Piotr ŁUBKOWSKI, Dariusz LASKOWSKI
WOJSKOWA AKADEMIA TECHNICZNA,
Gen. S. Kaliskiego 2, 00-908 Warszawa

Niezawodność identyfikacji danych w systemach monitoringu

Dr inż. Piotr ŁUBKOWSKI

Uzyskał tytuł magistra inżyniera (1991) i doktora nauk technicznych (2002) w dziedzinie telekomunikacji i teleinformatyki w Wojskowej Akademii Technicznej. Od 1992 roku pracuje w Instytucie Telekomunikacji, Wydziału Elektroniki Wojskowej Akademii Technicznej. Realizuje badania w obszarze systemów i usług multimedialnych, jak również wspierania jakości QoS w heterogenicznych bezprzewodowych sieciach doraźnych.

e-mail: plubkowski@wat.edu.pl

Dr inż. Dariusz LASKOWSKI

Uzyskał doktora nauk technicznych w dziedzinie telekomunikacji w Wojskowej Akademii Technicznej. Koncentruje swoje zainteresowania w dziedzinie niezawodności, bezpieczeństwa i jakości systemów ICT. Jest autorem licznych artykułów w publikacjach krajowych i międzynarodowych.

e-mail: dlaskowski@wat.edu.pl

Streszczenie

Systemy monitoringu wideo od szeregu lat wykorzystywane są w celu zwiększenia poziomu bezpieczeństwa nadzorowanych obiektów i dóbr materialnych. W każdym z wymienionych zastosowań niezwykle istotnym zagadnieniem jest niezawodność procesów nadzoru i monitorowania. W artykule przedstawiono analizę wpływu oświetlenia, odległości obiektu od sensora czy rozdzielczości sensora na poprawną identyfikację. Przeprowadzone badania umożliwiają określenie przydatności systemu monitoringu w określonych warunkach środowiskowych i technicznych.

Słowa kluczowe: monitoring, identyfikacja, niezawodność.

Reliability of data identification in monitoring systems

Abstract

Nowadays, many areas have to be protected. Monitoring systems (MS) effectively support this kind of processes. A monitoring system provides an image of the area containing the monitored objects. These systems are also used to increase the safety of people. That is why the efficiency is important in the reliable monitoring system (RMS). These issues are interpreted as the possibility of correct identification of the collected data. The reliability of elements, the environmental exposure as well as the process of object detection and face identification analysis have important impact on the MS. Therefore, the main problem of the research is to answer the question: what is the reliability of the identification data (i.e. people) in the real-time monitoring system? The paper presents the main results of the study. The study was conducted in the MS demonstrator consisting of a telecommunication network with implemented video monitoring sensors. Various experiments were performed to adjust the lighting, the distance from the camera and the number of face images in the database. The developed method has to determine the reliability of the identification data. It takes into account the influence of degrading factors which are present in the monitoring system environment. On the basis of the obtained results we specify a set of recommendations for the reference MS.

Keywords: monitoring, identification, reliability.

1. Wstęp

Systemy monitoringu wideo od szeregu lat wykorzystywane są w celu zwiększenia poziomu bezpieczeństwa obywateli i ochranianych obiektów. Z monitoringiem wideo spotykamy się zarówno w obiektach użyteczności publicznej i państwowej, w miejscach powszechnie dostępnych jak i na obszarach o dostępie ograniczonym. Systemy monitoringu wideo stanowią połączenie urządzeń rejestrujących (sensorów), przesyłających, przechowujących oraz odtwarzających w jedną integralną całość. Umożliwiają obserwację osób czy obiektów w czasie rzeczywistym oraz rejestrację zdarzeń w celu ich późniejszej analizy.

Wykrywanie i identyfikacja osób jest jedną z podstawowych zalet oferowanych we współczesnych systemach monitoringu. Automatyczne wykrywanie i rozpoznawanie osób na podstawie rysów twarzy jest aktywnym obszarem badań obejmującym różne dziedziny nauki. Kompletny system analizy obrazu twarzy powinien być zdolny do zlokalizowania twarzy w danym obrazie, identyfikacji punktów rysów twarzy, opisu wyrazu twarzy, a także rozpoznawania ludzi. Większość systemów analizy i rozpoznawania twarzy działa przy założeniu, że położenie twarzy w kadrze jest znane. Jednakże to założenie jest prawdziwe tylko w sytuacji obrazów o jednolitym tle.

