STUDIA INFORMATICA 2012
Volume 33 Number 2B (106)

Witold WABIK
Politechnika Wrocławska

SYSTEM MONITORINGU Z AUTOMATYCZNYM WYKRYWANIEM POTENCJALNYCH ZAGROŻEŃ

Streszczenie. Praca zawiera opis systemu monitoringu budynku. System wyposażony został w moduł sztucznej inteligencji, pozwalający na rozpoznanie widocznych na zdjęciach kamer osób. System umożliwia wykrycie zagrożeń w czasie rzeczywistym oraz analizę zarejestrowanych zdarzeń w celu ich wyjaśnienia.

Słowa kluczowe: monitoring, hurtownia danych, detekcja twarzy, identyfikacja twarzy

MONITORING SYSTEM TO DETECT POTENCIAL DANGEROUS SITUATIONS

Summary. Publication contains description of building monitoring system. System has AI module to allow it to identify people on camera images. System detects danger situations in real-time and allows user to analyze recorded events.

Keywords: monitoring, data warehouse, detecting faces, identify faces

1. Geneza problemu

1.1. Zdefiniowanie problemu

Monitoring wideo stał się w ostatnich latach jednym z podstawowych narzędzi zapewnienia bezpieczeństwa. Bezinwazyjność monitoringu prowadzonego przy użyciu kamer powoduje, że mogą być instalowane praktycznie wszędzie, nie powodując uciążliwości dla obserwowanych osób.

Użycie monitoringu pozwala szybko zareagować na niebezpieczne zdarzenia oraz na przeprowadzenie analizy po fakcie, pozwalające na lepsze zrozumienie zarejestrowanych

zdarzeń. Implementacja mechanizmów powiadamiania usuwa potrzebę utrzymywania ochroniarza przez całą dobę w budynku – system wzywałby go jedynie w przypadku identyfikacji zagrożenia i bezpośrednio w dane miejsce.

W założeniu system ma umożliwiać wykrywanie potencjalnych zagrożeń niesionych przez osoby zidentyfikowane w budynku. W przeciwieństwie do identyfikacji osób na postawie kodu DNA lub obrazu siatkówki oka, identyfikacja na postawie obrazu kamer monitoringu ma pewne problemy z dokładnością rozpoznania. Bliźniacy jednojajowi są dla tej metody nierozróżnialni. Nie ma też możliwości identyfikacji osób z twarzami w dużej mierze zakrytymi. Dlatego w przypadku zabezpieczania ważnych obiektów tworzony system nie mógłby być jedynym systemem zabezpieczenia, a musiałby być jedynie systemem wspierającym.

Poza wykrywaniem w czasie rzeczywistym system powinien umożliwiać gromadzenie danych i ich późniejszą szczegółową analizę. Otwartym pytaniem pozostaje jednak, w jakim stopniu powinna być możliwa analiza osobistych danych osób monitorowanych, aby nie naruszyć ich prywatności.

1.2. Rodzaje zagrożeń

Zagrożenia bezpieczeństwa osób oraz mienia pozostającego w budynkach można podzielić ze względu na czas ich analizy – na aktualne i minione. Od typu zagrożenia zależeć będzie, jakie działania umożliwi system w celu neutralizacji zagrożenia.

Zagrożenia aktualne powinny być przez system identyfikowane w czasie rzeczywistym, tak aby, po poinformowaniu odpowiednich służb, możliwa była reakcja na nie (w szczególności ich zażegnanie).

Zagrożenia minione powinny zostać, za pomocą systemu, dogłębnie zanalizowane. Celem analizy jest zrozumienie zagrożenia (kto je spowodował i dlaczego) oraz zapobiegnięcie ponownemu nadejściu zagrożenia (np.: przez ujęcie sprawcy przestępstwa).

W systemie monitoringu budynku kluczową rolę odgrywa zarządzanie dostępem w czasie rzeczywistym. Każda z osób obecnych w budynku ma przydzielone uprawnienia do przebywania w poszczególnych częściach budynku. Uprawnienia te mogą być ograniczone czasowo, np. pracownicy etatowi mogą przebywać w budynku tylko w godzinach pracy.

