Zbigniew Kasprzyk[1], Wojciech Wawrzyński[2], Mirosław Siergiejczyk[3]
Politechnika Warszawska Wydział Transportu Zakład Telekomunikacji w Transporcie

Model symulacyjny Systemu Kontroli Dostępu stosowanego w bazach logistycznych

1. WSTĘP

Elektroniczne systemy bezpieczeństwa coraz częściej stosuje się w obiektach mających znaczenie strategiczne [1]. W bazach logistycznych bardzo istotną problematyką jest zagadnienie zapewnienia bezpieczeństwa ładunków i obsługi logistycznej. Istotne staje się zatem wprowadzenie rozwiązań, które ograniczą dostęp osób do pomieszczeń i obszarów magazynowych w których znajdują się cenne ładunki. W artykule przedstawiono model symulacyjny Systemu Kontroli Dostępu (SKD) [2] w środowisku Matlab/Simulink. W niniejszym opracowaniu przedstawiono model symulacyjny Systemu Kontroli Dostępu mający za zadanie identyfikację osób uprawnionych do przekroczenia granicy obszaru zastrzeżonego oraz umożliwienie im wejścia lub wyjścia z pomieszczenia, niedopuszczenia do przejścia przez osoby nieuprawnione granicy obszaru zastrzeżonego, wytworzenie sygnału alarmowego informującego o próbie przejścia osoby nieuprawnionej przez granicę obszaru zastrzeżonego.

2. SYSTEM KONTROLI DOSTĘPU

System kontroli dostępu jest to zespół wzajemnie powiązanych urządzeń elektronicznych oraz mechanicznych, których działanie ma na celu ograniczenie użytkownikom (całkowite lub w określonym czasie) dostępu do stref tego systemu. Identyfikowanie użytkowników przez system kontroli dostępu zależny jest od zastosowanego typu urządzenia identyfikującego. Użytkownik, który chce przejść przez przejście kontrolowane, musi potwierdzić swoją tożsamość. Może to uczynić np. poprzez przyłożenie karty zbliżeniowej, podanie kodu lub pozwolenie na odczytanie cechy biometrycznej [2]. Interfejs przesyła odczytaną informację do centrali kontroli dostępu, gdzie zostaje ona porównana z wcześniej zaprogramowanymi i zapamiętanymi danymi użytkownika. Jeśli jest ona zgodna, to poprzez interfejs przejścia kontrolowanego następuje uruchomienie aktywatorów przejścia (np. otwarcie zamka elektrycznego czy włączenie elektrycznego napędu otwierającego drzwi). Jeśli informacja nie jest zgodna z zarejestrowanymi wcześniej danymi, to użytkownik nie może przejść, ponieważ nie nastąpi uruchomienie aktywatorów przejścia. W systemie kontroli dostępu są także czujki, które określają, czy drzwi zostały zamknięte po przejściu uprawnionej osoby albo czy nie zostały otwarte w sposób niedozwolony (np. siłowy). W systemie może występować także moduł komunikacji z innymi centralami kontroli dostępu i innymi systemami zarządzania bezpieczeństwem budynku.

Systemy kontroli dostępu można podzielić:

a) ze względu na funkcję:
   - kontrola obszaru (grupa pomieszczeń),
   - kontrola pomieszczenia,
b) ze względu na wyposażenie:
   - przejście kontrolowane jednostronnie,
   - przejście kontrolowane dwustronnie.

Przejście kontrolowane zazwyczaj jest wyposażone w:

- czytnik (coraz częściej biometryczny),

[1] zka@wt.pw.edu.pl
[2] wwa@wt.pw.edu.pl
[3] msi@wt.pw.edu.pl

- czujki stanu skrzydła drzwi,
- przycisk otwarcia,
- przycisk ewakuacyjnego otwarcia drzwi (wymagania ppoż.),
- element ryglujący (np. rygiel, zwora, zamek),
- samozamykacz (jednofazowy lub dwufazowy),
- pochwyt (pochwyty).