Na skuteczność procesu analizy, wykrywania i identyfikacji twarzy wpływ mają także takie czynniki jak oświetlenie, odległość obiektu od sensora czy obecność obiektów drugoplanowych utrudniają identyfikację. Nie bez znaczenia są także parametry techniczne sensora i urządzeń przesyłających i rejestrujących oraz wykorzystywane techniki transmisji danych (przewodowe czy bezprzewodowe). Każdy z wymienionych czynników degradujących wpływa na niezawodność procesu identyfikacji. Uwzględniając powyższe przyjęto, iż zasadniczym problemem badawczym zdefiniowanym w ramach niniejszej publikacji jest udzielnie odpowiedzi na pytanie: Jak wskazane czynniki degradujące wpływają na niezawodność procesu identyfikacji osób w rzeczywistym systemie monitoringu?

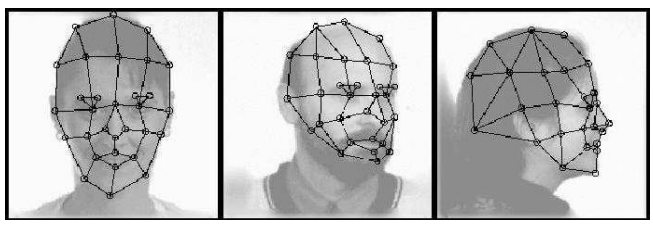
2. Charakterystyka metod identyfikacji

Proces rozpoznawania twarzy realizowany jest z wykorzystaniem określonych algorytmów oraz z uwzględnieniem zasadniczych cech obrazu cyfrowego. Bardzo często w procesie identyfikacji wykorzystuje się kilka metod jednocześnie, co służy poprawie skuteczności ich działania, ale może prowadzić także do wzrostu stopnia skomplikowania funkcjonowania algorytmu. Łączenie algorytmów wprowadza także trudność we właściwej identyfikacji metody stosowanej przez określoną aplikację. Generalnie wyróżnia się następujące grupy metod [1]: bazujące na lokalnych cechach, całościowe i hybrydowe.

Metody bazujące na lokalnych cechach, nazywane także metodą siatki dynamicznych połączeń, realizowane są w oparciu o modelowanie twarzy przy użyciu takich jej elementów jak oczy, usta czy nos. Wykorzystywane są również wzajemne zależności pomiędzy ich rozmieszczeniem. Rozpoznanie (identyfikacja) ogranicza się w przypadku tej metody do porównania układu elementów stanowiących cechy twarzy [2] przy założeniu, że wszystkie twarze mają zbliżoną strukturę topologiczną. Układ ten może być zobrazowany przy pomocy grafów (rys. 1) w opisie, których wykorzystuje się tzw. falkę Gabora [3]. Węzły grafu reprezentują charakterystyczne punkty obrazu, zaś krawędzie łączące te węzły tworzą wektory odległości pomiędzy nimi [4]. Rozpoznawanie polega na ustawieniu grafu na badanym obrazie, wyznaczeniu jego parametrów i porównaniu z grafami modelowymi przechowywanymi w bazie danych.

W metodzie całościowej wykorzystywana jest analiza głównych składowych Obrazu oraz analiza dyskryminacyjna. Metoda polega na redukcji podstawowego obrazu twarzy, który stworzony jest z tysięcy pikseli, do obrazu zawierającego tylko istotną jego część.

