Adam Dąbrowski
Damian Cetnarowicz
Tomasz Marciniak
Paweł Pawłowski

Ograniczenia i tendencje rozwojowe monitoringu wizyjnego na tle przepisów i europejskich norm technicznych

Prof. dr hab. inż. Adam Dąbrowski – kieruje Pracownią Układów Elektronicznych i Przetwarzania Sygnałów Katedry Sterowania i Inżynierii Systemów na Wydziale Informatyki Politechniki Poznańskiej. Jest specjalistą w zakresie cyfrowego przetwarzania sygnałów, systemów multimedialnych i projektowania układów mikroelektronicznych. Jest członkiem wielu organizacji i towarzystw naukowych oraz komitetów naukowych i redakcyjnych czasopism oraz konferencji krajowych i zagranicznych. Aktualnie jest Przewodniczącym Oddziałów: Signal Processing oraz Circuits and Systems Polskiej Sekcji IEEE (*Institute of Electrical and Electronics Engineers*).

Dr inż. Damian Cetnarowicz – adiunkt w Pracowni Układów Elektronicznych i Przetwarzania Sygnałów Katedry Sterowania i Inżynierii Systemów na Wydziale Informatyki Politechniki Poznańskiej. W roku 1997 uzyskał tytuł magistra inżyniera w zakresie Elektroniki i Telekomunikacji. W 2008 r. otrzymał stopień doktora w dziedzinie Automatyka i Robotyka. W badaniach naukowych zajmuje się cyfrowym przetwarzaniem sygnałów z wykorzystaniem algorytmów sztucznej inteligencji.

Dr inż. Tomasz Marciniak – adiunkt w Pracowni Układów Elektronicznych i Przetwarzania Sygnałów Katedry Sterowania i Inżynierii Systemów na Wydziale Informatyki Politechniki Poznańskiej. W roku 1994 uzyskał tytuł magistra inżyniera w zakresie Elektroniki i Telekomunikacji. W 2003 r. otrzymał stopień doktora w dziedzinie Automatyka i Robotyka. W badaniach naukowych zajmuje się głównie analizą efektywnej implementacji algorytmów biometrycznych, cyfrowego przetwarzania sygnałów w systemach multimedialnych z wykorzystaniem procesorów sygnałowych.

Dr inż. Paweł Pawłowski – adiunkt w Pracowni Układów Elektronicznych i Przetwarzania Sygnałów Katedry Sterowania i Inżynierii Systemów na Wydziale Informatyki Politechniki Poznańskiej. W roku 2000 uzyskał tytuł magistra inżyniera w zakresie Elektroniki i Telekomunikacji. W 2007 r. otrzymał stopień doktora w dziedzinie Automatyka i Robotyka. W badaniach naukowych zajmuje się głównie cyfrowymi procesorami sygnałowymi, mikrokontrolerami i problematyką dokładności obliczeń.

Streszczenie

W rozdziale przedstawiono przepisy i normy techniczne (zarówno krajowe, jak i europejskie) dotyczące systemów nadzoru i monitoringu wizyjnego oraz systemów biometrycznych ze szczególnym uwzględnieniem analizy twarzy oraz tęczówki oka ludzkiego.

Abstract

This chapter presents regulations and technical norms (both Polish and European) concerning inspection and vision monitoring systems as well as biometric systems with particular attention paid to the face and human eye iris recognition.

1. Wprowadzenie

Korzystanie z systemów monitoringu miejskiego jest najwygodniejszą, najszybszą, najbardziej wiarygodną i najbardziej skuteczną metodą rozpoznawania zdarzeń wymagających powiadomienia i interwencji ze strony służb ratownictwa i nadzoru publicznego, np. na terenach zurbanizowanych.

Metody tego typu są dużo lepsze niż powiadamianie o zdarzeniach przez samych mieszkańców np. za pomocą telefonów alarmowych, ponieważ, jak podaje Centrum Projektów Informatycznych na swojej stronie internetowej „nawet aż 76 % zgłoszeń w Wojewódzkim Centrum Powiadamiania Ratunkowego (WCPR) w Poznaniu jest fałszywych lub nie wymaga żadnej interwencji służb".

Z zagadnieniami monitoringu wizyjnego wiążą się techniki biometrycznego rozpoznawania ludzi zwłaszcza na podstawie analizy twarzy oraz tęczówki oka ludzkiego, które są coraz częściej stosowane np. do zautomatyzowanej kontroli dostępu.

Na obecnym etapie rozwoju tych technik potrzebne jest jednak opracowanie szczegółowych, precyzyjnych i restrykcyjnych przepisów prawnych oraz norm technicznych dotyczących ich stosowania, aby coraz bardziej rozpowszechniane techniki monitoringu i rozpoznawania biometrycznego nie przekształcały się w systemy niekontrolowanej, a nawet totalnej inwigilacji.

Analizowane w niniejszym rozdziale krajowe i europejskie przepisy prawne oraz normy techniczne wyznaczają nie tylko zasady projektowania i eksploatowania, w tym przechowywania zbieranych danych, ale także kierunki dalszego rozwoju i nowe właściwości systemów nadzoru wizyjnego i biometrycznego. Dotyczą więc tych systemów, które są stosowane obecnie oraz tych, które dopiero powstaną i będą stosowane w przyszłości.

2. Normalizacja dozorowanych systemów CCTV w Polsce i w Europie jako systemów zabezpieczeń

Możliwości przechowywania, przetwarzania i wykorzystywania danych zbieranych na podstawie monitoringu wizyjnego, a tym samym perspektywy rozwoju tych technologii reguluje szereg przepisów o różnym stopniu szczegółowości i obszarach zastosowania. Szczególne znaczenie dla rozwoju systemów monitoringu w Polsce mają normy europejskie i krajowe dotyczące budowy i eksploatacji systemów dozoru CCTV (ang. *closed circuit television*).