Obecnie w systemach kontroli dostępu coraz częściej stosuje się biometrię [3,4]. Pozwala ona na precyzyjną identyfikację osób dzięki sprawdzeniu ich niepowtarzalnych, charakterystycznych cech anatomicznych. Sprawdzane mogą być m.in.:

- geometria dłoni,
- linie papilarne,
- geometria twarzy,
- geometria ucha,
- geometria ust,
- budowa oka (cechy charakterystyczne tęczówki i siatkówki oka),
- układ żył nadgarstka,
- barwa głosu.

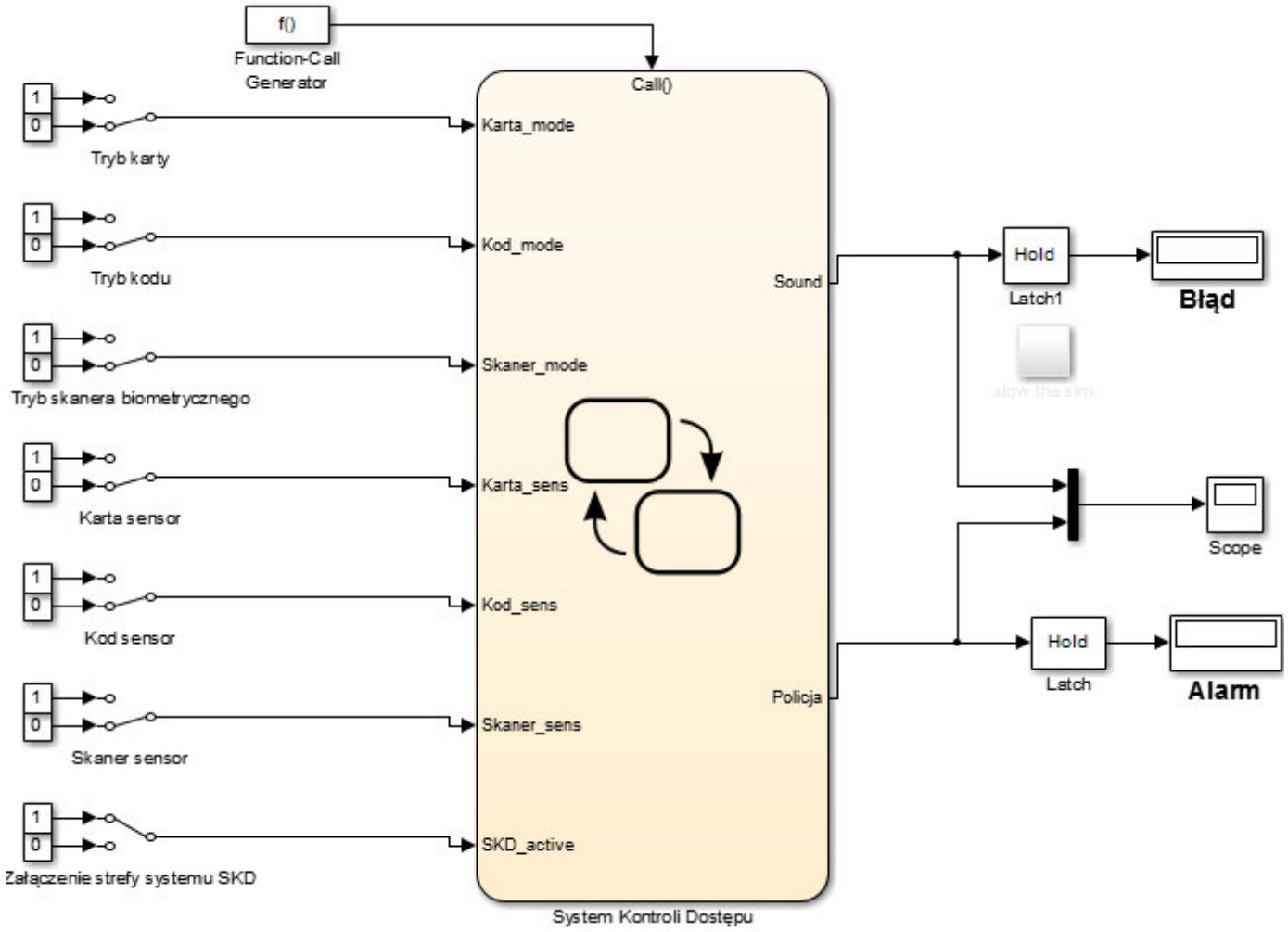
Do cech behawioralnych można zaliczyć m.in.:

- mowę,
- ruch ust,
- ruch gałki ocznej,
- pismo,
- chód.