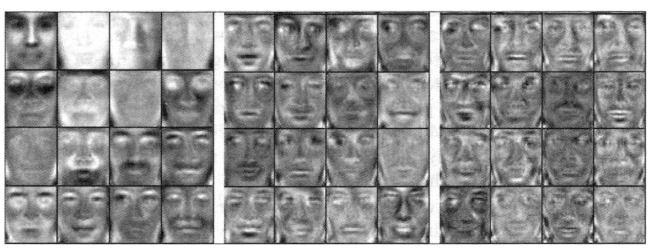
Istotą tej metody jest to, aby pozostawić te cechy, które niosą jakąś informację i odróżnić je od np. „szumu", który spowodowany jest złym oświetleniem. W tym celu obraz twarzy przekształca się w ten sposób, aby tworzyła go liniowa kombinacja obrazów bazowych (rys. 2), zwanych „twarzami własnymi" (ang. eigenfaces) [5].



Rys. 1. Schemat wykorzystania grafu do opisu twarzy [4]
Fig. 1. The use of graph scheme to face description [4]

W procesie analizy głównych składowych powszechnie wykorzystywane jest przekształcenie Karhunena-Loevego (K-L), a metody bazujące na tym przekształceniu stanowią obecnie dominującą grupę rozpoznawania twarzy. Z kolei analiza dyskryminacyjna wykorzystywana w tej metodzie wykorzystuje kryterium Fishera umożliwiające optymalizację wyniku wyszukiwania [4].

Ostatnią z prezentowanej grupy metod jest metoda hybrydowa bazująca na aktywnych modelach kształtu ASM (ang. Active Shape Models) [6], czyli na strukturze zawierającej informacje o średnim kształcie obiektu danego typu oraz dane opisujące najbardziej charakterystyczne modyfikacje tego kształtu. Postać danego modelu może być zmieniana poprzez algorytmy, które próbują go dopasować do rzeczywistego obiektu i zarazem nie dopuszczają do jego nienaturalnych deformacji.



Rys. 2. Obraz twarzy rozłożony na ważoną sumę twarzy własnych [5]
Fig. 2. The face image decomposed into a weighted sum of the eigenfaces [5]

Rozpoznawanie w omawiane metodzie polega na porównaniu wektora parametrów modelu dopasowanego do badanego obrazu twarzy z wektorami zgromadzonymi w bazie danych [4]. Modelowaniu podlega nie tylko kształt całej twarzy, ale także rozkłady jasności pikseli wokół każdego charakterystycznego punktu. Lokalne modele, które reprezentują otoczenie tych punktów wykorzystywane są do modyfikacji i przemieszczania całego modelu.

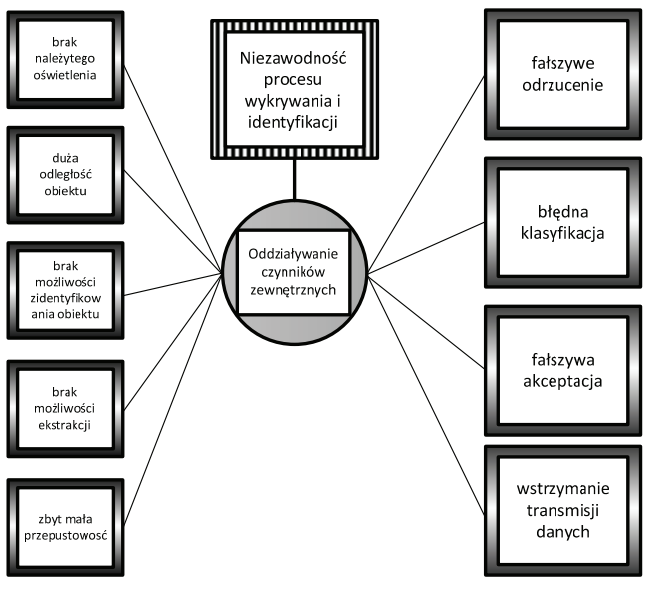
3. Analiza zagrożeń procesu poprawnej identyfikacji

Zdolność systemu monitoringu do poprawnego wykrywania i identyfikacji zagrożeń jest jednym z istotnych czynników warunkujących skuteczność, efektywność i niezawodność jego działania. Stąd też w procesie analizy niezawodnej identyfikacji wziąć należy pod uwagę dodatkowo zagrożenia oraz wywołane nimi skutki, które w bezpośredni sposób oddziaływają na ten proces. Ta, tak zwana analiza ryzyka jest częścią procesu walidacji wyników badań zaprezentowanych w dalszej części artykułu.

