki komunicirajo na frekvenci 125kHz, se uporabljajo v starejših sistemih za kontrolo vstopa.

Najbolj popularni 125 kHz čipi, ki so namenjeni samo za branje, so EM4200 oziroma predhodniki EM4102 ali EM4100. Od bralno-pisalnih čipov pa so najbolj priljubljeni EM4550, T5577 in čipi z oznako Q5 [11].



Slika 14: EM4200 [23]



Slika 15: EM4550 [24]

### *RFID kartice z visoko frekvenčnim čipom in NFC*

Kartice komunicirajo na frekvenci 13,56 MHz. To frekvenčno območje zagotavlja večji bralni doseg in hitrejšo komunikacijo. Najbolj priljubljeni čipi iz visoko frekvenčnega območja so MIFARE Classic® 1K, ki vsebujejo bralno-pisalni čip s spominom 1 kByte. Poleg njih so priljubljeni še MIFARE Classic® 1K/4K/8K, NTAG213, MIFARE DESFire® 2K/4K/8K, ICode SLI in MIFARE Ultralight®.

Razdalja, na kateri komunicirajo čipi s frekvenco 13,56 MHz, je 1 do 5 cm, uporabljajo pa se predvsem za registracijo delovnega časa, v logistiki in za plačilne kartice, pri katerih je potrebna visoka zaščita podatkov [11].



Slika 16: MIFARE Classic® 4K [25]

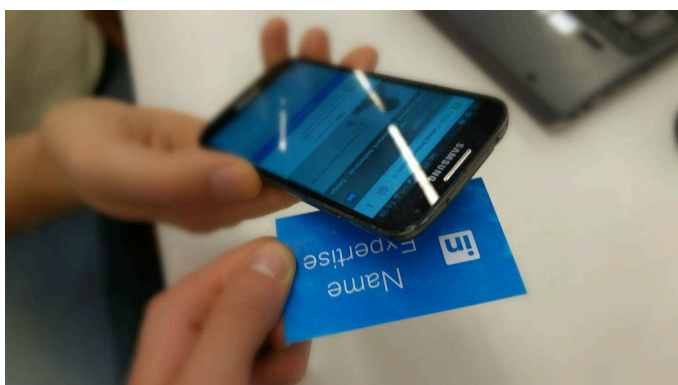
V zadnjem času pa se je začela uporabljati NFC-tehnologija ki prav tako deluje na frekvenci 13,56 MHz in predstavlja podskupino RFID-kartic. NFC-tehnologija nam omogoča varno brezkontaktno komunikacijo med dvema elektronskima napravama. Komunikacija je vzpostavljena zelo preprosto, saj ne potrebuje nobene posebne priprave kot pri drugih brezžičnih komunikacijah. Uporabniku omogoča brezžične transakcije, dostop do digitalne vsebine in povezovanje naprav, ki jih približamo drugo k drugi, razdalja, ki omogoča komunikacijo je 4 do 5 cm, z bližino naprav pa si zagotovimo večjo varnost. Dandanes so s tehnologijo NFC opremljeni tudi pametni telefoni, kar omogoča, da uporabnik na njih shranjuje kreditne kartice, darilne bone, kartice zvestobe, vozovnice, karte za ogled tekme. Telefon z nameščeno aplikacijo je ob približanju s pomočjo tehnologije NFC pošlje podatke na terminal Pay Pass (storitev MasterCarda za brezkontaktno plačevanje preko terminala) [6, 9, 12, 13, 19].



Slika 17: NFC tehnologija [26]

Ločimo tri načine povezovanja [6, 9, 12, 13, 19].

- Prvi je imenovan čitalec/bralac in napravi NFC omogoča branje podatkov z značk NFC, ki so na primer v reklamnih posterjih. Značke potrjene s strani NFC-foruma pa niso samo bralne, pač pa lahko nanje tudi zapišemo informacije.
- Drugi način s pomočjo tehnologije NFC omogoča shranjevanje podatkov na pametno kartico. Tak način je uporaben pri vozovnicah.
- Tretji način imenovan »peer to peer«, omogoča komunikacijo med dvema napravama. Napravi si lahko izmenjujeta datoteke in različne kontakte.



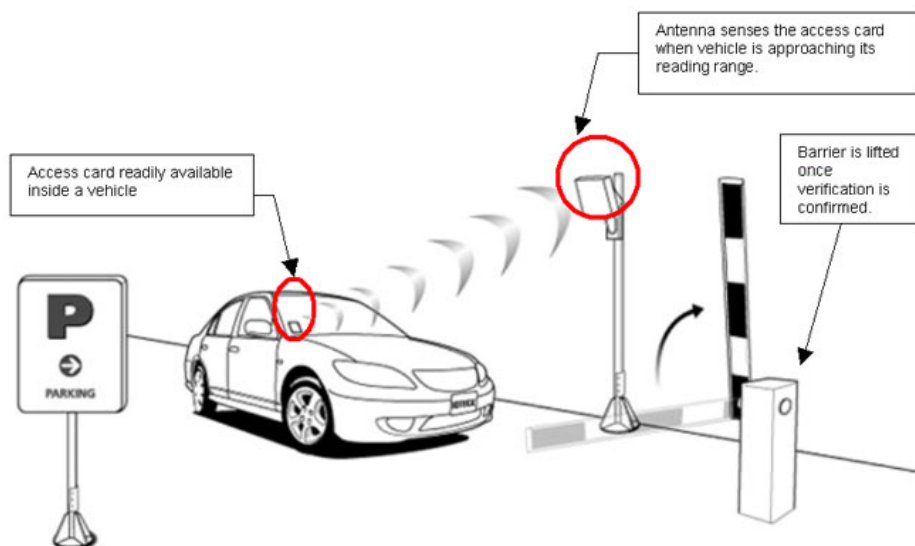
Slika 18: NFC branje podatkov [27]



Slika 19: peer to peer [28]

## RFID kartice z ultra visoko frekvenco

UHF-kartice komunicirajo na frekvenci med 860 in 915 MHz. Pri tej frekvenci je bralni doseg kar 12 m, zaradi česar so primerne za komunikacijo na večjih razdaljah. Kartice UHF RFID se uporabljajo v parkirnih sistemih, na območjih cestnin in v logističnih projektih. V teh karticah je priložen čip Alien Higgs-3 [11].