Europejska norma EN 50132 (oznaczona w Polsce jako PN-EN 50132) zawiera grupę technicznych standardów dotyczących systemów monitoringu [EN50132-1]. Norma ta została zdefiniowana przez właściwy Europejski Komitet Normalizacyjny, który nadał jej tytuł „Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach" (ang. *Alarm systems – CCTV surveillance systems for use in security applications*) [CENELEC]. Główne części tej normy to[1]:

PN-EN 50132-1:2012 Wymagania systemowe [EN50132-1]

PN-EN 50132-5-1:2012 Transmisja wideo – Ogólne wymagania eksploatacyjne [EN50132-5-1]

[1] Następujące części normy: PN-EN 50132-2-1 Kamery telewizji czarno-białej, PN-EN 50132-4-1 Monitory czarno-białe oraz PN-EN 50132-5 Teletransmisja zostały, dzięki rozwojowi technologicznemu, wycofane. Stan aktualny na dzień 14.01.2014 r.

PN-EN 50132-5-2:2012 Transmisja wideo – Protokoły sieciowe (IP) dotyczące transmisji wideo [EN50132-5-2]

PN-EN 50132-5-3:2013 Część 5-3 Transmisja wideo – Analogowa i cyfrowa transmisja wideo [EN50132-5-3]

PN-EN 50132-7:2013 Wytyczne stosowania [EN50132-7].

Norma PN-EN 50132-1 wyszczególnia minimalne wymagania dotyczące systemów dozorowych CCTV w zastosowaniach dotyczących zabezpieczenia, minimalne wymagania funkcjonalne i eksploatacyjne konieczne do akceptacji zarówno przez klienta, jak i dostarczyciela usług. Norma ta dotyczy także systemów CCTV współdzielących z innymi systemami dozoru takie zasoby systemowe jak: środki wykrywania, wyzwalania, połączeń wewnętrznych, sterowania, komunikacji i zasilania [EN50132-1].

Norma EN 50132-5-1 definiuje minimalne wymagania eksploatacyjne dotyczące transmisji wideo, bezpieczeństwa i jej zgodności z podstawowymi zasadami połączeń IP, podstawowe zasady strumieniowania wideo, kontrolę strumienia, komunikaty zdarzeń oraz funkcje rozpoznania i opisu [EN50132-5-1].

Część 5-2 (norma EN 50132-5-2) bazuje na wymaganiach określonych w części 1, szczegółowo określa wymagania dotyczące protokołów, technologii, modeli transmisji, powiadomień, komunikatów, obsługi błędów i innych detali technicznych dotyczących protokołów sieciowych, wykorzystywanych do transmisji wideo i komunikacji pomiędzy elementami cyfrowych systemów CCTV [EN50132-5-2].
Część 5-3 (norma EN 50132-5-3) szczegółowo określa pozostałe (nie wykorzystujące sieci IP) interfejsy i techniki transmisji wideo, tj. dotyczące sygnałów analogowych oraz sygnałów cyfrowych bez kompresji.

Część 7 (norma EN 50132-7) zawiera ogólne wskazówki implementacyjne dotyczące doboru elementów składowych, planowania, instalowania, przekazywania do eksploatacji, obsługi i technik testowania systemów CCTV [EN50132-7].

2.1. Stopnie bezpieczeństwa

Norma europejska EN 50132-1:2010 określa cztery stopnie bezpieczeństwa (ang. *grades of security*). Dany stopień bezpieczeństwa wynika z poziomu zagrożenia wyrażanego

prawdopodobieństwem wystąpienia zdarzenia i potencjalnymi stratami wynikającymi z konsekwencji tego zdarzenia [EN50132-1]:

1) Stopień 1 – zagrożenie niskie (brak dodatkowych zabezpieczeń, brak dodatkowych ograniczeń);
2) Stopień 2 – zagrożenie niskie do średniego (niski poziom zabezpieczeń, proste ograniczenia dostępu);
3) Stopień 3 – zagrożenie średnie do wysokiego (konieczny wysoki poziom bezpieczeństwa, złożone ograniczenia dostępu);
4) Stopień 4 – zagrożenie wysokie (konieczny bardzo wysoki poziom bezpieczeństwa, bardzo złożone ograniczenia dostępu).

2.2. Integralność danych

Zabezpieczenie dowolnego systemu telewizji przemysłowej lub dozorowej CCTV jest uzależnione od integralności systemu oraz integralności przesyłanych danych. Integralność danych jest kontrolowana trzema mechanizmami:

1) identyfikacja danych (dokładne określenie źródła pochodzenia danych, czasu, daty itp.);
2) autentykacja danych (zabezpieczenie przed modyfikacjami, usuwaniem lub dodawaniem danych);
3) bezpieczeństwo danych (zabezpieczenie przed nieautoryzowanym dostępem do danych).

W przypadku gdy system umożliwia eksport danych, sama operacja ich eksportu nie może modyfikować ich pierwotnej postaci. System powinien umożliwiać określenie przez użytkownika źródła eksportowanych danych (wideo) oraz zakresu czasowego [EN50132-1].
Systemy zaliczane do działających zgodnie ze stopniami bezpieczeństwa 3 i 4 powinny zapewniać metody weryfikacji integralności danych i metadanych (tj. skróconych opisów innych, często złożonych danych). Przykładowe możliwe do zastosowania techniki to: znak wodny, suma kontrolna i oznakowanie celowe (ang. *fingerprint*).