Czytniki biometryczne znalazły wiele zastosowań. W systemach kontroli dostępu są stosowane już od lat siedemdziesiątych ubiegłego wieku. Początkowo (ze względu na wysokie koszty) instalowano je tylko w systemach przeznaczonych dla obiektów wymagających specjalnych zabezpieczeń gwarantujących wysoki poziom bezpieczeństwa. Dzięki bardzo szybkiemu rozwojowi technologii mikroprocesorowych układów elektronicznych w ostatnich latach, a przez to tańszym produktom, cena czytników biometrycznych zdecydowanie obniżyła się, a ich precyzja i niezawodność działania bardzo wzrosły. Dzięki temu można stosować je w wielu systemach przeznaczonych dla różnych odbiorców.

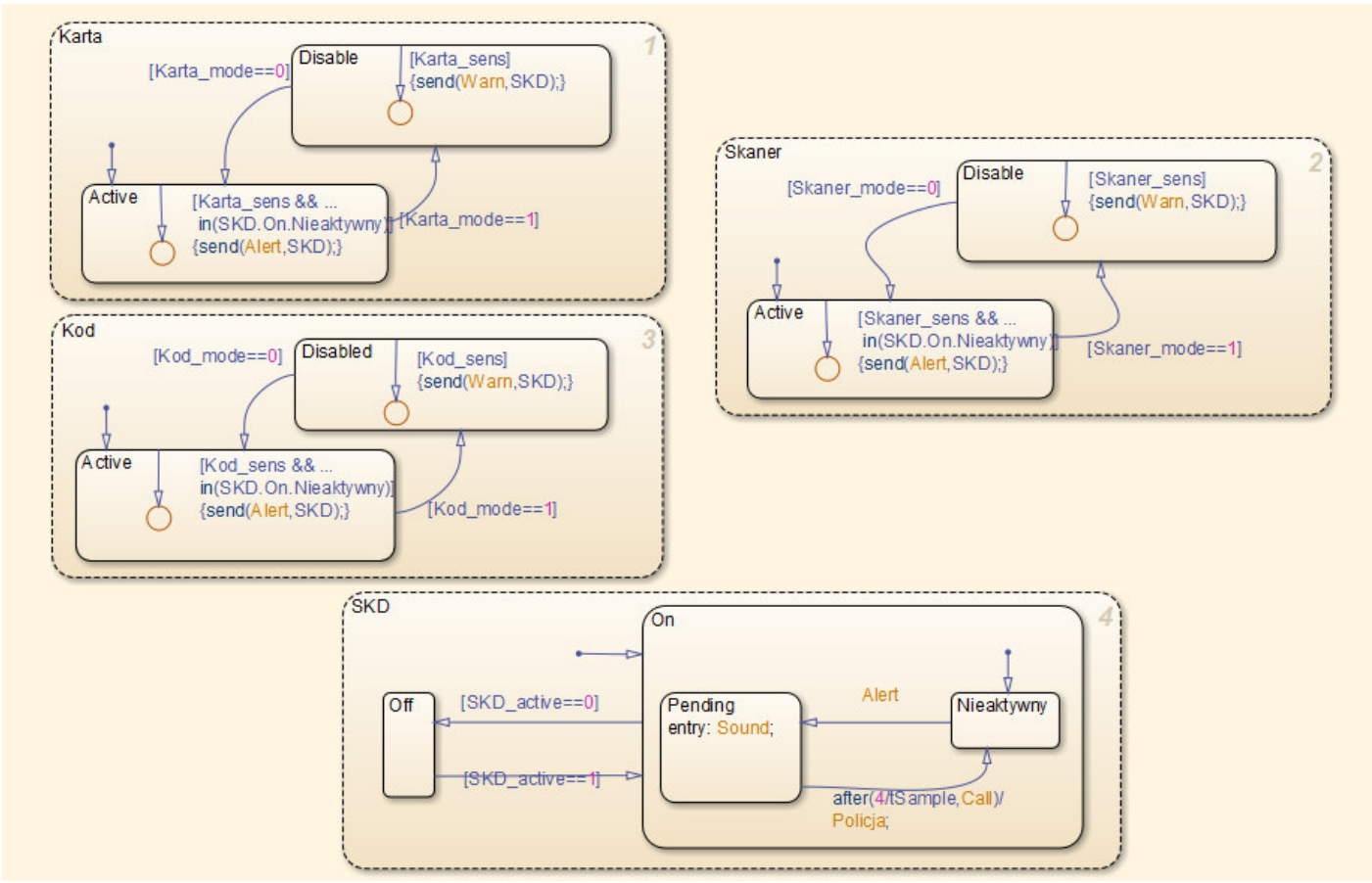
3. Model symulacyjny Systemu Kontroli Dostępu w środowisku Matlab/Simulink