Slika 20: RFID UHF [29]

## ZAPISOVANJE RFID ZNAČK

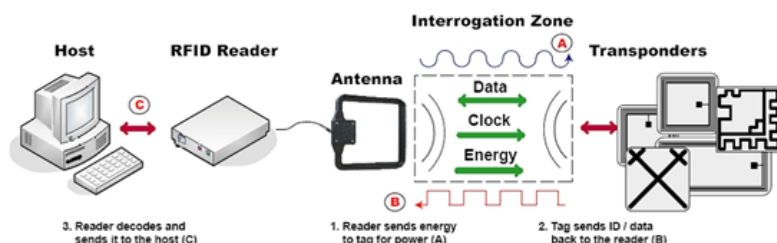
Ko so značke izdelane, so brez funkcije, zato je nanje treba zapisati podatke oziroma jih enkodirati. Enkodiranje lahko izvedemo s [1, 11]:

- čitalnikom, vgrajenim v RFID-tiskalnik,
- samostojnim čitalnikom.

Glede na zapisovanje podatkov obstaja več vrst RFID-značk. Na nekatere lahko podatke zapišemo samo enkrat, na druge pa večkrat ali celo neomejenokrat. Ko čitalnik zapisuje podatke na značke, za to potrebuje nekaj sto milisekund. Prav tako je pomembno, da pri programiranju več značk posamezno značko osamimo, saj je zapisovanje podatkov brezžično in lahko pride do vnosa napačnih podatkov na napačno značko [1, 11].

# ČITALEC RFID ZNAČK

Čitalniki razbirajo podatke tako, da oddajajo radijske valove, na katere se značka odzove in identificira, če se nahaja znotraj področja delovanja čitalnika [2].



Slika 21: Čitalec RFID [30]

## POTEK DELA

Pri praktičnem delu smo se odločili, da bi avtomatizirali beleženje prisotnosti učencev. Pri tem smo potrebovali RFID čitalec (RFID-RC522), RFID značke, premostitvene žice, USB kabel, osnovno ploščo (ARDUINO UNO) in računalnik. Prav tako smo se pozanimali o programu ARDUINO, s katerim smo napisali program.

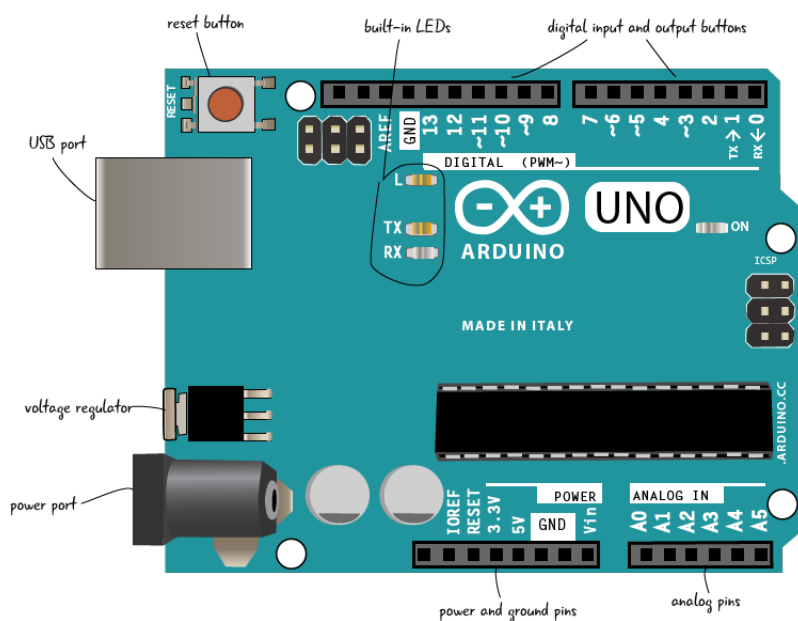


Slika 22: Arduino [31]

Na osnovni plošči ARDUINO UNO se nahaja gumb za ponastavitev v primeru težav. LED diode s svetlobnimi znaki javljajo napetost plošče in komunicirajo z računalnikom, tako z neenakomernim utripanjem pomagajo pri odpravljanju težav v programu. Nekateri digitalni pini so označeni s ~ (tilda) in jih imenujemo *PWM* pini. To so posebni pini na katerih lahko dosežemo nastavljive vrednosti, od 0 do 255 Hz in ne samo *HIGH* (visoko) ali *LOW* (nizko). Torej na primer, če bi v program zapisali `analogWrite(pin,127)`, bo polovico časa *OUTPUT* (izhod) na *HIGH* (visoko) in polovico na *LOW* (nizko). V programu lahko `pinMode()` nastavimo



na *INPUT* (vhod) ali *OUTPUT* (izhod). Če je nastavljen na *OUTPUT* (izhod), bo napetost za *HIGH* (visoko) 5V (ali 3.3V na 3.3V ploščah) in 0V za *LOW* (nizko). Če pa je nastavljen na *INPUT* (vhod) bo *digitalWrite()* avtomatsko omogočil *HIGH* (visoko) ali onemogočil *LOW* (nizko). Analogni *INPUT* (vhodni) pini, so lahko uporabljeni enako kot digitalni pini, vendar se lahko pri analognih pinih izbere poljubna vrednost, enako kot pri *PWM* pinih. Pini za električno energijo in ozemljitev so pini s katerimi povežemo napravo (čitalec-RFID), na potrebno napetost in ozemljitev (*GND*). Električni vhod je pod nadzorom regulatorja napetosti, ki regulira potrebno napetost za ARDUINO UNO ploščo. USB vhod, ki ga povežemo z računalnikom s pomočjo USB kabla, da lahko prenesemo program. USB kabel lahko služi tudi kot vir napetosti.