Wykorzystywane współcześnie sieci monitoringu wideo charakteryzują się takimi właściwościami jak częste zmiany topologii, mobilność użytkowników i dostawców usług, wykorzystanie łączy bezprzewodowych oraz ograniczonej mocy przetwarzania i pojemności węzłów sieci. Z kolei na właściwą pracę sensora wpływ mają takie czynniki jak oświetlenie, odległość obiektu od sensora czy obecność obiektów drugoplanowych utrudniają identyfikację. Nie bez znaczenia są także wspomniane już parametry techniczne, a w szczególności czułość przetwornika, ogniskowa, rozdzielczość czy zastosowany rodzaj kompresji. Biorąc pod uwagę powyższe zidentyfikować można następujące zagrożenia związane z niezawodną identyfikacją danych: brak należytego oświetlenia obiektu (zbyt mała czułość przetwornika) lub brak pracy w trybie podczerwieni, zbyt duża odległość obiektu od kamery (brak właściwego doboru ogniskowej), brak możliwości wyspecyfikowania obiektu (zbyt mała rozdzielczość sensora), brak możliwości ekstrakcji (mała rozdzielczość, czułość), brak przepustowości (niewłaściwa kompresja). Wymienione zagrożenia mogą prowadzić do następujących problemów związanych z procesem niezawodnej identyfikacji (rys. 3):

- fałszywe odrzucenie – obiekt, który ma swój wzór w bazie danych jest nierozpoznany i odrzucony ze względu na to, że nie posiada swojego odpowiednika,
- błędna klasyfikacja – obiekt, który posiada swój wzór w bazie danych jest nieodpowiednio przypisany do innego wzoru w bazie,
- fałszywa akceptacja – obiekt, który nie posiada swojego wzoru w bazie danych zostaje przypisany do wzoru, który już istnieje w bazie.

Wymienione zagadnienia uwzględnione były w trakcie realizowanych badań, chociaż uniknięcie niektórych zagrożeń wydaje się niemożliwe zwłaszcza, jeżeli wziąć pod uwagę oddziaływanie zewnętrznych czynników. Stąd też producenci oprogramowania wykorzystywanego w procesie identyfikacji i wykrywania zagrożeń coraz częściej skłaniają się w kierunku stosowania metod wykorzystujących mechanizmy „uczenia się", czyli takie, które w oparciu o pewien zasób cech niskopoziomowych potrafią wydobyć wiedzę o informacji zapisanej w obrazie.



Rys. 3. Analiza zagrożeń i problemów niezawodnej identyfikacji w aspekcie oddziaływania czynników zewnętrznych (opracowanie własne)
Fig. 3. Threat analysis and problems of reliable identification in terms of the influence of external factors

Przykładem takiego programu jest aplikacja „Multiple face detection and recognition in real time" (MFRRT) wykorzystana do realizacji stanowiska badawczego zrealizowanego w laboratoryjnej sieci monitoringu, które posłużyło do realizacji prezentowanych poniżej eksperymentów. Prezentowana aplikacja wykorzystuje w procesie detekcji i rozpoznania twarzy metodę tzw. „twarzy własnych" wykorzystującą analizę głównych składowych PCA (Prinipal Component Analysis). W procesie rozpoznawania wykorzystywana jest biblioteka EmguCV, oferująca szereg istotnych funkcji związanych z rozpoznawaniem i identyfikacją, a w tym rozpoznawanie znaków, wykrywanie twarzy czy ruchu obiektów.

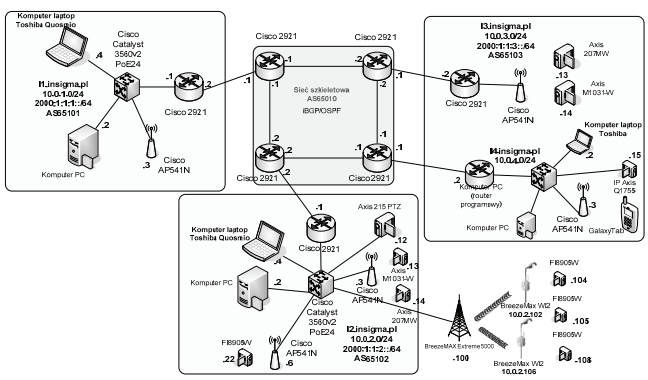
4. Środowisko badawcze dla identyfikacji w systemie monitoringu