Głównym zadaniem przy analizie już dokonanych niepożądanych zdarzeń jest odnalezienie osób odpowiedzialnych za nie. Dopiero wtedy można wobec kogoś wysunąć konsekwencje (albo upomnienie, jeżeli przewinienie było małe, albo nawet więzienie, w przypadku zdarzeń o charakterze kryminalnym). Dlatego podstawową analizą, jaką powinien umożliwiać system, jest przedstawienie listy osób widzianych przez kamery monitoringu w miejscu i czasie zdarzenia.

Istotne przy analizie minionych zdarzeń jest odkrycie osób pomagających w realizacji niepożądanych zdarzeń. Po odnotowaniu, np. kradzieży, system powinien pomóc w ujęciu sprawcy (albo przez złapanie go „na gorącym uczynku", albo przez wyznaczenie listy świadków). Ale sprawca nie musi działać sam. Może się okazać, że druga osoba chodzi przed zdarzeniem, dając sprawcy informację, w jakich miejscach znajdują się cenne rzeczy. Analiza podobnych zdarzeń powinna wykazać, które osoby widziane były, we w miarę równych odstępach czasu, przed wybranymi zdarzeniami. Byłyby to osoby podejrzane o współpracę.

W budynkach, w których prowadzone są rozmaite spotkania, powstaje kolejne zagrożenie. Osoby, niekoniecznie dbające o sprzęt, na którym pracują (np. w salach komputerowych na uczelni), mogą prowadzić do jego usterek. Warto zbadać, po jakich spotkaniach pojawiła się informacja o niedziałającym wyposażeniu. Możliwe jest, że spotkania łączyć będzie osoba prowadzącego, który nie dość bacznie kontroluje podopiecznych. Może się jednak okazać, że na każdym spotkaniu była ta sama osoba, której jedynym celem było zniszczenie sprzętu. Pomocne może okazać się porównanie list osób zapisanych na spotkanie z listą osób zarejestrowanych przez system monitoringu.

W przypadku gdy zarządzona zostanie ewakuacja budynku (np. podczas pożaru), służby ratunkowe powinny mieć możliwość sprawdzenia, czy ktoś w budynku został, a jeżeli tak, to w jakim jego miejscu.

Wpływ na bezpieczeństwo ma z pewnością właściwy wybór służby ochraniającej własność. Analizy, mające wyłonić firmę gwarantującą najlepszą ochronę, powinny wziąć pod uwagę niekorzystne zdarzenia, którym nie zapobiegły działania firmy. Mogą to być zarówno popełnione przestępstwa, jak i liczba osób, które uzyskały nieuprawniony dostęp do różnych miejsc budynku. Analizy powinny uwzględniać także ocenę pojedynczych pracowników ochrony.

2. Proponowane rozwiązanie

Proponowane jest użycie istniejących już systemów monitoringu, wraz z dodatkowym modułem umożliwiającym identyfikację osób widocznych na zdjęciach kamer monitoringu. Pozwoli to na automatyczne rejestrowanie obecności osób w budynku.

System rejestruje obecność osób w budynku oraz przechowuje zdjęcia zaobserwowanych osób, aby w razie wątpliwości, co do poprawnego rozpoznania ich przez system, możliwa była korekta automatycznej identyfikacji.

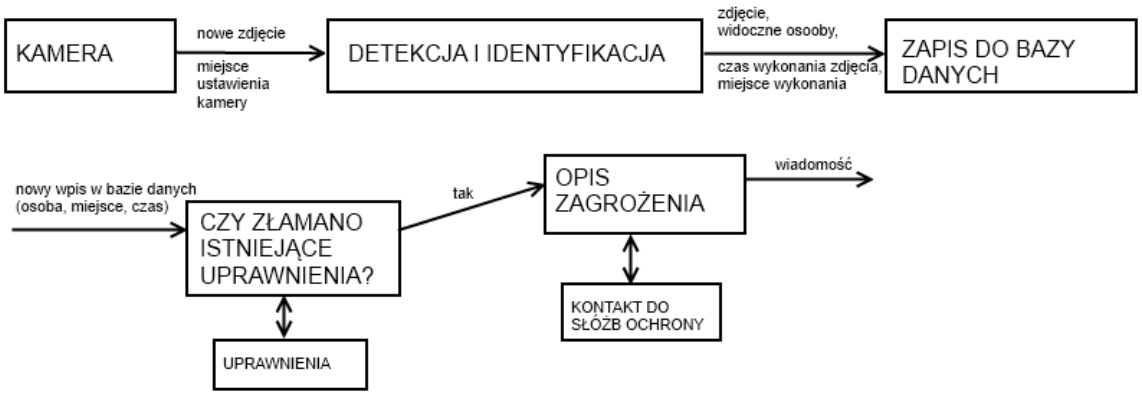
W proponowanym systemie główną rolę odgrywają trzy procesy:

- proces detekcji twarzy na zdjęciu,
- proces identyfikacji wykrytej twarzy,
- proces detekcji zagrożeń.