System CCTV stopnia 4, w celu zabezpieczenia przed niepowołanym przeglądaniem danych przez osoby bez właściwych uprawnień, musi realizować kodowanie danych. Dodatkowo system o najwyższym stopniu bezpieczeństwa powinien zapewniać metodę bezpiecznego

kopiowania i eksportowania danych. Wszystkie metody użyte w systemie muszą być precyzyjnie zdefiniowane w dokumentacji systemu [EN50132-1].

2.3. Kontrola dostępu

Dostęp do danych w systemie CCTV powinien być kontrolowany w celu rozróżnienia przypisanych uprawnień. Dla systemów trzeciego i czwartego stopnia bezpieczeństwa uprawnienia administratora i super-użytkownika powinny pozwalać na następujące operacje [EN50132-1]:

1) podgląd danych uzyskiwanych z monitorowanego obszaru, w tym danych wideo;
2) przegląd danych zarejestrowanych, w tym danych wideo (jeśli nie ma innych przeszkód);
3) przegląd informacji o przechowywaniu danych, jeżeli są one częścią systemu telewizji przemysłowej;
4) drukowanie i zapisywanie obrazów;
5) eksport danych i obrazów;
6) usuwanie danych i obrazów (wymagane jest dodatkowe potwierdzenie).

2.4. Parametry techniczne

Norma europejska EN 50132-5-1:2011 specyfikuje szereg technicznych parametrów dotyczących transmisji sygnału wideo w systemach CCTV [EN50132-5-1].

W systemach, w których realizowane są usługi wymagające określenia czasu, należy stosować tzw. oznaczenie czasu (ang. *time stamping*), gdy czas musi być określony z dokładnością od 1 ms do 50 ms opcjonalnie można zaimplementować protokół NTP w wersji 3 (ang. *network time protocol*, zob. także RFC 1305). Adres IP serwerów czasu powinien być udostępniany przez serwer DHCP (ang. *dynamic host configuration protocol*) w opcji Network Time Server. Rozróżnia się cztery klasy dokładności czasowej od T1 do T4, których dokładność transmisji strumienia wideo sięga od 80 ms (dla T1) do 1 ms (dla T4) [EN50132-5-1].

Należy zwrócić uwagę, że czas połączenia (ang. *interconnection time*), który upływa przy inicjowaniu transmisji strumienia ze źródła do wybranego odbiornika, powinien być uwzględniany szczególnie w systemach ze zmotoryzowanymi kamerami typu PTZ, co jest skrótem utworzonym od P – obrót (ang. *pan*), T – pochylanie (ang. *tilt*), Z – zbliżenie (ang.

zoom). Kamery PTZ obserwują otoczenie, wykonując zaprogramowany ruch bądź są sterowane ręcznie. Czas połączenia powinien być znacznie krótszy niż czas związany z jedną sekwencją danej kamery (ang. *dwell time of the camera sequence*) [EN50132-5-1]. Urządzenia transmisji wideo powinny charakteryzować się maksymalnym czasem ustanowienia połączenia każdego nowego strumienia od 2000 ms (tzw. kasa 1) do 250 ms (tzw. klasa 4) [EN50132-5-1].

Inne wymagania wydajnościowe dotyczące strumieniowania wideo, wskazywane przez normę [EN50132-5-1], zebrano w tabeli 2.1.

Tab. 1. Wymagania eksploatacyjne dotyczące strumieniowania wideo

Typ parametru	Zakres (obejmuje stopnie bezpieczeństwa od 1 do 4)
Maksymalny międzyszczytowy odchył czasu pakietu RTP (ang. *peak-to-peak RTP packet jitter*, RTP – *real-time transport protocol*)	20–160 ms
Maksymalny dozwolony czas niedostępności urządzenia	30–189 s
Maksymalny czas rozpoznania braku sygnału	2–8 s

W systemach CCTV często stosuje się wiele niekompatybilnych standardów strumieniowania wideo i sterowania strumieniowaniem. W opisywanej normie EN 50132-5-1:2011 [EN50132-5-1] wprowadzono więc ogólne wymagania dla zastosowań współczesnych standardów strumieniowania. Protokoły transmisji wideo zebrano w tabeli 2, dokonując podziału ze względu na wykorzystywane protokoły warstwy transportowej, w tym dwa najważniejsze, tj. TCP i UDP (ang. TCP – *transport control protocol*, UDP – *user datagram protocol*) oraz najważniejszy protokół warstwy sieciowej – IP (ang. IP – *internet protocol*). Prawa kolumna tabeli 2 zawiera odpowiadające numery dokumentów RFC (ang. *request for comments* – dokumenty źródłowe, najczęściej stanowiące podwaliny pod dokumenty normatywne).

Tab. 2. Wymagania dotyczące strumieniowania wideo

Protokół transportowy	**Numer RFC**
RTP za pomocą UDP/IP	RFC 3550 – protokół RTP użyty w połączeniu z RFC 2326 i RFC 4566
HTTP za pomocą TCP/IP	RFC 2616
RTP za pomocą TCP	RFC 4571
JPEG za pomocą RTP	RFC 2435
JPEG za pomocą HTTP	RFC 793

Druga część powyżej omówionej normy, tj. norma EN 50132-5-2:2011 szczegółowo definiuje protokoły transmisji wideo [EN50132-5-2]. Spośród ponad 600 stron technicznego tekstu warto zwrócić uwagę na zasady tworzenia pakietów dla kodeków audio i wideo w protokole RTP [EN50132-5-2]. W tabeli 3 zebrano najpopularniejsze kodeki (ang. *codec* – koder/dekoder) audio i wideo oraz związane z nimi dokumenty RFC.