Do realizacji eksperymentu badawczego wykorzystano istniejącą infrastrukturę laboratoryjnej sieci monitoringu (rys. 4) [7, 8, 9]. Wnioskowanie nt. poprawności zestawienia komponentów sieciowych w zakresie przesyłania danych, będących odzwierciedleniem informacji z systemu monitoringu, opiera się na statystycznym oszacowaniu nieuszkadzalności platformy sprzętowo-programowej tworzącej łańcuch realizacji usługi.

Komponenty platformy badawczej są produktami renomowanych dostawców urządzeń i oprogramowani zarówno systemowego jak i aplikacyjnego. Dlatego też wydaje się zasadnym stwierdzenie, iż zestawiony układ pomiarowy stanowi poprawny i „wysoce" nieuszkadzalny testbed. Z przeprowadzonych badań, wynika, że tego rodzaju środowisko badawcze może zostać uznane, jako źródłem wiarygodnych i powtarzalnych danych wyjściowych adekwatnie do danych wejściowych.

Dla zapewnienia współpracy z istniejącym systemem monitoring aplikacja MFRRT została zmodyfikowana w zakresie możliwości dołączenia kamer IP [10]. W omawianym systemie wykorzystywane są kamery IP firmy AXIS serii PTZ215, 1031W, 207MW i Q1755 oraz kamery FI8905W. Do komunikacji z kamerami wykorzystywany jest protokół RTSP (ang. Real-Time Streaming Protocol).

Aplikacja umożliwia stworzenie własnej bazy danych obiektów, w której zapisane są obrazy twarzy osób identyfikowane z wykorzystaniem przypisanych identyfikatorów ID. Baza twarzy powstaje automatycznie w katalogu „TrainedFaceas", który zawsze znajduje się w katalogu głównym programu. Obrazy mogą być zapisywane wprost z kamery w sposób automatyczny (przy pierwszej identyfikacji osoby) lub dodane z pliku zewnętrznego (z rozszerzeniem .bmp).



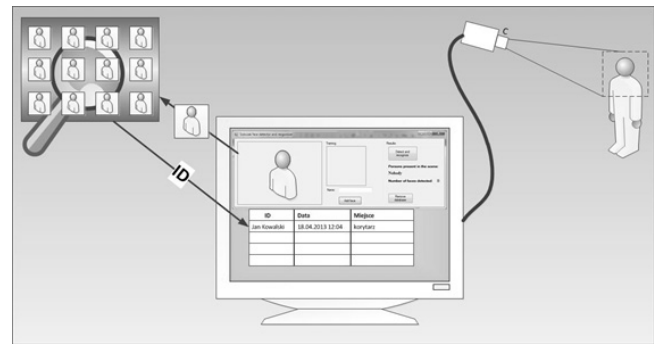
Rys. 4. Schemat laboratoryjnej sieci monitoringu (opracowanie własne)
Fig. 4. Diagram of the laboratory monitoring network

Uproszczony schemat procesu identyfikacji z wykorzystaniem aplikacji w środowisku laboratoryjnej sieci monitoringu przedstawiony został na rysunku (rys. 5). W celu sprawdzenia wpływu czynników środowiskowych na sprawność i niezawodność funkcjonowania procesu identyfikacji w rzeczywistym systemie monitoringu przeprowadzony został szereg eksperymentów.

Podczas testów sprawdzano, jaki wpływ na rozpoznanie twarzy mają warunki środowiskowe, takie jak oświetlenie i odległość od kamery oraz uwarunkowania techniczne związane z rozdzielczością kamery. Sprawdzono także wpływ liczby zdjęć twarzy w bazie danych na szybkość i dokładność identyfikacji. Założono, że podczas eksperymentów baza korzystać będzie z jednego albo sześciu zdjęć.

