**RODZAJE SYSTEMÓW KONTROLI DOSTĘPU**

**PRZEGLĄD**

***Wstęp:***

Istnieje duża grupa rodzajów systemów kontroli dostępu. Omawiane systemy mogą występować w dowolnej kombinacji dlatego też ciężko jest wymienić je wszystkie. W przeglądzie zawarte są podstawowe rozwiązania spotykane najczęściej.  
  
Systemy kontroli dostępu możemy podzielić na dwie grupy:Obraz zawierający diagram

Opis wygenerowany automatycznie

***Fizyczne*** systemy kontroli polegają na fizycznym posiadaniu przedmiotu lub właściwości pozwalającej na uzyskanie dostępu. Oznacza to że bez określonej rzeczy – klucza nie jesteśmy w stanie uzyskać dostępu.

***Intelektualne*** systemy dostępu są zawarte w sferze umysłu człowieka, tzn. hasło ma taką formę że jego przechowanie możliwe jest w pamięci człowieka natomiast przekazanie hasła odbywać się może za pomocą jakiekolwiek interfejsu człowiek – urządzenie.

***Przegląd systemów kontroli dostępu fizycznych:***

1. System kontroli oparty o odczyt kart, przedmiotów za pomocą komunikacji falowej (magnetyczna, RFID itd.)

Systemy te opierają się na module odbiornika i nadajnika ( transponder ). Istnieje dosyć dużo odmian tego typu systemu. Głównie występuje tutaj czip, układ scalony zamknięty w postaci przedmiotu który jest w stanie komunikować się z układem dostępu. Zasada działania polega na komunikacji bezstykowej poprzez wysyłane fale radiowe, magnetyczne lub innego rodzaju.



Rysunek . Moduł dostępu z czytnikiem RFID

Tego rodzaju systemy są powszechnie stosowane w zamkniętych instytucjach gdzie istotne jest posiadanie dostępu na podstawie posiadanego stanowiska. Systemy te są również powszechne w miejscach publicznych czy siłowniach.



Rysunek . Popularny system odczytu kart w miejscu publicznym

Wadą tego rozwiązania są następujące:

- potrzeba posiadania fizycznie klucza dostępu

- możliwość zgubienia lub uszkodzenia klucza dostępu

- możliwość kradzieży klucza dostępu

1. System kontroli oparty na biometrii

Systemy te opierają się na kontroli dostępu za pomocą cech fizycznych użytkownika. Głównie spotykane to:

- rozpoznawanie twarzy

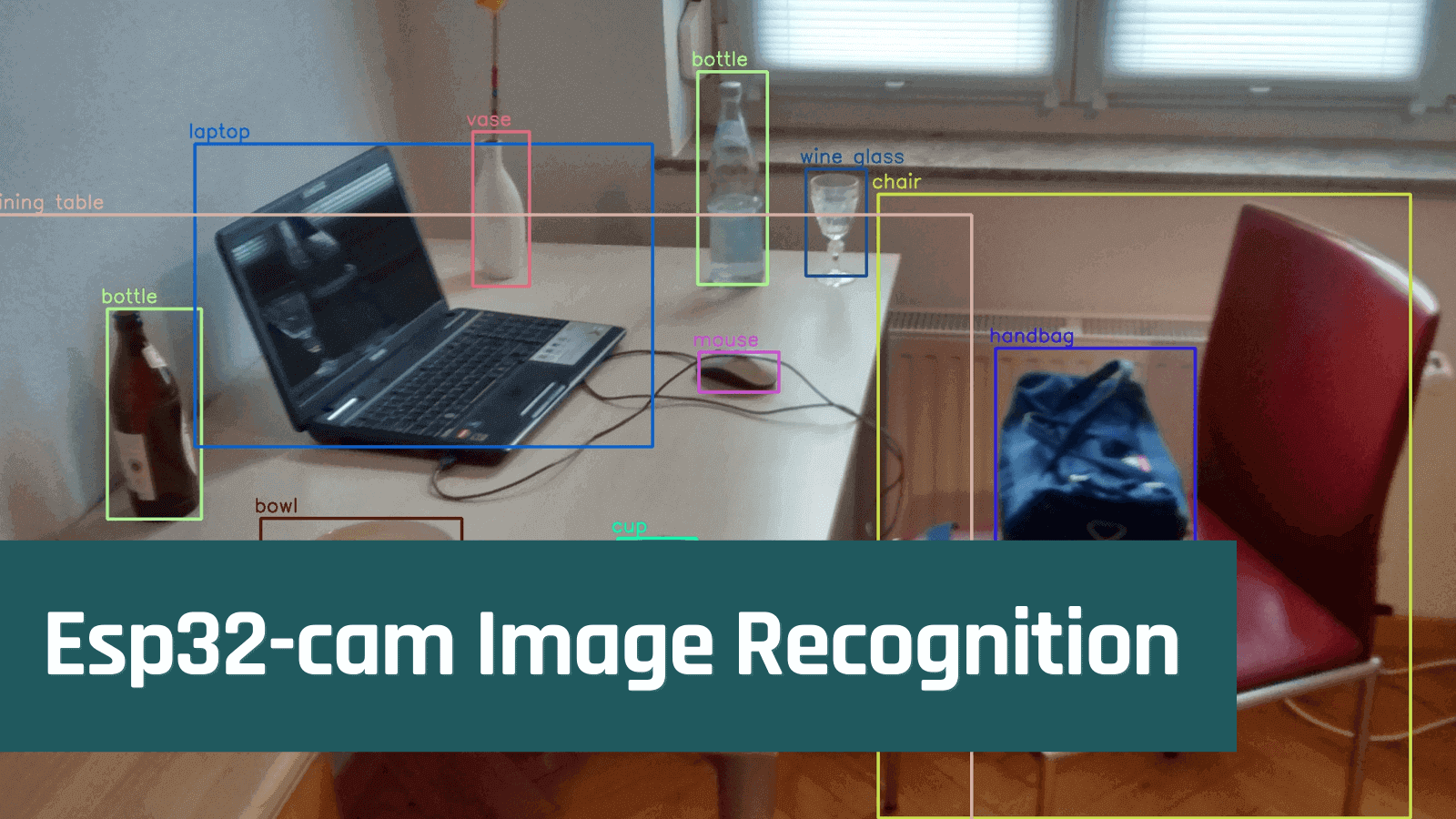
- rozpoznawanie odcisku palca

- rozpoznawanie głosu



Rysunek . System biometryczny dostępu za pomocą odcisku palca

Sposoby te, choć popularne w telefonach nie są często spotykane w miejscach publicznych lub instytucjach firmowych. Mierzone cechy są indywidualne dla każdego człowieka a przez to osobiste. Moduły realizujące wymienione wcześniej czynności są skomplikowane. Dużą zaletą tego systemu w porównaniu do poprzedniego jest fakt że takiego klucza dostępu nigdy nie zapomnimy oraz nie zgubimy, nie może być on też skradziony. Ciężko jest też włamać się do takiego systemu bez uprzedniej wiedzy użytkowników. Systemy te z racji na swoje zaawansowanie są trudniejsze do złamania choć słabe ogniwo w tym systemie może być przyczyną łatwego dostępu. Choć rzadko spotykane, są one stosowane przy dużym stopniu bezpieczeństwa. Przy dużym zaawansowaniu systemy te są trudne do sforsowania a przy tym przyjazne dla użytkowników.



Rysunek . System dostępu oparty na rozpoznawaniu twarzy

Systemy te wymagają dosyć dokładnego opracowania i opierają się na wykorzystaniu różnych zasad działania, algorytmów informatycznych , zasad optycznego zapisu informacji oraz analizie obrazu.