Tab. 3. Wymagania dotyczące kodowania, dekodowania i strumieniowania wideo

Kodek		**Numer RFC**
wideo	Motion JPEG	RFC 2435
	MPEG-2	RFC 2250
	MPEG-4 SP/ASP	RFC 3016, RFC 3640
	H.264 AVC	RFC 3984
audio	G.726	RFC 3551
	MPEG-1 Layer II i II	RFC 2250
	AAC	RFC 3640

W załączniku II normy EN 50132-5-2:2012 prezentowane są usługi internetowe (ang. *web services*) związane z protokołem IP [EN50132-5-2]. Część ta zawiera omówienie przypadków różnych scenariuszy zarówno dla sieci LAN (sieci lokalne), jak i WAN (sieci rozległe). Opis dotyczy wielu procedur, począwszy od wdrożenia sieciowych nadajników wideo NVT (ang. *network video transmitter*) poprzez fazę konfiguracji, a skończywszy na fazie strumieniowania w czasie rzeczywistym w sieciach LAN i WAN. Skoncentrowano się na interfejsie pomiędzy sieciowym nadajnikiem wideo NVT, a ujściem sygnału, w tym przypadku sieciowym klientem wideo NVC (ang. *network video client*). W normie uwzględniono także automatyczne rozpoznawanie urządzeń, konfigurację urządzeń, opis zdarzeń, sterowanie kamerami zmotoryzowanymi PTZ, analizę sygnału wideo oraz funkcje strumieniowania w czasie rzeczywistym [EN50132-5-2].

2.5. Eksploatacja usług internetowych

Zgodnie z normą EN 50132-5-2:2012 wszystkie funkcje konfiguracyjne i zarządzające powinny być dostępne poprzez internetowe usługi sieciowe [EN50132-5-2].

Pojęcie internetowych usług sieciowych (ang. *web services*) jest związane z unifikacją metod integracji aplikacji z użyciem otwartych, niezależnych od platform sprzętowych i programowych standardów takich jak: format XML (język znaczników, ang. *extensible markup language*), protokół SOAP 1.2 Part 1 (protokół zdalnego dostępu do obiektów, ang. *simple object access protocol*) i język WSDL 1.1 (język opisu usług sieciowych, ang. *web services description language*), powszechnie wykorzystywanych w sieciach IP. Format XML jest wykorzystywany jako składnia opisu danych, protokół SOAP zapewnia przesył wiadomości, a WSDL służy do opisu usług. Wszystkie wykorzystywane usługi wymieniają dane za pomocą wspólnego schematu XML, a poszczególne usługi są rozróżniane za pomocą odpowiednich klauzul [EN50132-5-2] i są dostarczane jako dokumenty w języku WSDL. Język WSDL jest normalizowany przez konsorcjum W3C [WSDL].

3. Karta demokratycznego stosowania monitoringu wizyjnego

Przepisy i dozwolone zasady stosowania monitoringu wideo zebrano w tzw. Karcie demokratycznego stosowania monitoringu wizyjnego w miastach europejskich (ang. *Charter for the democtratic use of video-surveillance in European cities*)[2] sformułowanej przez

[2] http://www.cctvcharter.eu/index.php?id=31555&L=yfrdzljjxhgjv [dostęp: 18.12.2014 r.].

Europejskie Forum Bezpieczeństwa Miejskiego[3] (ang. EFUS – *European Forum for Urban Security*) [CHARTER]. Celem karty jest zagwarantowanie obywatelom, że systemy monitoringu wizyjnego będą wykorzystywane zgodnie z poszanowaniem ich praw i wolności. Gwarancja ta jest bardzo istotna, ponieważ systemy CCTV:

1) wpływają na wolność mieszkańców na terenie monitorowanym;
2) są rozbudowywane żywiołowo i w sposób przekraczający pierwotne założenia np. ze względu na ciągły i szybki rozwój technologiczny;
3) są lub mogą być powodem zaniepokojenia, niepewności, poczucia inwigilacji i dyskomfortu wśród mieszkańców.

Karta definiuje siedem podstawowych zasad dotyczących demokratycznego stosowania monitoringu wizyjnego [CHARTER]:

1) zasada legalności: projektowanie i rozwój systemu monitoringu wizyjnego może następować tylko w zgodzie z obowiązującym prawem i przepisami;
2) zasada niezbędności: instalacja systemu monitoringu wizyjnego musi być uzasadniona;
3) zasada proporcjonalności: projekt, instalacja, obsługa i późniejszy rozwój systemów monitoringu wizyjnego muszą odbywać się rozsądnie i stosownie do potrzeb;
4) zasada przejrzystości: władze, które wprowadzają miejski system monitoringu wizyjnego, muszą mieć jasną i spójną strategię jego działania;
5) zasada odpowiedzialności: prawo do prowadzenia obserwacji i rejestracji obrazu w przestrzeni publicznej za pomocą systemu monitoringu wizyjnego jest zarezerwowane dla wąskiej grupy ściśle określonych i uprawnionych do tego typu działalności podmiotów – podmioty te są odpowiedzialne za systemy instalowane w ich imieniu;
6) zasada niezależnej kontroli: w celu utrzymania skutecznego działania systemu monitoringu wizyjnego należy wprowadzić wskaźniki skuteczności oraz kontrole zewnętrzne;
7) zasada udziału obywateli: należy dołożyć wszelkich starań, aby zachęcić obywateli do angażowania się we wszystkie etapy funkcjonowania systemu monitoringu wizyjnego.

[3] http://www.efus.eu [dostęp: 18.12.2014 r.].