W doborze odpowiednich algorytmów detekcji twarzy oraz identyfikacji, istotne jest, jak często uruchamiany będzie każdy z tych procesów. Dla małego systemu, obejmującego 3 kamery, proces detekcji twarzy uruchamiany będzie 259200 razy dziennie (przyjmując częstotliwość pobierania obrazu z kamery równy jednej sekundzie). Proces identyfikacji osób uruchamiany będzie jedynie w chwili, gdy na obrazie wykryta zostanie twarz. Oznacza to, że będzie uruchamiany dużo rzadziej (w kontekście jednego dnia), ale przy dużym natężeniu osób w krótkim czasie, może wykrywać wiele osób na jednym zdjęciu i będzie uruchamiany więcej razy niż proces detekcji.

Wobec tego proces detekcji twarzy powinien być przeprowadzany bardzo szybko, a proces identyfikacji mógłby używać zarówno szybkich algorytmów (w czasie dużego natężenia osób), jak i wolniejszych algorytmów, zapewniających większą dokładność rozpoznania.

Proces detekcji zagrożenia przedstawia rysunek 1.



Rys. 1. Proces detekcji zagrożeń (powyżej – detekcja oraz identyfikacja, poniżej – detekcja zagrożeń)
Fig. 1. Schema of dangerous situation detection proces (above – person detection and identification, below – permissions break detection)

System monitoringu zapisuje informacje o każdej detekcji osób w budynku. Dzięki wiedzy, skąd pochodzi zdjęcie (gdzie była umiejscowiona kamera) oraz o czasie wykonania zdjęcia, możliwe jest opisanie każdej detekcji krotką (osoba, miejsce, czas). Ponieważ w bazie istnieje wykaz miejsc, do których uprawniony dostęp ma każda z osób, możliwe jest wykrycie, czy osoba nie uzyskuje nieuprawnionego dostępu do danej części budynku. Jeżeli tak właśnie jest, to przygotowana jest wiadomość opisująca to zdarzenie. Następnie zostaje wysłana do służb ochrony, których dane znajdują się w bazie.

Poza ochroną w czasie rzeczywistym system pozwala na tworzenie raportów umożliwiających lepsze zrozumienie zdarzeń już po fakcie.