Testy wykonano na komputerze typu laptop z procesorem Intel Dual Core 2.0 GHz, wyposażonym w pamięć RAM 6 GB i system operacyjny Windows 7 oraz z wykorzystaniem kamery IP AXIS 215 PTZ. Poszczególne eksperymenty wykonane zostały w następujących konfiguracjach:

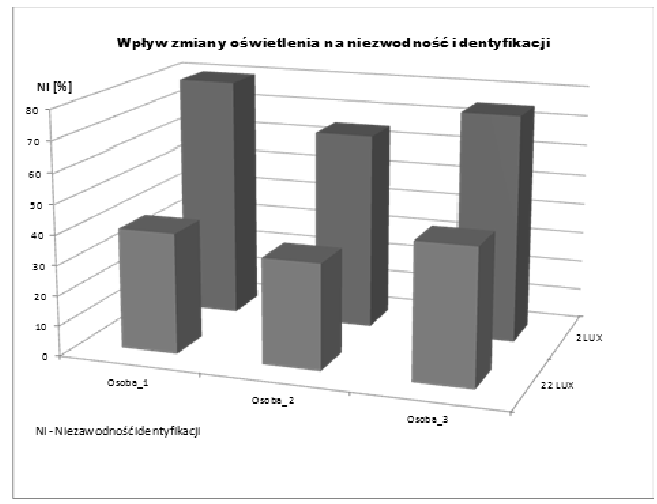
1) Zmiana oświetlenia – Testy przeprowadzono na trzyosobowej grupie z włączonym sztucznym oświetleniem o natężeniu 122LUX-ów oraz bez oświetlenia (wartość zmierzona równa 2LUX-y), odległość od kamery wynosiła 1m.
2) Zmiana liczby obrazów twarzy w bazie danych – Badania przeprowadzono dla dwóch zbiorach obrazów jednej twarzy w bazie.
3) Zmiana rozdzielczości kamery – Testy przeprowadzone zostały, w pierwszym przypadku, gdy kamera pracowała w trybie niskiej rozdzielczości QCIF (176x144), a następnie przełączona została do trybu wysokiej rozdzielczości 4CIF (704x576). Podczas badań w pomieszczeniu było włączone sztuczne oświetlenie.



Rys. 5. Schemat procesu identyfikacji osób w laboratoryjnej sieci monitoringu
Fig. 5. Diagram of people identification process in a laboratory network

Przed realizacją badań postanowiono przyjąć kryterium niezawodnego rozpoznania obiektu, który będzie znajdował się w polu obserwacji systemu monitoringu oraz jego cechy specyficzne są zapisane w bazie danych o obiektach. Kryterium to zostało ustalone w postaci wartości prawdopodobieństw rozpoznania:
1) Wystarczającego równej, co najmniej 50%.
2) Zadawalającego równej, co najmniej 60%.
3) Poprawnego równej, co najmniej 70%.
4) Docelowy równej, co najmniej 90%.

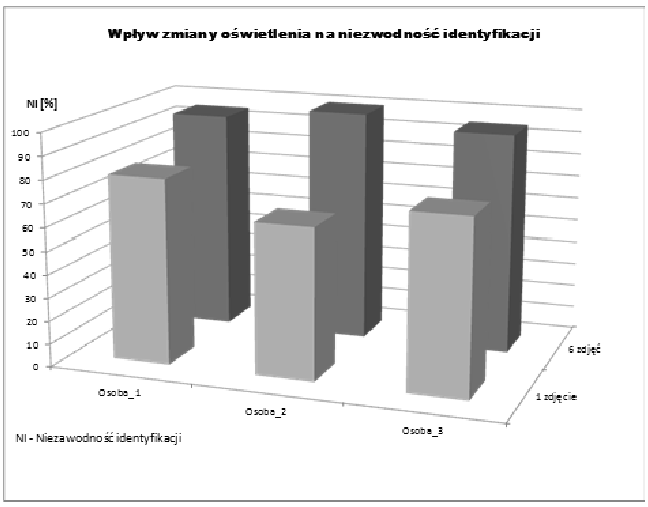
Na rysunkach (rys. 6, rys. 7) przedstawiono wyniki eksperymentu określającego wpływ zmiany oświetlenia oraz liczby zdjęć obiektu w bazie danych na niezawodność procesu identyfikacji.