Model symulacyjny systemu kontroli dostępu został sporządzony w środowisku Matlab/Simulink z wykorzystaniem pakietu stateflow, czyli wykorzystując diagramy stanu. Model został wykonany z wykorzystaniem przykładu [5] zaprezentowanego w środowisku Matlab/Simulink. Model symulacyjny systemu reprezentowany za pomocą diagramów stanu przedstawiono na rysunku 1 i 2. Na rysunku 1 przedstawiono elementy modelu symulacyjnego realizujące zadania opisywanego systemu kontroli dostępu. Do wejścia podsystemu (ang. *subsystem*) będącego diagramem stanów (ang. *Stateflow charts*) podłączone są bloki realizujące funkcję przełącznika ustawiającego stałe wartości zmiennych binarnych określających stan elementów systemu. W systemie kontrola dostępu realizowana jest za pomocą trzech elementów: karty zbliżeniowej, manipulatora umożliwiającego wpisanie kodu oraz skanera biometrycznego sprawdzającego niepowtarzalne, charakterystyczne cechy anatomiczne użytkownika systemu. Działanie diagramu stanów jest synchronizowane w każdym kroku symulacji za pomocą bloku *Function-Call Generator*. W bloku tym określony jest czas trwania próbki oraz ilość iteracji w których realizowana jest symulacja w każdym z diagramu stanów znajdującym się w bloku subsystemu.



Rys. 1. Model symulacyjny systemu SKD w środowisku Matlab/Simulink
Źródło: opracowanie własne z wykorzystaniem [5].

Na rysunku 2 przedstawiono właściwy diagram stanów opisujący zmiany stanu obiektu w postaci SKD pod wpływem działania operacji zewnętrznych w postaci zmian stanów elementów systemu: karty zbliżeniowej, manipulatora oraz skanera biometrycznego. Stany karty, manipulatora i skanera biometrycznego w każdym kroku symulacji odczytują wartości binarne zmiennych wprowadzanych na wejście do diagramu stanów. Wartości te reprezentują stany poszczególnych elementów systemu. W przypadku gdy wartość binarna sensora jest w stanie wysokim oznacza to że sensor będący składową systemu kontroli dostępu jest aktywny, w przeciwnym wypadku oznacza to błąd czyli próbę identyfikację użytkownika przy nieaktywnym trybie działania sensora. Wartości binarne trybów pracy elementów systemu określają ich stan. W przypadku gdy stan trybu pracy elementów jest w stanie wysokim oznacza to poprawną identyfikację użytkownika, w przeciwnym wypadku brak identyfikacji i uruchomienie alarmu w systemie. Stan nr 4 w diagramie stanów (rysunek 2) w każdym kroku symulacji odczytuje stan strefy systemu SKD. W przypadku gdy strefa detekcji jest załączona (wartość zmiennej ma stan wysoki) oznacza to aktywność działania systemu kontroli dostępu w bazie logistycznej, w przeciwnym wypadku strefa jest nieaktywna. Dodatkowo gdy stan załączonego alarmu nie zostanie zdezaktywowany przez użytkownika systemu w czasie określonym jako 4/t*(krok symulacji) wtedy system powiadomi odpowiednie służby porządkowe (policja, straż pożarna, itd.).