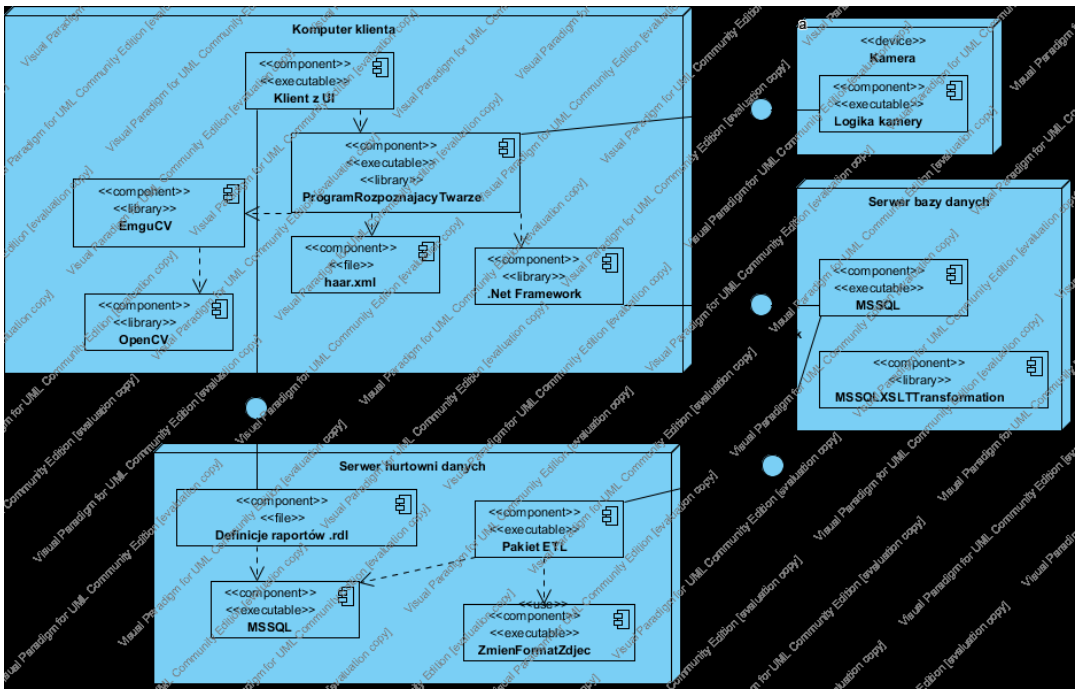
2.1. Architektura systemu

Podczas projektowania systemu wyróżniono dwie role użytkowników –administratora oraz dyspozytora. Administrator zajmuje się zapewnieniem systemowi aktualnych danych

oraz jego konfiguracją, a dyspozytor, analizując komunikaty systemu, czuwa nad bezpieczeństwem na monitorowanym obszarze. Jednocześnie z systemu może korzystać wielu dyspozytorów (np. przy wdrożeniu systemu do zespołu budynków – należy dostarczyć informację o aktywności osób w budynku), dlatego klient systemu musi komunikować się z centralną bazą danych na oddzielnym serwerze.

Ze względu na duży przyrost danych, do analizy gromadzonych przez system danych wykorzystano oddzielny system analityczny. Powinien on znajdować się na dedykowanym serwerze.

Rozdział komponentów systemu przedstawia rysunek 2.



Rys. 2. Rozmieszczenie komponentów systemu
Fig. 2. System component diagram

2.2. Metody detekcji twarzy oraz identyfikacji osób

Na podstawie przeglądu literatury dokonano wyboru metod detekcji twarzy oraz identyfikacji osób do zaimplementowania w systemie.

W przypadku detekcji brane pod uwagę były trzy metody: oparta o kaskady cech Haara [2, 6], oparta na modelu koloru skóry [8], oparta na histogramie zorientowanych gradientów [7]. Wydaje się, że najodpowiedniejszą metodą jest metoda oparta na kaskadach Haara. Działa pod każdym względem (dokładność, odsetek false alarm oraz czas) lepiej niż HOG, a także nie posiada ograniczeń metod opartych na modelu koloru skóry (możliwości analizy jedynie kolorowych zdjęć). W przypadku gdyby liczba fałszywych detekcji okazała się zbyt duża, możliwe byłoby uzupełnienie metody o dodatkową walidację z inną metodą.

W przypadku metod identyfikacji brane pod uwagę były cztery podstawowe metody: Eigenface [3], sieci neuronowe [9], maszyny wektorów nośnych [1], metody aktywnego kształtu [10]. Na podstawie literatury wybrane zostały metody sieci neuronowych oraz SVM, jako zapewniające najwyższą dokładność rozpoznania. Zaimplementowanymi strategiami rozwiązania problemu wielu klas są OVO (*One versus one*) i OVHO (*One versus higher order*) [5]. W przypadku sieci neuronowej testy obejmowały obie te strategie oraz pojedynczą sieć rozwiązującą problem n-klas.

Dodatkowo, jako metoda referencyjna, zaimplementowana została metoda Eigenface (ze względu na jej małą dokładność, użycie jej powinno ograniczyć się do scenariuszy testowych, a nie realnego systemu).

2.3. Testy wydajnościowe

W proponowanej architekturze może wystąpić problem w chwili zbyt dużej liczby osób korzystających z budynku.

Tabela 1

Wyniki testów identyfikacji

Metoda	Dokładność rozpoznania	Odsetek fałszywych alarmów	Czas identyfikacji (ms)	Czas utworzenia klasyfikatora (ms)
Eigenface	61,5%	38,1%	1,711	3392,19
SVM OVO	66,7%	31,9%	181,22	6179,35
SVM OVHO	63,5%	25,0%	21,22	5360,30
Sieć neuronowa	61,1%	15,0%	2,22	40568,20
Sieć neuronowa OVO	59,1%	16,5%	175,05	20833,00
Sieć neuronowa OVHO	49,0%	38,0%	16,57	12043,00

Detekcja przy użyciu metody opartej na kaskadach cech Haara trwa średnio 120 – 140 ms.