Karta demokratycznego stosowania monitoringu wizyjnego przewiduje plany na przyszłość. Miasta, które podpisały tę Kartę, powinny dołożyć wszelkich starań, aby dotrzymać jej stosowania i upowszechniania jej zasad w wymiarze lokalnym oraz krajowym. Zobowiązują się także do ciągłej wymiany informacji w zakresie rozwoju i ewolucji technologicznej w dziedzinie monitoringu oraz mają dążyć do wprowadzenia europejskich oznaczeń i certyfikacji. W Karcie przedstawiono pomysł zdefiniowania wspólnego języka systemu monitoringu wizyjnego dla obywateli Europy, co przełożyłoby się na utworzenie europejskiego znaku określającego obszary będące pod nadzorem kamer [CHARTER].

Warto także wspomnieć o konferencji The city under surveillance – personnel, legal aspects, and technology of CCTV (Inwigilacja miasta – obsługa, aspekty prawne i technologia CCTV), która miała miejsce w Częstochowie w dniach 19–20 maja 2011 r. Zdarzenie to było okazją do promocji polskojęzycznej wersji karty EFUS[4] powstałej z inicjatywy miasta Sosnowiec i Akademii Monitoringu Wizyjnego.

4. Normy biometryczne

Zastosowanie biometrii jako dziedziny, w której bada się możliwości wykorzystania naturalnych, biologicznych, ludzkich cech w celu identyfikacji osób, wymaga opracowania kolejnych przepisów i norm technicznych określających granice stosowania tych narzędzi i powszechność ich zastosowań. Przepisy i normy biometryczne definiują następujące zagadnienia:

1) formaty wymiany danych biometrycznych;
2) interfejsy aplikacji komputerowych;
3) prezentację wyników testów;
4) wymagania dotyczące sprawozdań z testów.

Rozróżnia się cztery główne kategorie norm biometrycznych:

1) interfejsy połączeniowe;
2) formaty wymiany danych;
3) profile aplikacji;
4) testowanie wydajności i sposób raportowania.

[4] http://www.cctvcharter.eu/index.php?id=31838&L=woiwxipxpdu [dostęp: 18.12.2014 r.].

Do organów instytucjonalnych, zajmujących się normowaniem w zakresie biometrii należą:

1) INCITS M1 (ang. *International Committee for Information Technology Standards* M1) – komitet ten składa się z pięciu niezależnych grup roboczych:
    a) biometryczne interfejsy połączeniowe (ang. *biometric technical interfaces*),
    b) formaty wymiany danych biometrycznych (ang. *biometric data interchange formats*),
    c) profile aplikacji biometrycznych (ang. *biometric profiles*),
    d) testowanie wydajności i sposoby raportowania (ang. *biometric performance testing and reporting*),
    e) społeczne aspekty zastosowań biometrii (ang. *societal aspects of biometric implementations*);

2) JTC1/SC37 (ang. *Joint Technical Committee 1/Subcommittee 37*) – komitet składa się z sześciu grup roboczych, które ściśle współpracują z grupami INCITS M1:
    a) zharmonizowany słownik biometryczny (ang. *harmonized biometric vocabulary*),
    b) biometryczne interfejsy techniczne (ang. *biometric technical interfaces*),
    c) formaty wymiany danych biometrycznych (ang. *biometric data interchange formats*),
    d) funkcjonalna architektura biometryczna i profile pokrewnych (ang. *biometric functional architecture and related profiles*),
    e) testy biometryczne i ich raportowanie (ang. *biometric testing and reporting*),
    f) powiązane aspekty prawne i społeczne (ang. *cross-jurisdictional and societal aspects*);

3) OASIS (ang. *Organization for the Advancement of Structured Information Standards*);

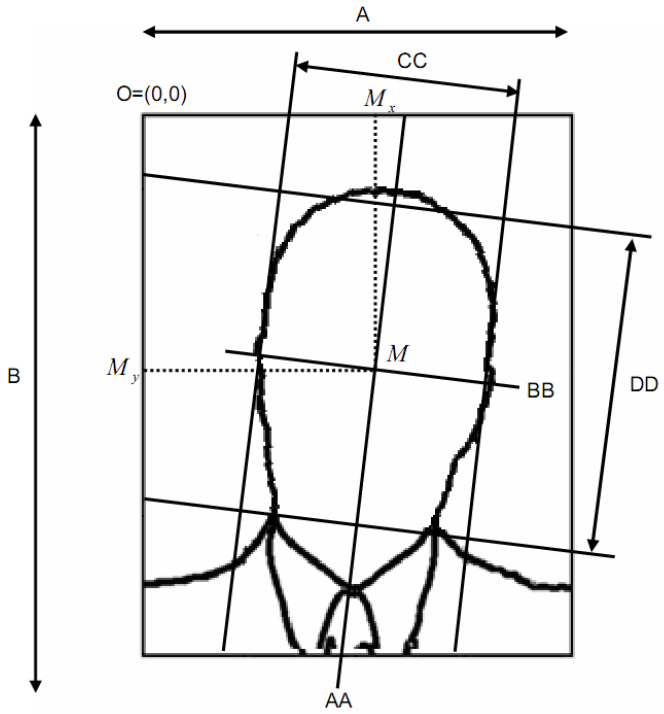
4) NIST (ang. *National Institute of Standards and Technology*).

4.1. Analiza najważniejszych norm biometrycznych

Przy realizacji systemów wykorzystujących biometrię należy uwzględnić postanowienia normatywne związane z przetwarzaniem danych. Poniżej skupiono się na przetwarzaniu obrazów i normach definiujących rozpoznawanie osób na podstawie analizy twarzy oraz tęczówki oka.