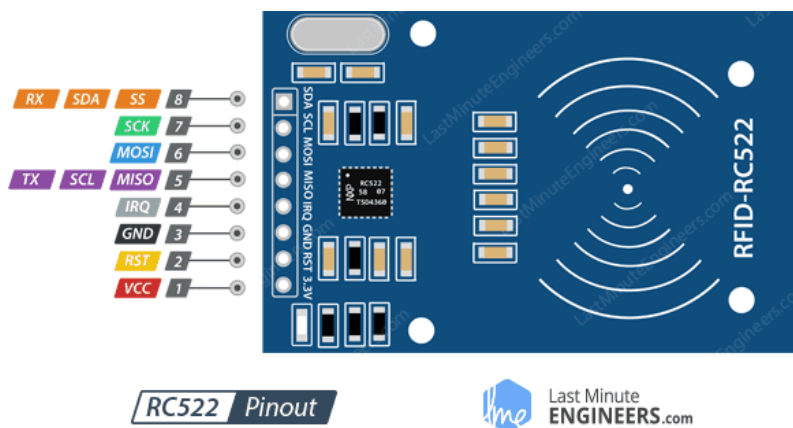


Slika 23: ARDUINO UNO plošča [32]

RFID-RC522 je čitalnik RFID značk. Deluje na frekvenci 13,56 MHz, torej na visoki frekvenci. Branje značk poteka na doseg 5 cm in bere pasivne značke. Ima 8 pinov in vsak ima svojo nalogo :

- VCC- namenjen je za napajanje modula, to je od 2.5 do 3.3 volta. Torej se ga priključi na ploščo na pin 3.3V, če se priključi na pin 5V bo to najverjetneje uničilo RFID čitalec.
- RST- namenjen je za ponastavitev in izklop. Ko je napetost na LOW se čitalec izklopi, ko pa je napetost HIGH se modul ponastavi.
- GND- je pin namenjen ozemljitvi in se poveže z pinom GND na plošči.
- IRQ- pin, ki opozori če je RFID značka v bližini.

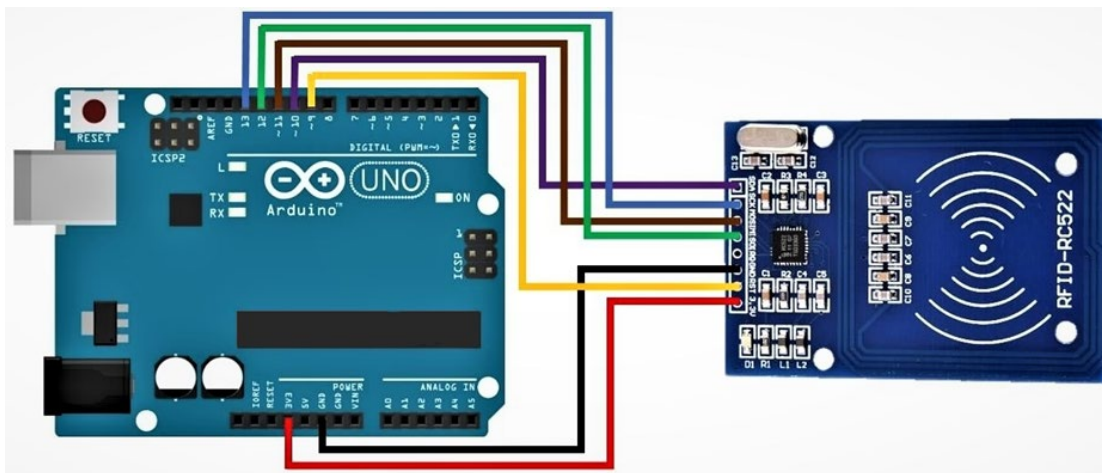
- MISO / SCL/ Tx- Nadrejena naprava (Arduino) sprejema podatke in podrejena jih oddaja.
- MOSI- Nadrejena naprava (Arduino) oddaja podatke in podrejena jih sprejema
- SCK- sprejema signal od nadrejene naprave.
- SS / SDA / Rx- Nadrejena naprava se odloči, s katero podrejeno bo komunicirala.



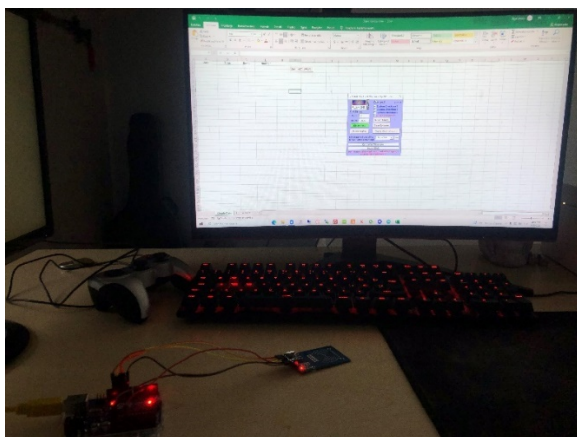
Slika 24: RFID- RC522 [33]

Ko smo spoznali lastnosti Arduino uno plošče in RFID-RC522 smo morali komponenti povezati, pri tem smo si pomagali s premostitvenimi žicami. Vezava pa je potekala tako (slika 34):

1. VCC je vezan na pin 3.3V na plošči (rdeča),
2. RST je vezan na pin ~9 na plošči (rumena),
3. GND je vezan na pin GND na plošči (črna),
4. Tx / SCL / MISO je vezan na pin 12 na plošči (zelena),
5. MOSI je vezan na pin ~11 na plošči (rjava),
6. SCK je vezan na pin 13 na plošči (modra),
7. Rx / SDA / SS je vezan na pin ~10 na plošči (vijolična).