Proces detekcji i identyfikacji przebiega na tej samej stacji roboczej. Proces detekcji zagrożenia dokonywany jest w środowisku bazy relacyjnej, czyli na oddzielnej stacji roboczej.

Czas rozpoznania (przy zastosowaniu metody SVM ze strategią OVO), dla założonej przepustowości (300 osób na minutę), pozwala na poprawne działanie systemu.

W przypadku instalacji systemu w środowisku uczelni lub szkoły, możliwe jest zaobserwowanie krótkotrwałego zwiększonego obciążenia systemu (na przerwie, tuż przed lub po zajęciach). Aby wyeliminować sytuację, w której w tym krótkotrwałym momencie zostaną przekroczone możliwości systemu, wprowadzono mechanizm kolejkowania identyfikacji (najdłuższego procesu). Nie powinno się standardowo korzystać z tego mechanizmu (powoduje opóźnienia w dostarczeniu informacji do dyspozytora oraz służb ochrony), ale jedynie w sytuacjach awaryjnych.

2.4. Dane przetwarzane przez system

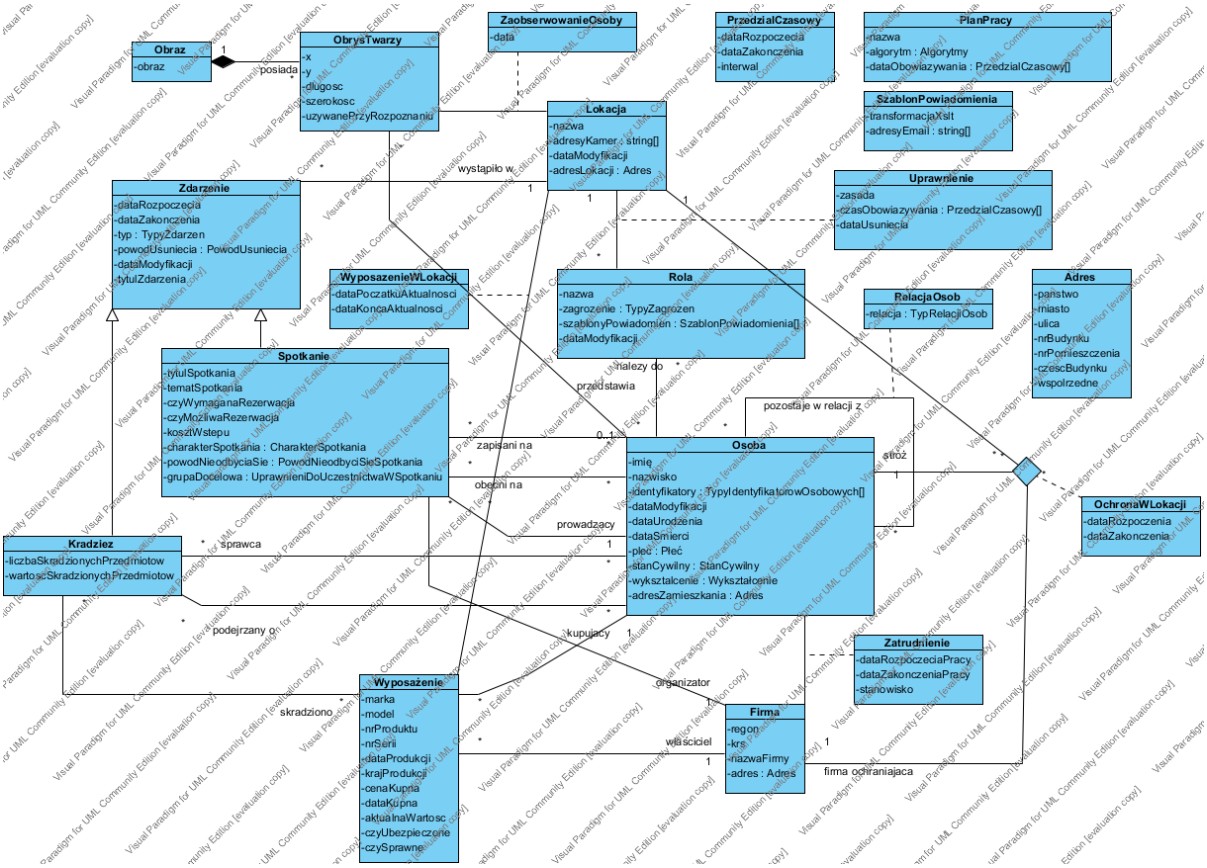
Podstawowy model, na którym dałoby się prowadzić analizy, obejmuje dane osób, lokacji oraz dane obecności osób w budynku.