4.1.1. Ujęcie twarzy

Zagadnienie problemu właściwego ujęcia twarzy określają normy ANSI/INCITS 385-2004, (ang. *Information technology – Face Recognition Format for Data Interchange*) oraz ISO/IEC 19794-5:2005 (*Information technology – Biometric data interchange formats – Part 5: Face image data*).



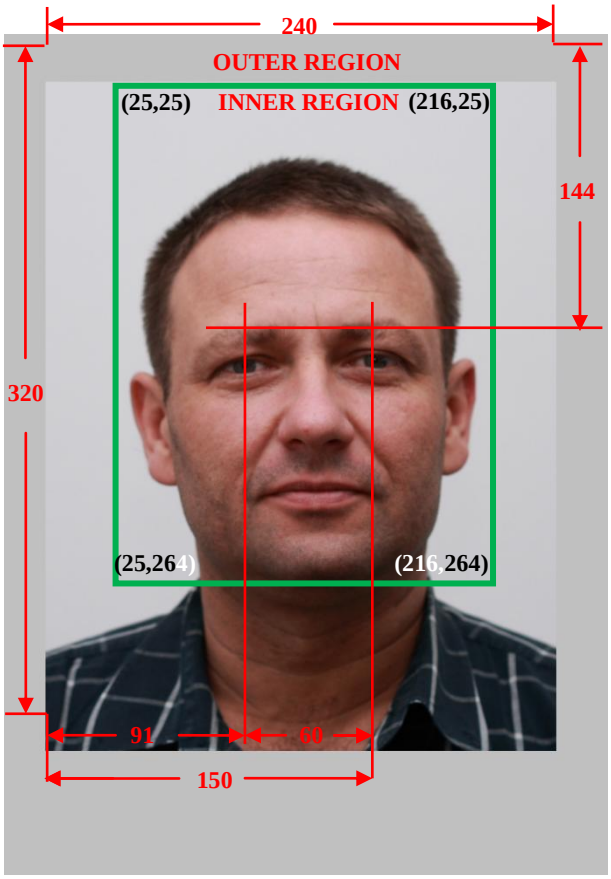
Rys. 1. Wymiary opisujące ujęcie twarzy [ISO1]

Rysunek 1 ilustruje sposób opisu ujęcia twarzy na potrzeby sformułowania wymagań dalszego przetwarzania obrazu. Linia AA leży w pobliżu środka ust i środka nosa. Linia BB przechodzi przez środek lewego oka i środek prawego oka. Przecięcie linii AA z linią BB wyznacza punkt M, który jest centralnym punktem twarzy. Współrzędna Mx powinna zawierać się w przedziale od 45 do 55 % szerokości obrazu A. Współrzędna My powinna zawierać się w przedziale od 30 do 50 % wysokości obrazu B. Szerokość twarzy CC powinna zawierać się w przedziale od 50 do 75 % wartości A, natomiast wysokość twarzy DD powinna zawierać się w przedziale od 60 do 90 % wartości B. Rotacja twarzy mierzona wzdłuż każdej z osi AA i BB powinna zawierać się w zakresie 0±5°. Rotacja mierzona wzdłuż osi prostopadłej do AA i BB powinna zawierać się w zakresie 0±8°. Stosunek wysokości obrazu i szerokości, czyli B/A powinien zawierać się w zakresie od 1,25 do 1,34 [ANSI1, ISO1].

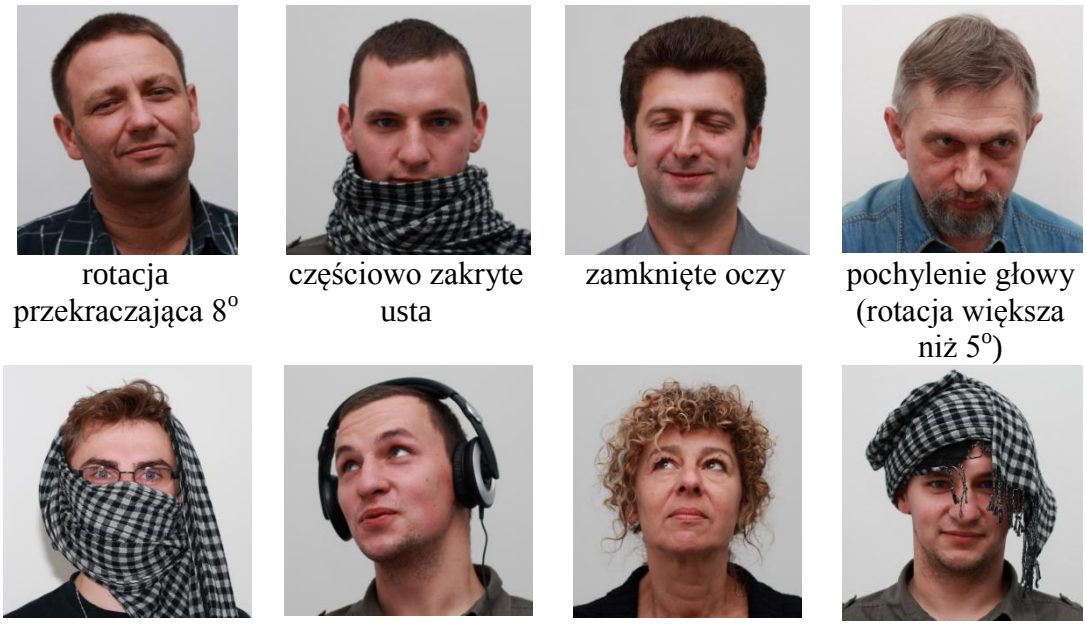
4.1.2. Definicja obszaru wewnętrznego i zewnętrznego, przykłady ułożenia twarzy

Na rysunku 2 zaprezentowano obraz, który spełnia wszystkie kryteria poprawności zgodnie z normą ISO/IEC JTC1/SC37 N506 (ang. *Biometric Data Interchange Formats Part 5: Face Image Data*) [ISO2]. Na tym rysunku zaznaczono charakterystyczne odległości w obrazie twarzy na obrazie o rozdzielczości 320×240 pikseli (odległości wyrażono w pikselach), przy czym dodatkowo zaznaczono granicę między obszarem wewnętrznym i zewnętrznym.