Rys. 2. Diagram stanów opisujący zmiany stanu obiektu Systemu Kontroli Dostępu pod wpływem działania operacji zewnętrznych realizowanych przez elementy systemu

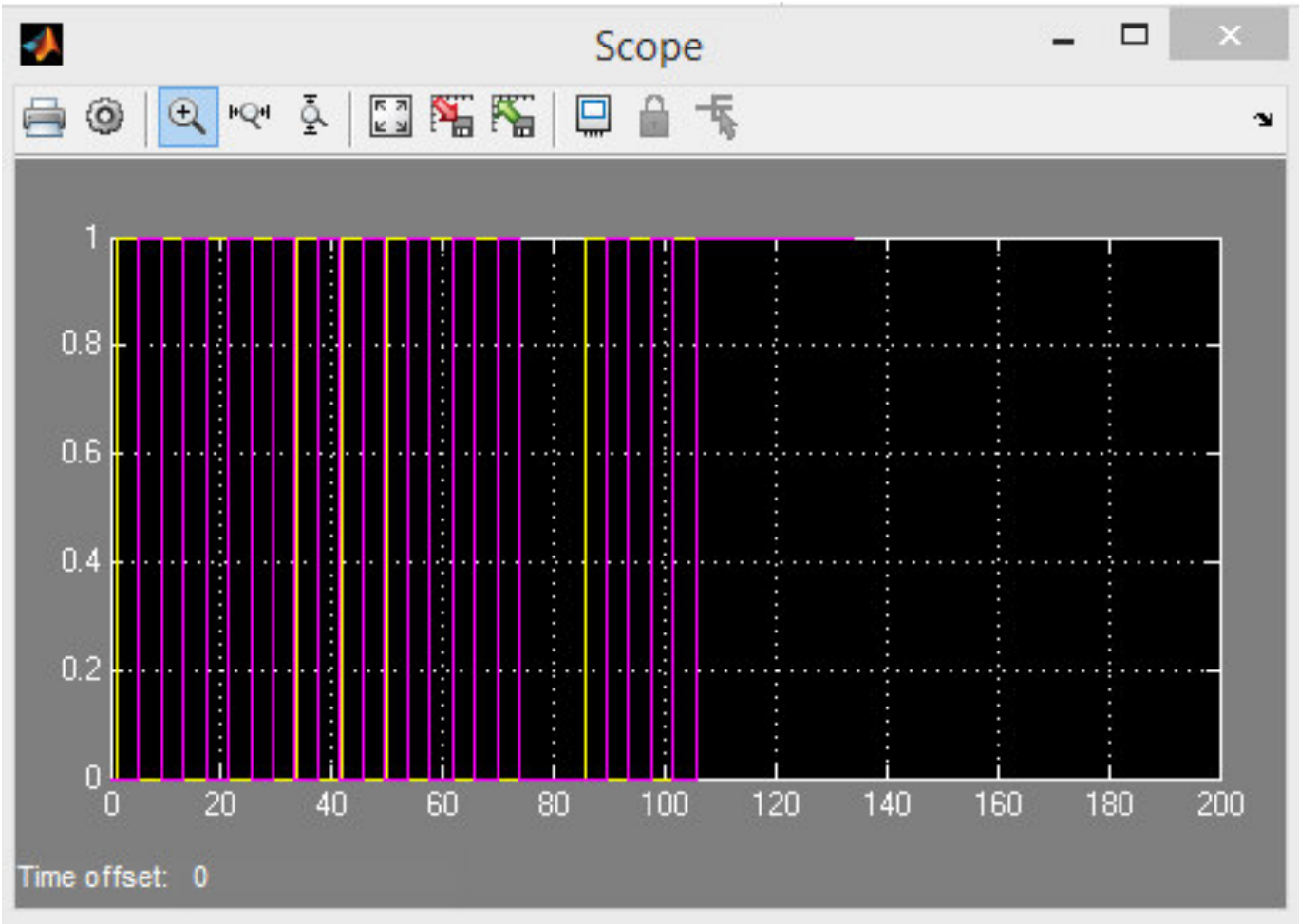
Źródło: opracowanie własne.