Dzięki wprowadzeniu uprawnień możliwe jest automatyczne wykrycie nieuprawnionego dostępu do części budynku. Osobom przypisywane są przez administratora odpowiednie role, a rolom – uprawnienia. W chwili wykrycia nieuprawnionego dostępu, sprawdzane są szablony powiadomień związane ze złamanym uprawnieniem i zostanie wysłana zgodna z nimi wiadomość.

W systemie przechowywane są też informację o tym, kto i kiedy zajmował się ochroną budynku. Przechowywane są informację o rozmieszczeniu w budynku wartościowego sprzętu, zdarzeniach zaplanowanych przez administratora budynku (wraz z informacją o osobach mających uczestniczyć w zdarzeniu) oraz o zdarzeniach nieoczekiwanych, niepożądanych (np. kradzieży).

Dzięki zgromadzeniu dodatkowych danych można przeprowadzić szczegółowe analizy (ocena firm ochrony, osoby obecne podczas podobnych zdarzeń).

Wszystkie klasy systemu relacyjnego przedstawią rys. 3 oraz tabela 2.



Rys. 3. Model klas domenowych systemu monitoringu
Fig. 3. Domain class model

Tabela 2

Klasy domenowe systemu monitoringu

Klasa	Opis
Adres	Opisuje położenie rzeczywistego budynku
Firma	Reprezentuje firmę będącą pracodawcą osób rejestrowanych w systemie lub zajmującą się ochroną monitorowanych budynków
Kradzież	Opisuje zdarzenie, które wydarzyło się w jednej z monitorowanych lokacji
Lokacja	Reprezentuje wyznaczone przez użytkownika miejsce w świecie rzeczywistym. Podlega ono obserwacji przez kamery monitoringu
Obraz	Przechowuje dane binarne pliku graficznego, na którym odnaleziono twarz. Format pliku jest zgodny ze standardem .BMP
Obrys Twarzy	Przechowuje dane o położeniu twarzy na obrazie
Ochrona lokacji (klasa asocjacyjna)	Określa przedział czasu, w którym wyznaczona firma oraz stróż zajmowali się ochroną danej lokacji
Osoba	Reprezentuje osoby mogące być rozpoznane przez system monitoringu
Plan Pracy	Określa, kiedy system monitoringu ma pracować oraz który z algorytmów rozpoznania twarzy ma zostać użyty
Relacja osób (asocjacyjna)	Określa związki łączące dwie osoby. Mogą to być związki rodzinne (ojciec, matka, dziecko), koleżeńskie lub pracownicze (przełożony)
Rola	Reprezentuje grupę osób posiadających zdefiniowane uprawnienia
Spotkanie	Reprezentuje zdarzenia spotkania wielu osób w lokacji monitorowanego budynku
Szablon Powiadomienia	Przechowuje dane o powiadomieniach wysyłanych pocztą elektroniczną w razie złamania uprawnień
Uprawnieni do uczestnictwa w spotkaniu (typ wyliczeniowy)	Reprezentuje możliwe grupy osób, które są uprawnione do uczestnictwa w spotkaniu
Uprawnienie	Określa, w których lokacjach mogą przebywać członkowie określonych ról
Wyposażanie w lokacji (klasa asocjacyjna)	Określa przedział czasu, w którym dane wyposażenie znajdowało się w danej lokacji monitorowanego budynku
Wyposażenie	Reprezentuje cenne urządzenie znajdujące się w monitorowanych budynkach
Zaobserwowanie Osoby	Reprezentuje zdarzenie wykrycia obecności osoby w określonej lokacji w danym czasie
Zatrudnienie (asocjacyjna)	Określa przedział czasu, w którym osoba pracowała dla firmy na określonym stanowisku

2.5. Raporty systemu analitycznego

2.5.1. Ocena ochrony

Ocena ochrony to roczne zastawienie zawierające wyniki pracy firm ochrony zabezpieczających teren monitorowanych budynków. Dla każdej z firm, w każdym miesiącu, przypisane są: liczba zaobserwowań osób przez system monitoringu, liczba zaobserwowań osób, które złamały nadane im uprawnienia, odsetek zaobserwowań ze złamanymi uprawnieniami oraz liczba kradzieży.