Slika 25: Vezava osnovne plošče z RFID- RC522 [34]



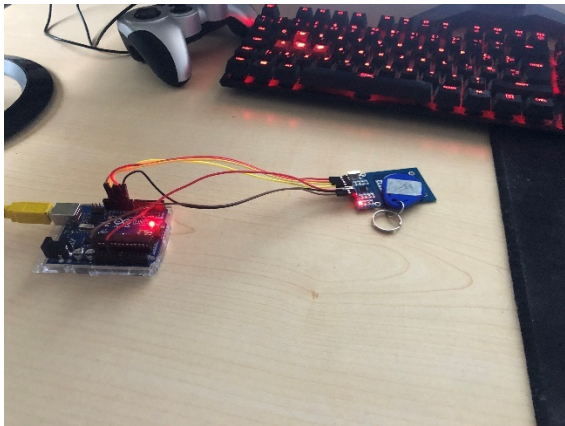
Slika 26: Povezava plošče z čitalnikom [35]

V program Arduino (sliki 40 in 41) smo vpisali pine, ki smo jih uporabili pri vezavi in jim določili njihov namen. Vpisali smo tudi podatke katere želimo, da se prikažejo na zaslonu računalnika po zaznani kartici. Ko smo program napisali smo računalnik in ARDUINO UNO ploščo povezali s USB kablom preko katerega se je prenesel program, v našem primeru je USB kabel služil kot vir električne energije.



Slika 27: USB kabel [36]

Spodaj (sliki 37, 38) sta primera, kako bi potekalo beleženje dijakov. Vsak dijak bi dobil kartico na kateri bi bilo zapisano ime, priimek, datum in uro prihoda, zraven lahko dodamo še razred. Ko bi čitalec RFIC-RC522 razbral podatke, bi program poslal informacije do osnovne plošče. Tam se shranijo in izvršujejo ukazi, nato bi program poiskal lastnika te kartice in v Microsoft Excel zapisal potrebne podatke (slika 39).



Slika 28: Prepoznavna obeska [37]



Slika 29: Prepoznavna kartice [38]

Ime	Date	Ura prihoda
Sergej Trstenjak	22.2.2022	7:48:36
Jan Smolko	22.2.2022	7:48:39

Slika 30: Izpis podatkov [39]

```

#include <SPI.h>
#include <MFRC522.h>

#define SS_PIN 10
#define RST_PIN 9

MFRC522 mfrc522(SS_PIN, RST_PIN);

byte card_ID[4]; //kartica ima 4 byte
byte Name1[4]={0x25,0x6F,0x03,0x6D}; //prvi UID
byte Name2[4]={0xB5,0xD6,0xB1,0xD5}; //drugi UID
//vec ucencev=vec stevilka(Name3,...)

//program odcita samo prihod(odcita kartico samo enkrat)
int NumbCard[2]; //stevilo vseh dijakov(kartic)
int j=0;

int const RedLed=6;
int const GreenLed=5;
int const Buzzer=8;

String Name; //ime
long Number; //zaporedna stevilka
int n; //stevilka kartice

void setup() {
  Serial.begin(9600); //poveze komunikacijo z racunalnikom
  SPI.begin(); //vkljuci SPI
  mfrc522.PCD_Init(); //Vkljuci citalec

  Serial.println("CLEAR SHEET"); //zacne pri prvi vrstici
  Serial.println("LABEL,Date,Time,Name,Number"); //zapise datum uro ime in zaporedno stevilko

  pinMode(RedLed,OUTPUT);
  pinMode(GreenLed,OUTPUT);
  pinMode(Buzzer,OUTPUT);

}

void loop() {
  //caka da se kartica prisloni
  if (! mfrc522.PICC_IsNewCardPresent()) {
    return; //ce ni kartice gre od zacetka dokler se kartica ne prisloni
  }
  //odcita kartico
  if (! mfrc522.PICC_ReadCardSerial()) {
    return; //prebere kartico in da podatke od kartice
  }
}

```

Slika 31: Program [40]

```

card_ID[i]=mfrc522.uid.uidByte[i];

    if(card_ID[i]==Name1[i]){
        Name="Jan smolko";//lastnik kartice
        Number=1;//zaporedna stevilka
        j=0;//prva kartica se oznaci z 0=j
    }
    else if(card_ID[i]==Name2[i]){
        Name
        ="Sergej Trstenjak";//lastnik kartice
        Number=2;//zaporedna stevilka
        j=1;//druga kartica je oznacena z 1=j
    }
    else{
        digitalWrite(GreenLed,LOW);
        digitalWrite(RedLed,HIGH);
        goto cont;//go directly to line 85
    }
}

if(NumbCard[j] == 1){//preveri ali je citalec zaznal kartico
//za uporabo dodatnega zaslona
//Serial.println("Already Exist");
}
else{
NumbCard[j] = 1;
n++;
Serial.print("DATA,DATE,TIME," + Name);//poslje ime v excel tabelo
Serial.print(",");
Serial.println(Number); //poslje zaporedno stevilko v excel tabelo
digitalWrite(GreenLed,HIGH);
digitalWrite(RedLed,LOW);
digitalWrite(Buzzer,HIGH);
delay(30);
digitalWrite(Buzzer,LOW);
Serial.println("SAVEWORKBOOKAS,Names/WorkNames");
}
delay(1000);
cont:
delay(2000);
digitalWrite(GreenLed,LOW);
digitalWrite(RedLed,LOW);

//ob prihodu vseh dijakov se excel tabela shrani in excel zapre(dodatno)-npr. 5 kartic n==5
//if(n==2){

// Serial.println("FORCEEXCELQUIT");
// }
,