Wady rozwiązania:

- stosunkowo drogie moduły

- dedykowane pod mniejszą ilość osób

- skomplikowana zasada działania ( dostępu )

- brak możliwości zmiany klucza dostępu ( jedna cecha fizyczna osoby )

***Przegląd systemów kontroli dostępu intelektualnych:***

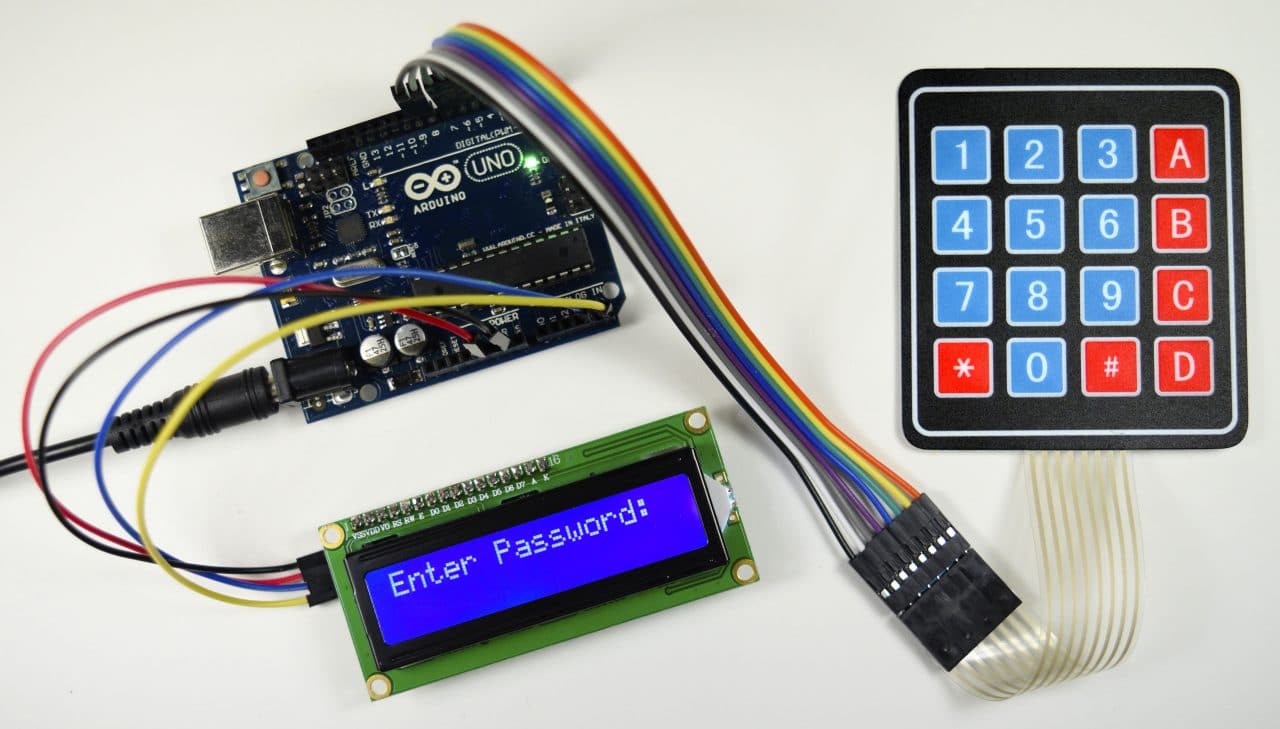
1. System dostępu oparty na kodzie alfanumerycznym

Systemy te są najpowszechniej stosowane. Łatwe w implementacji oraz stosunkowo bezpieczne. Jedynymi modułami potrzebnymi do realizacji tej metody dostępu są mikrokontroler zaprogramowany do odczytywania i porównywania haseł oraz moduł klawiatury służącej jako interfejs człowiek-maszyna.



Rysunek . System dostępu przez hasło alfanumeryczne

Istotnym modułem w tej kwestii jest również wyświetlacz poprawiający czytelność tego co dzieje się podczas podejmowania próby uzyskania dostępu.