Następnie przedstawiane jest podobne zestawienie obejmujące pracowników ochrony. Końcowym elementem raportu jest wykaz dziesięciu stróży, podczas których służby najczęściej łamano uprawnienia.

Raport pozwala ocenić, które z firm najlepiej zabezpieczają budynki, a z którymi lepiej rozwiązać umowę. W razie dużej liczby zaobserwowań osób ze złamanymi uprawnieniami można poprosić firmę o wyjaśnienia.

2.5.2. Dane osoby

Raport zawiera dane personalne wybranej osoby. Poza nimi przedstawione są maksymalnie trzy zdjęcia twarzy oraz związki rodzinne osoby. W dalszej części zamieszczony jest wykaz znanych relacji z innymi osobami. Kolejny wykaz obejmuje także relacje z innymi osobami, ale są one tworzone na podstawie odnotowanych w bazie zaobserwowań przez system monitoringu wybranej osoby razem z innymi osobami.

2.5.3. Osoby podczas zdarzenia

Raport zawiera dane osób, które były najczęściej widziane w miejscu i czasie zdarzenia (zdarzeń). Raport pozwala na odnalezienie osób mogących wyjaśnić zdarzenie, ponieważ były jego świadkami lub aktywnymi uczestnikami.

2.5.4. Zaobserwowania w czasie zdarzenia

Raport prezentuje wykaz zaobserwowań przez system monitoringu wybranej osoby w czasie i miejscu zdarzeń. Raport pozwala na dokładną analizę, w jakim czasie widziana była osoba oraz czy złamała uprawnienia.

2.5.5. Zaobserwowania przed zdarzeniem

Raport prezentuje wykaz osób widzianych przed wybranymi zdarzeniami w równych odstępach czasu. Podaje, w jakim przedziale czasowym zaobserwowano taką regularność oraz jaki był interwał czasowy między odnotowaniem osoby a zdarzeniem.

Raport pozwala wyłapać ewentualne osoby współpracujące z prowodyrem zdarzenia.

2.5.6. Grupa osób widziana podczas zaobserwowania

Raport przedstawia wykaz innych osób widzianych w czasie odnotowania obecności wybranej osoby w danym miejscu i czasie.

2.5.7. Spotkania przed usterką

Raport przedstawia wykaz spotkań, jakie miały miejsce bezpośrednio przed zgłoszeniem usterki w wyposażeniu budynku.

2.5.8. Uczestnicy spotkania

Raport zawiera dane osób związanych z organizowanym spotkaniem. Są to osoby zapisane na spotkanie, osoby, które były na spotkaniu wg listy obecności oraz osoby będące na spotkaniu wg systemu monitoringu. Dane te w powiązaniu z raportem „spotkania przed usterką", pozwalają na ustalenie, które osoby mogły dopuścić się jakichś zniszczeń.

3. Podsumowanie

3.1. Zrealizowane cele

Celem pracy było zaprojektowanie systemu monitoringu budynków, który poprawiłby bezpieczeństwo osób znajdujących się w monitorowanym obiekcie. Należało zidentyfikować zagrożenia, którym system mógłby przeciwdziałać. Ponieważ system automatycznie identyfikuje osoby pojawiające się na zdjęciach monitoringu, należało przeprowadzić badania odpowiadające na pytanie, jaką metodę identyfikacji należy zaimplementować?

System reaguje na każdorazowe zidentyfikowanie osoby w budynku, natychmiastowo sprawdzając, czy jest to osoba mogąca przebywać w miejscu, w którym została zauważona. W przypadku zidentyfikowania zagrożenia informowane są o nim zdefiniowane przez administratora systemu podmioty.

W artykule zawarte zostały projekt oraz implementacja systemu hurtowni danych, pozwalającego na integrację danych z wielu systemów monitoringu oraz na ich analizę pod kątem wyszukania osób mogących pomóc w wyjaśnieniu odnotowanych zdarzeń.

W pracy zawarte zostało porównanie metod identyfikacji osób. Zaimplementowano metody Eigenface, SVM oraz sieci neuronowe. W wyniku badań wybrano metodę SVM, jako gwarantującą największą dokładność identyfikacji. W systemie możliwe jest używanie także dwóch pozostałych, zaimplementowanych metod.