```

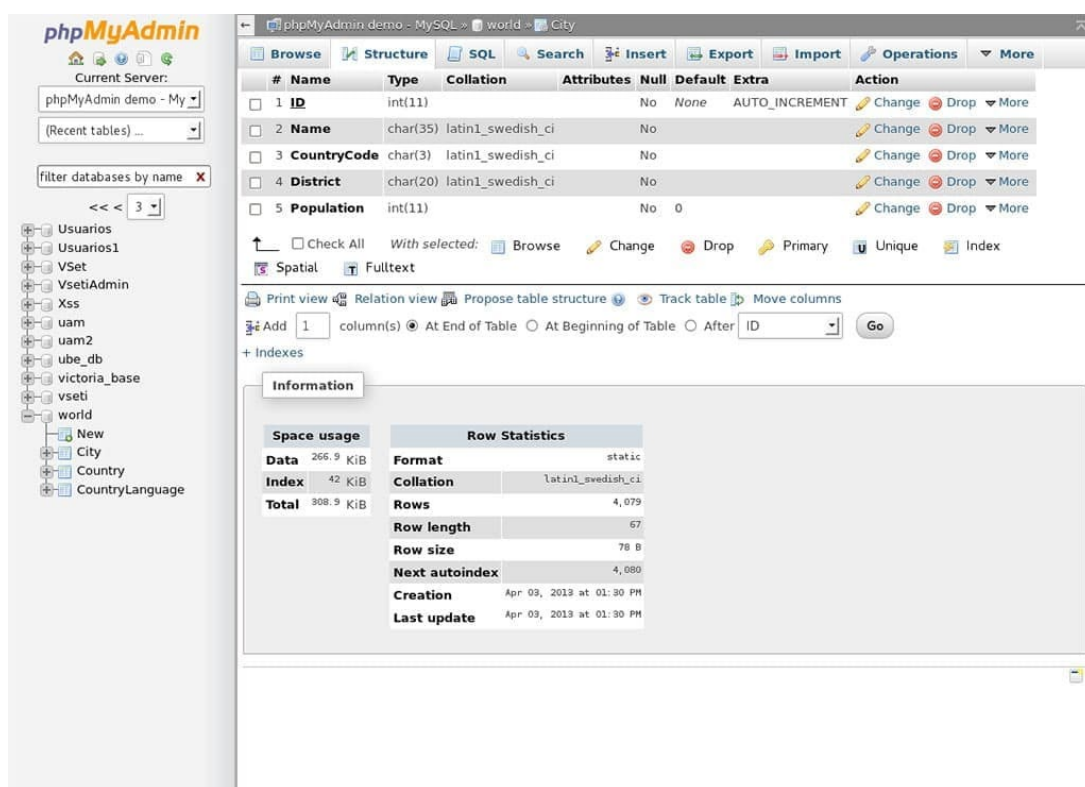
---

Slika 32: Program [41]

# MOŽNOSTI IZBOLJŠAVE

## *Povezava z podatkovno bazo*

Možno bi bilo povezati program s podatkovno bazo in s tem še olajšati delo. S povezavo bi bilo mogoče shranjevati podatke in jih kasneje uporabiti. Sicer je rešitev z Excelom primerna vendar ima pomanjkljivosti.



Slika 33: PHpMyAdmin [42]

## *Povezava z eAsistentom*

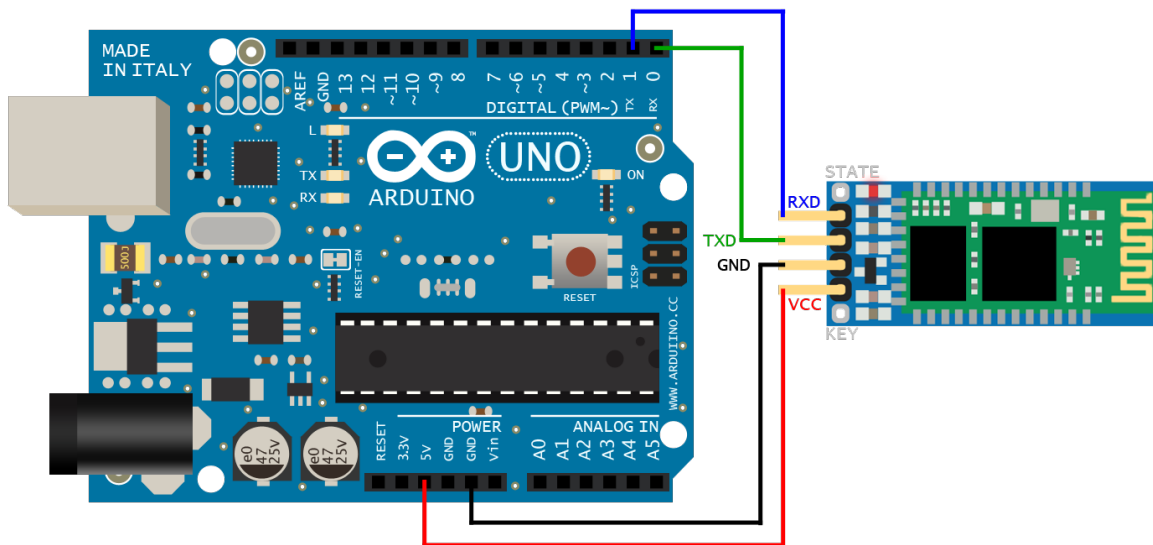
Če bi program povezali z eRedovalnico v eAsistentu, bi program lahko podatke namesto beleženja v Excel vpisoval direktno kot manjkajoče in s tem popolnoma odpravil ročno vpisovanje. S tem bi odpravili ogromno porabo časa, saj veliko profesorjev porabi več minut, da na začetku ure vpiše manjkajoče dijake.