Rys. 6. Niezawodność identyfikacji w funkcji natężenia oświetlenia
Fig. 6. The identification reliability as a function of the light intensity

Rysunek 6 przedstawia wpływ zmiany oświetlenia przy jednym zdjęciu w bazie. Jak można zauważyć, przy braku sztucznego oświetlenia następuje wzrost niezawodności procesu identyfikacji. Wynika to z faktu, że badana kamera posiada funkcję pracy w trybie nocnym, co w efekcie przy zastosowanym algorytmie identyfikacji pozwala dokładnie wykryć granice twarzy oraz zidentyfikować ciemne punkty obrazu, jako oczy i usta, stanowią-

ce najbardziej charakterystyczne punkty analizowanego obrazu. Kolejny rysunek (rys. 7) prezentuje wyniki badania niezawodności procesu identyfikacji w funkcji liczby zdjęć danej osoby znajdujących się w bazie danych.



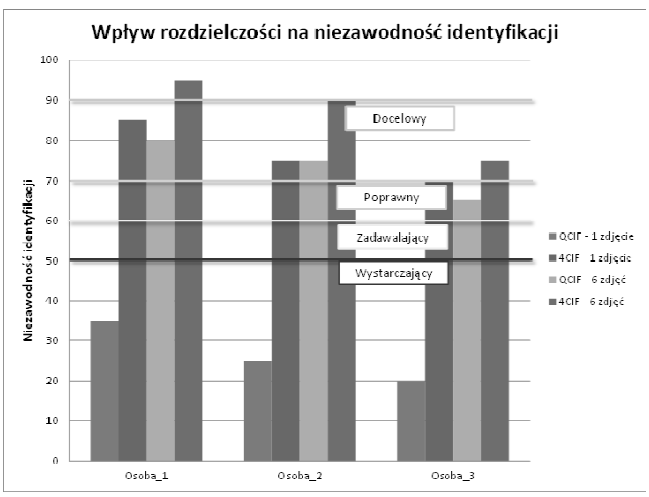
Rys. 7. Niezawodność identyfikacji w funkcji liczby zdjęć (bez oświetlenia)
Fig. 7. The identification reliability as a function of the number of photos (without lighting)

Wyniki pomiarów wskazują, że liczba zdjęć twarzy w bazie ma wpływ na jakość tego procesu, i jest to wpływ zauważalny.

Ostatnia seria eksperymentów związana była z określeniem wpływu parametrów kamery (rozdzielczość) na niezawodność procesu identyfikacji. Podczas testów kamera pracowała w trybie niskiej rozdzielczości QCIF (176x144), a następnie przełączona została do trybu wysokiej rozdzielczości 4CIF (704x576).

Wyniki eksperymentów zaprezentowane na rysunku 8 przedstawiają niezawodność identyfikacji dla wszystkich badanych przypadków, czyli z 1 zdjęciem i 6 zdjęciami w bazie danych. Analizując otrzymane wyniki stwierdzić należy, że poprawna identyfikacja możliwa jest nawet przy niewielkiej rozdzielczości kamery. Zastosowanie takiego wariantu pracy nie daje jednak 100% gwarancji poprawnej pracy systemu.

W trakcie eksperymentu stwierdzono, że przy małej rozdzielczości w układzie z 1 zdjęciem w bazie, zwłaszcza w odniesieniu do osoby nr 3, stwierdzono bardzo często występowanie błędu fałszywego odrzucenia (ponad 60% przypadków) i błędu fałszywej klasyfikacji. Ponadto w przypadku, gdy w obiektywie kamery znajdowały się równocześnie 3 osoby system nie był w stanie ich poprawnie zidentyfikować.