Na rysunku 3 przedstawiono natomiast przykłady niewłaściwych ujęć twarzy według normy ISO/IEC JTC1/SC37 N506 (ang. *Biometric Data Interchange Formats Part 5: Face Image Data*) [ISO2].



Rys. 2. Odległości (w pikselach) pomiędzy charakterystycznymi punktami twarzy [ISO2]



Rys. 3. Przykłady niewłaściwych ujęć twarzy

4.1.3. Jakość obrazów i cechy ujęć

Jakość obrazów i cechy ujęć definiują normy ISO/IEC JTC1/SC37N 1477: (ang. *Biometric Sample Quality Standard – Part1: Framework*) oraz ISO/IEC JTC1/SC37 N1477: (ang. *Biometric Sample Quality – Part 5: Face Image Data Sample Quality*) [ISO3, ISO4]. Analizę normy [ISO1] podjęto w pracy [JITA2009]. Najbardziej istotne cechy określające jakość obrazu ujęto w tabeli 4.

Norma ISO/IEC JTC 1/SC 37 N 1977 (ang. *Text 29794-5, Biometric Sample Quality – Part 5: Face Image Data Sample Quality*) [ISO5] definiuje również algorytmy do dynamicznej regulacji następujących parametrów w procesie akwizycji:

1) jasność obrazu;
2) kontrast obrazu;
3) postrzegany kontrast obrazu;
4) postrzegany kontrast obrazu z uwzględnieniem częstotliwości przestrzennych;
5) odległość osoby od aparatu (kamery).

Tab. 4. Najbardziej istotne cechy określające jakość obrazu

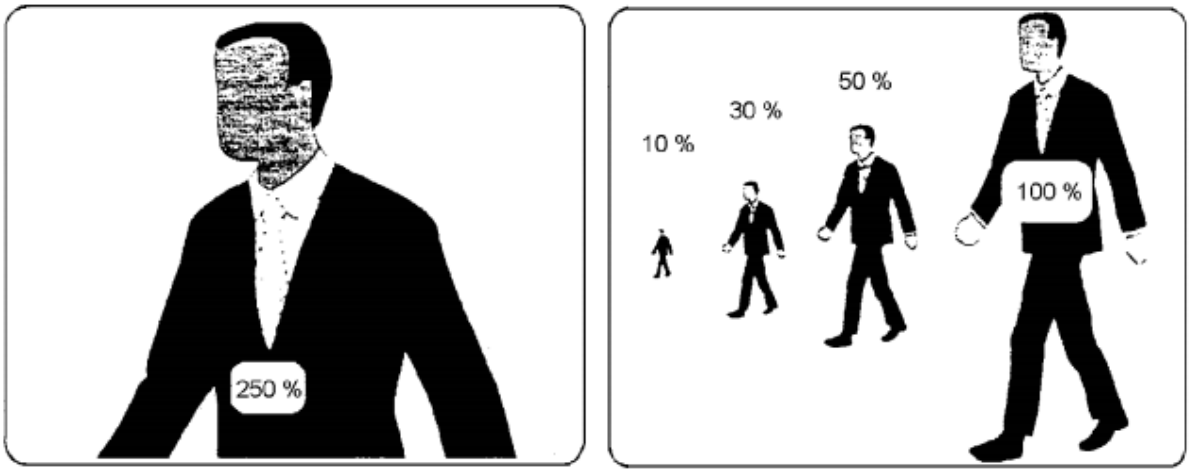
grupa cech	cecha	stan właściwy – opis ograniczeń
ujęcie (widok)	postawa	minimalizująca odchylenie
	oświetlenie	równomierne, bez cieni
	tło	kolor jednolity
	oczy	• otwarte i wyraźnie widoczne • odległość między oczami min. 60 pikseli
	okulary	bez odbić, ciemny odcień lub grube oprawki
	usta	zamknięte, wyraźnie widoczne
fotografia	odległość od aparatu (kamery)	umiarkowany rozmiar głowy
	kolor	neutralny, bez efektu czerwonych oczu
	ekspozycja	odpowiednia jasność
reprezentacja cyfrowa	ostrość	Bez nieostrych obszarów (dobra ostrość)
	rozdzielczość	• Rozmiar obrazu z twarzą – szerokość × wysokość 240 pikseli × 320 pikseli (stosunek 1:1,333, QVGA) • wysokość głowy 0,78'' – 300 dpi • szerokość głowy 0,5'' – 480 dpi • reprezentacja kolorów 24-bit (RGB), 8 bit (monochromatyczny) • JPEG/JPEG2000 standard kompresji • obszar wewnętrzny – maks. kompresja dla odcieni szarości z JPEG lub JPEG2000 10:1 • obszar wewnętrzny – maks. kompresja dla kolorów z JPEG 20:1, dla kolorów z JPEG2000 10:1 • obszar zewnętrzny – maks. kompresja dla odcieni szarości z JPEG lub JPEG2000 30:1 • obszar zewnętrzny – maks. kompresja dla kolorów z JPEG 60:1, dla kolorów z JPEG2000 30:1

4.1.4. Wykrywanie osób w systemie CCTV

W celu zapewnienia wymaganej skuteczności i niezawodności rozpoznawania obiektów za pomocą systemów monitoringu wizyjnego (tzw. systemów CCTV) zalecany rozmiar (w tym także rozdzielczość) obiektów obserwowanych na ekranie monitora powinien być związany z zadaniem, które wykonuje operator np.: identyfikacja, rozpoznawanie, wykrywanie lub sterowanie.