Rysunek . System z dostępem alfanumerycznym na mikrokontrolerze Arduino

Choć te systemy są popularne i często stosowane to jednak mają kilka istotnych wad:

- krótkie hasła są stosunkowo słabe

- im dłuższe i silniejsze hasło tym dłuższy czas wprowadzania go

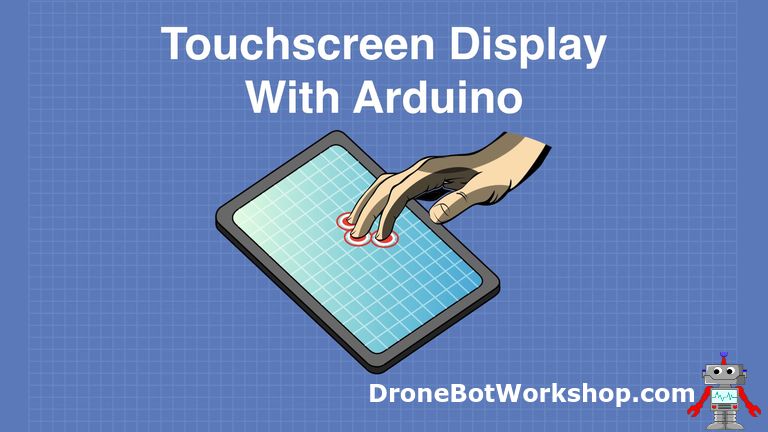
- duża szansa wycieku hasła na zewnątrz

- nie do zastosowania w miejscach publicznych bez sprzężenia z innym wspierającym systemem

- długie hasła ciężko się zapamiętuje

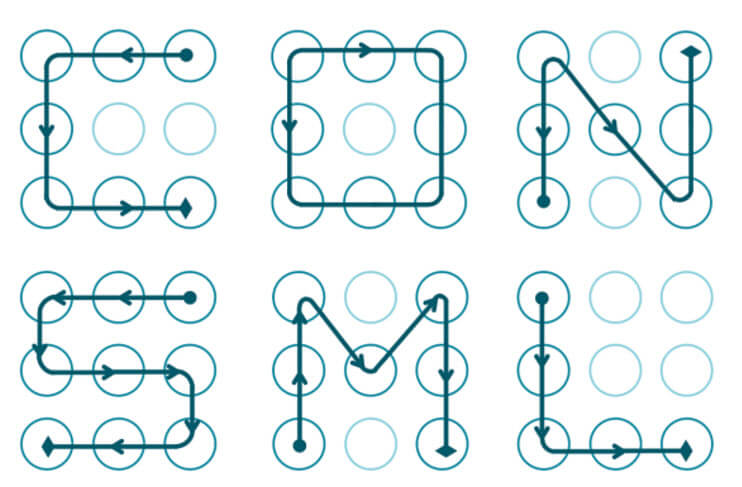
1. System dostępu za pomocą haseł symbolicznych

System ten można porównać do systemu z dostępem alfanumerycznym. W tym przypadku nie obędzie się bez wyświetlacza dotykowego na którym użytkownik wprowadza hasła w postaci graficznej.



Rysunek . System dostępu z wykorzystaniem ekranu dotykowego

Systemy dostępu graficznego muszą być uniwersalne i znormalizowane w taki sposób aby każdy użytkownik bez względu na swoje umiejętności motoryczne był w stanie powtórzyć dane hasło. Są rzadko stosowane w miejscach publicznych i instytucjach z racji na niedużą różnicę w zaletach.



Wady takiego systemu są następujące:

- kosztowny w implementacji

- wrażliwy na uszkodzenia

- nie wprowadza dodatkowego stopnia bezpieczeństwa

- łatwy do podglądnięcia

- skomplikowane symbole mogą być trudne do zapamiętania

Wybór rodzaju systemu:

Na podstawie wymienionych tutaj informacji zdecydowaliśmy się na zaprojektowanie i wykonanie **systemu biometrycznego opartego o rozpoznawanie twarzy oraz odcisku palca**. Motywujemy to tym że system będzie pracował w małym gronie osób a idealnie się do tego nadaje ( małe ryzyko złamania zabezpieczeń ). Dodatkowo system ten jest szybki pod względem udzielania dostępu oraz przyjazny dla użytkownika. Realizacja go pozwala na dopracowanie i eksperymentację, co nie jest potrzebne w przypadku innych rozwiązań. Wreszcie należy wspomnieć że system ten jest innowacyjny i posiada wiele korzystnych cech.