Slika 34: eAsistent [43]

### *Bluetooth povezava*

Na ploščo bi lahko dodali modul bluetooth, ki bi se brezžično povezal z računalnikom, namesto da bi bila plošča Arduino povezana z računalnikom preko kabla. S tem bi odpravili kable in vrtanje ter lažje ustvarili povezavo z računalnikom.



Slika 35: Modul bluetooth povezan z ploščo Arduino Uno [44]

### *Prstni odtis*

Kartice bi lahko zamenjali s čitalcem za prstne odtise. Mogoče je namreč, da bi nekdo svojo kartico posodil komu drugemu, s čimer bi bila prisotnost ponarejena. To bi bilo seveda v nasprotju z namenom programa. Trenuten problem je, da se biometrija ne sme uporabljati. Prepovedana pa je zato, saj bi s tem šle zbirale osebne podatke. Torej bo v prihodnosti možna uporaba prstnih čitalcev, le če bo možno zbiranje osebnih podatkov.





Slika 36: Čitalec prstnih odtisov [45]

# UGOTOVITVE IN SKLEPI

## *1 Hipoteza*

Z uporabo RFID značk na šoli bi bilo beleženje dijakov hitrejše, kot beleženje prisotnosti s strani profesorjev.

- Prvo hipotezo smo potrdili, saj čitalec potrebuje manj kot 1 sekundo, da razbere podatke z značke (kartice) med tem ko bi profesor potreboval več kot 1 sekundo, saj bi moral izprašati dijake po njihovi prisotnosti.

## *2 Hipoteza*

Z uporaba RFID značk na šoli bi bilo beleženje dijakov bolj natančno, kot beleženje prisotnosti s strani profesorjev.

- Drugo hipotezo smo zavrgli, saj bi lahko dijak uporabil dve znački (kartici), s katerima bi zabeležil prisotnost drugega neprisotnega dijaka. Med tem ko bi profesor natančno zabeležil prisotnost dijakov.

## *3 Hipoteza*

Z uporabo prstnih odtisov, bi bilo beleženje prisotnosti dijakov pristnejše kot z RFID značko.

- Tretjo hipotezo smo delno potrdili, saj smo to predlagali kot možnost izboljšave. S tem bi lahko dijak zabeležil le lastno prisotnost, saj ima vsak človek edinstvene prstne odtise. Vendar zaradi zbiranja osebnih podatkov, se biometrije ne sme uporabljati.

## ZAKLJUČEK

Beleženje artiklov in izdelkov je dandanes izjemno pomemben proces, prav tako je pomembno preverjanje prisotnosti oseb in preverjanje njihove istovetnosti z osebami, za katere se izdajajo. S tem podjetja poskrbijo za svojo varnost in varnost zaposlenih.

Pri praktičnem delu raziskovalne naloge nam je pomagal profesor Damjan Erhatic ter nam priskrbel potrebne dele za izdelavo in nam predstavil program Arduino. Pri teoretičnem delu pa smo si pomagali s podatki, ki smo jih našli na svetovnem spletu.

Izvedeli smo, da obstaja veliko različnih vrst črtnih kod, RFID-značk in vrst prepoznave z biometrijo. Raziskali smo tudi, po katerem načelu delujejo ter kako in iz česa so izdelane. Najbolj nas je navdušila tehnologija RFID v trgovskem poslovanju, saj bo v prihodnosti mogoče vse črtne kode nadomestila prav ta tehnologija. Kupec bi lahko svoje izdelke prinesel v območje delovanja RFID-čitalnika, ta pa bi v hipu razbral seznam RFID-odzivnikov na izdelkih in poslal podatke v računalnik. Nato bi se izpisal račun. Po plačnem računu bi se odprla varnostna vrata, skozi katera bi kupec odšel. Takšne trgovine ne bi potrebovale trgovcev, le nekaj skladiščnikov, ki bi na police nosili nove izdelke.

Dejstvo je, da bo tehnologija izpodrinila številne poklice, saj je njeno delovanje cenejše in natančnejše ter lahko za razliko od človeške delovne sile deluje 24 ur na dan. Vendar pa se lahko zgodi napaka v sistemu, ki delovanje tehnologije zaustavi. To napako pa bo moral še vedno poiskati in rešiti človek oziroma njegovo znanje.

# VIRI

## *Literatura*

1. Interaktivni mediji. Pridobljeno 3. 2. 2022 s spletne strani  
[https://studentski.net/gradivo/ulj\\_ntf\\_nt1\\_im1\\_sno\\_skripta\\_1\\_del\\_2013\\_2014\\_01](https://studentski.net/gradivo/ulj_ntf_nt1_im1_sno_skripta_1_del_2013_2014_01)
2. RFID oznake oz. RFID tagi in primerjava s QR kodo. Pridobljeno 3. 2. 2022 s spletne strani <https://www.mave.si/rfid-oznake-oz-rfid-tag-i-in-primerjava-s-qr-kodo-27-07-2020.html>
3. RFID (radio frequency identification). Pridobljeno 3. 2. 2022 s spletne strani  
<https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>
4. What is RFID and how does RFID work? Pridobljeno 3. 2. 2022 s spletne strani  
<https://www.abr.com/what-is-rfid-how-does-rfid-work/>
5. DNK. Pridobljeno 3. 2. 2022 s spletne stran  
[https://sl.wikipedia.org/wiki/Deoksiribonukleinska\\_kislina](https://sl.wikipedia.org/wiki/Deoksiribonukleinska_kislina)
6. What is the difference between NFC and RFID? Pridobljeno 3. 2. 2022 s spletne strani  
<https://www.globalpaymentsintegrated.com/en-us/blog/2020/04/21/what-is-the-difference-between-nfc-and-rfid>
7. Prstni odtis. Pridobljeno 3. 2. 2022 s spletne strani  
[https://sl.wikipedia.org/wiki/Prstni\\_odtis](https://sl.wikipedia.org/wiki/Prstni_odtis)
8. Prepoznavanje obraza. Pridobljeno 18. 2. 2022 s spletne strani  
<https://sl.eyewated.com/kaj-je-prepoznavanje-obraza/>
9. NFC (Near Field Communication). Pridobljeno 18. 2. 2022 s spletne strani  
<https://www.gsmarena.com/glossary.php3?term=nfc>
10. Radiofrekvenčna identifikacija (RFID). Pridobljeno 18. 2. 2022 s spletne strani  
[https://leoss.si/strokovnjak\\_svetuje/29/radiofrekvencna\\_identifikacija\\_rfid/](https://leoss.si/strokovnjak_svetuje/29/radiofrekvencna_identifikacija_rfid/)
11. Kaj so brezstične ali RFID kartice? Pridobljeno 25. 2. 2022 s spletne strani  
<https://www.mave.si/kaj-so-brezsticne-ali-rfid-kartice-19-10-2020.html>
12. Najpogostejši RFID / NFC čipi za varno identifikacijo uporabnikov in plačevanje. Pridobljeno 25. 2. 2022 s spletne strani <https://www.mave.si/najpogostejsi-rfid-/nfc-cipi-za-varno-identifikacijo-uporabnikov-in-placevanje--07-09-2021.html>