Po zbadaniu strategii OVHO potwierdzona została jej skuteczność. Przy dużym natężeniu osób możliwe jest jej wykorzystanie, co zmniejsza czas klasyfikacji bez dużej straty dokładności.

Użyta do detekcji twarzy metoda Violi-Jonesa pozwoliła na detekcję z miarą f-score powyżej 0,90, co sprawia, że może być bez dalszych modyfikacji stosowana w systemie.

3.2. Przyszłość systemu

Zbudowany system może być użyteczny. Określenie jego pełnego zakresu zastosowań możliwe będzie dopiero po przeprowadzeniu wdrożenia w środowisku docelowym. W przypadku pojawienia się nowych potrzeb użytkowników, na podstawie istniejącej hurtowni danych możliwe jest zbudowanie nowych raportów bądź rozbudowanie już dostarczonych.

System może być rozwijany w kierunku kompleksowego systemu zarządzania budyniem, tj. zrealizowania usług pozwalających na pełną modyfikację danych, np. spotkań, grafików ochrony czy danych wyposażenia (w tym momencie możliwy jest jedynie import z plików XML). W takim przypadku, ze względu na większą liczbę osób pracujących z systemem (cały dział administracyjny), należy rozważyć dostarczenie „cienkiego klienta" dostępnego przez przeglądarkę internetową.

Wyniki eksperymentu pokazują, że zastosowane metody nie rozwiązują w zadowalającym stopniu problemu identyfikacji w realnym środowisku. Należy przetestować nowsze metody identyfikacji.

BIBLIOGRAFIA

1. Li S. Z., Jain A. K.: Handbook of face recognition. Springer, 2005.
2. Viola P., Jones M.: Rapid Object Detection using Boosted Cascade of Simple Features. IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2001, Vol. 1, 2001, s. 511÷518.
3. Turk M., Pentland A.: Face Recognition Using Eigenfaces. IEEE Conference on Computer Vision and Pattern Recognition, Maui, Hawaii 1991.
4. Castrillon-Santana M., Deniz-Suarez O., Anton-Canalıs L., Lorenzo-Navarro J.: Face and Facial Feature Detection, Evalueation - Performance Evaluation of Public Domain Haar Detectors for Face and Facial Feature Detection. International Conference on Computer Vision Theory and Applications, Vol. 1, 2008.
5. Ou G., Murphey Y. L.: Multi-class pattern classification using neural network. Journal Pattern Recognition, Vol. 40, No. 1, 2007, s. 4÷18.

6. Erdem C., Ulukaya S., Karaali A., Erdem A.: Combining Haar Feature and skin color based classifiers for face detection. IEEE International Conference on Acoustics, Speech and Signal Processing, 2011, s. 1497÷1500.
7. Corviee E., Bremond F.: Combining face detection and people tracking in video sequences. 3rd International Conference on Crime Detection and Prevention, 2009, s. 1÷6.
8. Jones M., Rehg J.: Statistical color models with application to skin detection. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1999.
9. Rizon M., Firdaus Hashim M., Saad P.: Face Recognition using Eigenfaces and Neural Networks. American Journal of Applied Sciences 2(6), 2006, s. 1872÷1875.
10. Cootes T., Taylor C.: Statistical Models of Appearance for Computer Vision. University of Manchester, 2004.

Wpłynęło do Redakcji 31 stycznia 2012 r.

Abstract

The paper contains project and implementation of building monitoring system. Proposed system can recognize people on video-stream from camera. The system is able to react to event of recognition person who may be dangerous. It is sending messages to previously configured recipients (i.e. security agency).

Proposed system contains data warehouse to integrate data from many independent monitoring systems. Using data from warehouse, system is able to analyze recorded events and find their causes or context.

The paper contains comparison of face recognition methods in context of building monitoring. There are three algorithms implemented: Eigenface, support vector machine and neural networks. Tests aimed to identify best parameters to use with algorithms and to create recommendation when to use which algorithm.

Studies have shown that SVM-based method has best identification accuracy. Using OVHO (one-versus-higher-order) strategy let reduce time needed to recognize person (comparing to alternative strategy – OVO (one-versus-one)).

Adres

Witold Wabik: Instytut Informatyki, Politechnika Wrocławska, Wyb. Wyspiańskiego 27, Wrocław, Polska, 157699@student.pwr.wroc.pl.