Wyniki działania modelu symulacyjnego Systemu Kontroli Dostępu zaprezentowano w postaci wykresów czasowych zaprezentowanych w bloku (ang. scope).

Na wykresie na rysunku 3 zaprezentowano stany wyjściowe systemu SKD w zależności od zasymulowanej sytuacji działania poszczególnych jego elementów. Na osi pionowej zaprezentowano stan załączenia sygnału alarmowego w systemie SKD natomiast na osi poziomej przedstawiono czas symulacji w postaci ilości kroków symulacji. Symulacja trwała 200 kroków symulacji, gdzie stan wysoki na wykresie oznacza załączenie sygnału alarmowego w systemie SKD i po określonym czasie gdy alarm nie został zdezaktywowany powiadamiane były odpowiednie służby interwencyjne na miejsce zdarzenia. Po okresie 100 kroków symulacji system kontroli dostępu poprawnie identyfikował użytkownika systemu.

4. PODSUMOWANIE I WNIOSKI

W artykule zaprezentowano zagadnienia związane z Systemem Kontroli Dostępu mogącym mieć zastosowanie w bazach logistycznych. Przedstawiono model symulacyjny Systemu mający za zadanie identyfikację osób uprawnionych do przekroczenia granicy obszaru zastrzeżonego oraz umożliwienie im wejścia lub wyjścia z pomieszczenia, niedopuszczenia do przejścia przez osoby nieuprawnione granicy obszaru zastrzeżonego, wytworzenie sygnału alarmowego informującego o próbie przejścia osoby nieuprawnionej przez granicę obszaru zastrzeżonego. Analiza działania tego systemu umożliwi w dalszych badaniach tego zagadnienia na uwzględnienie kosztu zakupu i eksploatacji tego systemu.



Rys. 3. Wykres czasowy stanów wyjściowych systemu SKD
Źródło: opracowanie własne.

Streszczenie

W artykule zaprezentowano zagadnienia związane z Systemem Kontroli Dostępu stosowanym w bazach logistycznych. Przedstawiono model symulacyjny Systemu mający za zadanie identyfikację osób uprawnionych do przekroczenia granicy obszaru zastrzeżonego oraz umożliwienie im wejścia lub wyjścia z pomieszczenia, niedopuszczenia do przejścia przez osoby nieuprawnione granicy obszaru zastrzeżonego, wytworzenie sygnału alarmowego informującego o próbie przejścia osoby nieuprawnionej przez granicę obszaru zastrzeżonego. Analiza działania tego systemu umożliwi w dalszych badaniach tego zagadnienia na uwzględnienie kosztu zakupu i eksploatacji tego systemu.

Słowa kluczowe: system kontroli dostępu, elektroniczne systemy bezpieczeństwa, model symulacyjny SKD.

The simulation model of access control system used in logistics bases

Abstract

The article presents the issues related to the Access Control System used in logistics bases. The model of the simulation system with the task of identifying the persons authorized to cross the border of the reserved area and enable them to enter or exit the premises, to prevent unauthorized crossing the border of the re-served area, producing an alarm signal indicating that an unauthorized person attempt to pass through the border a reserved area. This will allow further study of this issue to take into account the cost of purchasing and operating the system.

Key words: access control system, electronic security systems, simulation model SKD.

LITERATURA

[1] Hołyst B., „Terroryzm. Tom 1 i 2”. Wydawnictwa Prawnicze LexisNexis, Warszawa 2011.
[2] Siergiejczyk M., Rosiński A., „Analiza funkcjonalna Systemu Kontroli Dostępu w aspekcie bezpieczeństwa systemów telematycznych”, XL Zimowa Szkoła Niezawodności, Szczyrk 2012.
[3] Dunstone T., Yager N., Biometric System and Data Analysis, Springer, 2009.
[4] Tistarelli M., Li S Z., Chellappa R., Handbook of Remote Biometrics for Surveillance and Security, Springer-Verlag, 2009.
[5] http://www.mathworks.com/help/stateflow/examples/modeling-a-security-system.html.