13. Kaj je NFC? Pridobljeno 25. 2. 2022 s spletne strani <https://www.mave.si/kaj-je-nfc.html>
14. Elektromagnetno valovanje. Pridobljeno 25. 2. 2022 s spletne strani [https://sl.wikipedia.org/wiki/Elektromagnetno\\_valovanje](https://sl.wikipedia.org/wiki/Elektromagnetno_valovanje)
15. Vovčak, Z. (2006) Vpliv uporabe črtne kode na izvajanje poslovnih procesov- primer vipap Videm Krško d.d. [Diplomsko delo, Univerza v Ljubljani, Ekonomska fakulteta]. peFprints [http://www.cek.ef.uni-lj.si/u\\_diplome/vovcak2293.pdf](http://www.cek.ef.uni-lj.si/u_diplome/vovcak2293.pdf)
16. Anžič, M. (2005) Vloga biometričnih metod pri preprečevanju terorizma. [Diplomsko delo, Univerza v Ljubljani, Fakulteta za družbene vede]. peFprints <http://dk.fdv.uni-lj.si/dela/Anzic-Marko.PDF>
17. Likozar, M. (2017) Prepoznavna oseb na osnovi očesne šarenice. [Diplomsko delo, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko]. peFprints [http://eprints.fri.uni-lj.si/3848/1/63130139-MATIC\\_LIKOZAR-Prepoznavna\\_oseb\\_na\\_osnovi\\_o%C4%8Desne\\_%C5%A1arenice..pdf](http://eprints.fri.uni-lj.si/3848/1/63130139-MATIC_LIKOZAR-Prepoznavna_oseb_na_osnovi_o%C4%8Desne_%C5%A1arenice..pdf)
18. Noviba, G. (2009) Identifikacija oseb po glasu. [Diplomsko delo, Univerza v Mariboru, Fakulteta za varnostne vede]. peFprints <https://dk.um.si/Dokument.php?id=12740>
19. Žebovec, M. (2014) Tehnologiji RFID in NFC in njuna uporaba. [Diplomsko delo, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko]. Pefprints [http://eprints.fri.uni-lj.si/2696/1/63090152-MATEJ\\_%C5%BDEBOVEC-Tehnologiji\\_RFID\\_in\\_NFC\\_in\\_njuna\\_uporaba.pdf](http://eprints.fri.uni-lj.si/2696/1/63090152-MATEJ_%C5%BDEBOVEC-Tehnologiji_RFID_in_NFC_in_njuna_uporaba.pdf)

## Slike

- Slika 1 pridobljena 3. 2. 2022:  
[https://encryptedtbn0.gstatic.com/images?q=tbn:ANd9GcRhj2kv2COK9yLfTvSDAOfV18\\_n8tp7H0kBeA&usqp=CAU](https://encryptedtbn0.gstatic.com/images?q=tbn:ANd9GcRhj2kv2COK9yLfTvSDAOfV18_n8tp7H0kBeA&usqp=CAU)
- Slika 2 pridobljena 3. 2. 2022:  
[https://www.monitor.si/media/monitor/slike/arhivrevije/2014/06/Novice/\\_\\_\\_1200/noveteh-prstniotdis.jpg](https://www.monitor.si/media/monitor/slike/arhivrevije/2014/06/Novice/___1200/noveteh-prstniotdis.jpg)
- Slika 3 pridobljena 3. 2. 2022:  
<https://vashtvmir.ru/wpcontent/uploads/2014/11/df8eca131098d99818d776462925b9ab.jpg>
- Slika 4 pridobljena 3. 2. 2022:  
<https://openlab.si/wp-content/uploads/2019/01/Facial-recognition-931x423.jpg>
- Slika 5 pridobljena 3. 2. 2022:  
<https://www.researchgate.net/profile/Federico-Marangoni-2/publication/230294330/figure/fig2/AS:267508141785098@1440790319958/Sonograms-and-oscillograms-for-the-sounds-produced-by-a-Ceratophrys-ornata-larvae-at.png>
- Slika 6 pridobljena 3. 2. 2022:  
<https://www.asiarfid.com/wp-content/uploads/2020/11/What-is-RFID-1.jpg>
- Slika 7 pridobljena 3. 2. 2022:  
[https://www.sml.com/wp-content/uploads/2021/11/RFID\\_Labels\\_n\\_Packaging-scaled.jpg](https://www.sml.com/wp-content/uploads/2021/11/RFID_Labels_n_Packaging-scaled.jpg)
- Slika 8 pridobljena 3. 2. 2022:  
[https://podskalco.si/6\\_storage/Iso18000-6c-%C5%BEivine-sledenje-uhf-%C5%BEivali-uho-oznako-uploads\\_83055.jpeg](https://podskalco.si/6_storage/Iso18000-6c-%C5%BEivine-sledenje-uhf-%C5%BEivali-uho-oznako-uploads_83055.jpeg)
- Slika 9 pridobljena 18. 2. 2022:  
<http://docplayer.si/docs-images/111/195941695/images/41-0.jpg>
- Slika 10 pridobljena 18. 2. 2022:  
[https://paultan.org/image/2021/11/MYRFID\\_LANE-1.jpg](https://paultan.org/image/2021/11/MYRFID_LANE-1.jpg)