Rys. 8. Niezawodność identyfikacji w zależności od rozdzielczości kamery
Fig. 8. The identification reliability based on the camera resolution

Znaczącą poprawę uzyskano w przypadku eksperymentu z bazą zawierającą 6 zdjęć, chociaż i w tej sytuacji równoczesna obecność wszystkich trzech osób stwarzała problemy identyfikacji. Natomiast w przypadku pracy w trybie wysokiej rozdzielczości system cechował się prawie 100% niezawodnością identyfikacji. Należy nadmienić, że także podczas tego eksperymentu wyniki uzyskane dla osoby nr 3 były najgorsze. Może to wynikać z faktu dużego podobieństwa rysów twarzy w stosunku do osoby nr 1. Celem wyeliminowania tego błędu należałoby zwiększyć liczbę zdjęć osoby identyfikowanej w bazie danych oraz rozszerzyć grupę badaną o kolejne osoby.

5. Wnioski

Przedstawiona w artykule analiza wpływu czynników degradujących umożliwia określenie przydatności systemu monitoringu do identyfikacji osób w określonych warunkach środowiskowych i technicznych. Stanowić może pewien zbiór rekomendacji i zaleceń niezbędnych do zastosowania w celu poprawy niezawodnej pracy tego systemu w zakresie identyfikacji i rozpoznania osób. Z przedstawionej analizy w oczywisty sposób wynika potrzeba posiadania rozbudowanej bazy obiektów twarzy, która zwiększa prawdopodobieństwo poprawnego wykrycia i rozpoznania osoby. Można również zauważyć, że współczesne kamery sieci monitoringu nie są już tak wrażliwe na zmianę warunków środowiskowych związanych z oświetleniem.

Reasumując stwierdzić należy, że chociaż nie istnieje system monitoringu dający 100% gwarancję niezawodnej identyfikacji, to jednak stosowanie określonych kryteriów (tj. poziomy: wystarczający, zadawalający, poprawny i docelowy), zaprezentowanych w niniejszym artykule, prowadzić będzie do uzyskania pożądanego „wysokiego" stopnia niezawodnej identyfikacji. Poziom pożądany będzie identyfikowany w postaci zmiennej wartości prawdopodobieństwa rozpoznania adekwatnie do zapotrzebowania i czasu przetwarzania danych. Otrzymane, w trakcie prowadzenia badań środowiskowych, wyniki stanowią determinantę do opracowywania i implementacji kolejnych mechanizmów identyfikacji obiektów, ponieważ obszar zastosowań niezawodnej identyfikacji obiektu w systemie monitoringu jest szeroki.

6. Literatura

[1] Zhao W., Chellappa R., Rosenfeld A., Phillips P.J., Face Recognition: A Literature Survey. ACM Computing Surveys, 399-458, 2003.
[2] Ruud M. Bolle and z ang. przeł. Mirosław Korzeniowski: Biometria. Warszawa, 2008.
[3] Wiskott L., Fellous J.M., von den Malsburg C., Face recognition by elastic bunch graph matching. IEEE Trans. Patt. Anal. Mach. Intell. 19, 775–779, 1997.
[4] Smiatacz M. and Malina W.: Automatyczne rozpoznawanie twarzy - metody, problemy, zastosowania, Techniki komputerowe 1/2007, 2007.
[5] Turk M., Pentland A.: Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 3(1), 71-86, 1990.
[6] Cootes T., Taylor C.: Active Shape Models - "Smart Snakes". Proc. British Mach. Vis. Conf. 1992, 266-275, 1992.
[7] Łubkowki P., Laskowski D.: Test of the multimedia services implementation in information and communication networks, Advances in Intelligent Systems and Computing (accepted for publication in 2014), Switzerland: Springer International Publishing AG.
[8] Laskowski, D., Łubkowski, P., Kwaśniewski, M.: Identification of suitability services for wireless networks, Przeglad Elektrotechniczny 89 (9), pp. 128-132, 2013.
[9] Łubkowki P., Laskowski D.: The end-to-end rate adaptation application for real-time video monitoring, Advances in Intelligent Systems and Computing, Springer International Publishing AG, Switzerland, Volume 224, 2013, pp 295-305, 2013.
[10] Sobczak M., Praca magisterska: Implementacja i testowanie systemu identyfikacji osób wykorzystującego dane z monitoringu IP, Warszawa, 2013.

otrzymano / received: 12.06.2014
przyjęto do druku / accepted: 01.08.2014 *artykuł recenzowany / revised paper*