- Slika 11 pridobljena 18. 2. 2022:  
[https://www.hopelandrfid.com/js/htmledit/kindeditor/attached/20180208/20180208085840\\_58514.png](https://www.hopelandrfid.com/js/htmledit/kindeditor/attached/20180208/20180208085840_58514.png)
- Slika 12 pridobljena 18. 2. 2022:  
<https://dsplab.feri.um.si/wp-content/uploads/darko-6.png>
- Slika 13 pridobljena 18. 2. 2022:  
[https://www.monitor.si/media/monitor/slike/clanki/2019/11/rfid/\\_\\_1200/rfid.jpg](https://www.monitor.si/media/monitor/slike/clanki/2019/11/rfid/__1200/rfid.jpg)
- Slika 14 pridobljena 18. 2. 2022:  
[https://www.dafrfidtagsfactory.com/js/htmledit/kindeditor/attached/20200910/20200910174444\\_34616.jpg](https://www.dafrfidtagsfactory.com/js/htmledit/kindeditor/attached/20200910/20200910174444_34616.jpg)
- Slika 15 pridobljena 18. 2. 2022:  
<https://image.made-in-china.com/2f0j00hvFQGMWcbeqT/ID-Card-EM4550-.jpg>
- Slika 16 pridobljena 18. 2. 2022:  
[https://sc01.alicdn.com/kf/HTB1GiMZmm\\_I8KJy0Foq6yFnVXao/200510285/HTB1GiMZmm\\_I8KJy0Foq6yFnVXao.jpg\\_.webp](https://sc01.alicdn.com/kf/HTB1GiMZmm_I8KJy0Foq6yFnVXao/200510285/HTB1GiMZmm_I8KJy0Foq6yFnVXao.jpg_.webp)
- Slika 17 pridobljena 18. 2. 2022:  
[https://womanuntamed.com/uploads/n/nfc-in-the-phone-what-is-it-and-how-to-use-it/nfc-in-the-phone-what-is-it-and-how-to-use-it\\_1.jpg](https://womanuntamed.com/uploads/n/nfc-in-the-phone-what-is-it-and-how-to-use-it/nfc-in-the-phone-what-is-it-and-how-to-use-it_1.jpg)
- Slika 18 pridobljena 18. 2. 2022:  
<https://content.instructables.com/ORIG/FF1/8IZL/II6C38SV/FF18IZLII6C38SV.jpg?auto=webp>
- Slika 19 pridobljena 18. 2. 2022:  
[https://assets-global.website-files.com/5aa16619a722600001c19c3f/5b7dd26768c174bf3e1590df\\_peer-to-peer.jpg](https://assets-global.website-files.com/5aa16619a722600001c19c3f/5b7dd26768c174bf3e1590df_peer-to-peer.jpg)
- Slika 20 pridobljena 18. 2. 2022:  
[https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTPL\\_fXw339MU92bklxUyGeSTNN3XXGX6N7F5iMdupRK0YyV5UyK3NpE9OhxCNku\\_zUK4Q&usqp=CAU](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTPL_fXw339MU92bklxUyGeSTNN3XXGX6N7F5iMdupRK0YyV5UyK3NpE9OhxCNku_zUK4Q&usqp=CAU)
- Slika 21 pridobljena 18. 2. 2022:  
<https://dsplab.feri.um.si/wp-content/uploads/darko-3.png>

- Slika 22 pridobljena 18. 2. 2022:  
<https://logodownload.org/wp-content/uploads/2019/03/arduino-logo-0.png>
- Slika 23 pridobljena 25. 2. 2022:  
<https://arduinotogo.com/wp-content/uploads/2016/06/arduino-uno-labelled.png>
- Slika 24 pridobljena 25. 2. 2022:  
<https://lastminuteengineers.b-cdn.net/wp-content/uploads/arduino/RC522-RFID-Reader-Writer-Module-Pinout.png>
- Slika 25 pridobljena 25. 2. 2022:  
<https://circuits4you.com/wp-content/uploads/2018/10/RFID-Reader-RC522-interface-with-Arduino.jpg>
- Slika 26: avtorska
- Slika 27 pridobljena 25. 2. 2022:  
<https://zbotic.in/wp-content/uploads/2020/07/AI0079.1.jpg>
- Slika 28: avtorska
- Slika 29: avtorska
- Slika 30: avtorska
- Slika 31: avtorska
- Slika 32: avtorska
- Slika 33 pridobljena 25. 2. 2022:  
<https://localhost.me/assets/img/pages/phpmyadmin.jpg>
- Slika 34 pridobljena 25. 2. 2022:  
<https://www.oszrece.net/files/2020/05/eAsisent.jp>
- Slika 35 pridobljena 28. 2. 2022:  
[https://lh3.ggpht.com/-pnK3I1l-Qhw/T\\_wf75kTbwI/AAAAAAAAABkA/mRFDJ93tpbw/s1600/Arduino+Bluetooth.png](https://lh3.ggpht.com/-pnK3I1l-Qhw/T_wf75kTbwI/AAAAAAAAABkA/mRFDJ93tpbw/s1600/Arduino+Bluetooth.png)
- Slika 36 pridobljena 28. 2. 2022:  
<https://th.bing.com/th/id/OIP.R7KgcHatYkQKRxlqQzJNrQAAAA?pid=ImgDet&rs=1>