W przypadku gdy obserwowanym obiektem jest osoba, a rozdzielczość obrazu w zainstalowanym systemie CCTV przekracza 400 linii (systemy analogowe pracujące w formacie D1, 4CIF, a także większość systemów hybrydowych i cyfrowych, w tym wszystkie tzw. mega-pikselowe), wówczas mają zastosowanie następujące zalecenia dotyczące rozmiaru obiektu [EN50132-7] (rysunek 4):

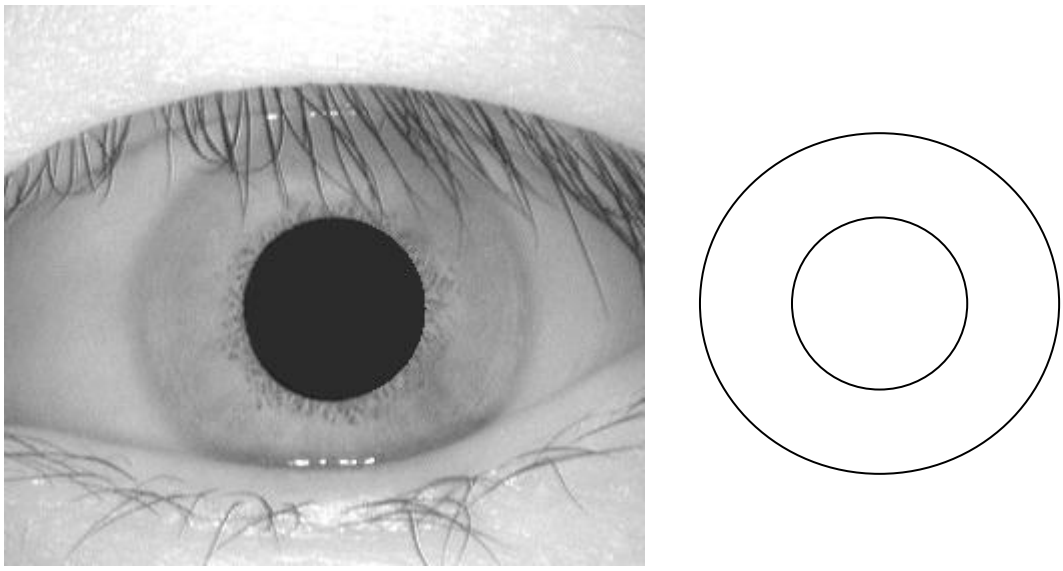
1) dla celów ogólnej identyfikacji, obiekt powinien zajmować co najmniej 20 % wysokości ekranu;
2) w sytuacjach precyzyjnej identyfikacji, obiekt powinien zajmować co najmniej 50 % wysokości ekranu;
3) w zadaniach wykrywania intruza, obiekt powinien zajmować co najmniej 10 % wysokości ekranu;
4) w zadaniach kontroli, tłum – obiekt powinien zajmować co najmniej 5 % wysokości ekranu.



Rys. 4. Schemat zalecanego minimalnego rozmiaru obserwowanych obiektów [EN50132-7]

4.1.5. Obraz tęczówki oka

Norma ISO/IEC 19794-6:2005 (ang. *Biometric data interchange formats – Part 6: Iris image data*) [ISO6], dotycząca tęczówki oka, definiuje strukturę danych zwaną DBD (ang. *biometric data block* – biometryczny blok danych), która zawiera cyfrowy format zapisu. Rysunek 5 pokazuje przykład obrazu tęczówki z obrazem kołowym (bez segmentacji).



Rys. 5. Obraz tęczówki oka (lewa strona) i obraz kołowy (prawa strona)

4.1.6. Specyfikacja BioAPI

Norma ISO/IEC 19784-1:2006 (ang. *Biometric application programming interface – Part 1: BioAPI specification*) [ISO7] określa zasady integracji technik wykorzystujących algorytmy biometryczne. Umożliwia aplikacjom programowym komunikację z jedną lub większą liczbą modułów zrealizowanych w różnych technologiach biometrycznych. Norma zawiera definicje struktur, które powinny być zaimplementowane w celu realizacji interfejsu programowania aplikacji API (ang. *application programming interface*).

5. Podsumowanie

Przedstawiona w tym rozdziale analiza przepisów i norm technicznych dotyczących monitoringu wizyjnego oraz systemów biometrycznych powinna być brana pod uwagę przy opracowywaniu, tworzeniu, projektowaniu i eksploatacji systemów monitoringu wizyjnego. Jest ona również ważna przy rozwijaniu nowych metod zarówno zbierania, przechowywania jak i analizy danych wizyjnych oraz biometrycznych.

Bibliografia

[EN50132-1] PN-EN 50132-1:2012 Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1. Wymagania systemowe, EN 50132-1-2010, *Alarm systems – CCTV surveillance systems for use in security applications – Part 1. System requirements*, 2012

[EN50132-5-1] PN-EN 50132-5-1:2012 Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 5-1. Transmisja wideo – Ogólne wymagania eksploatacyjne, EN50132-5-1:2011 *Alarm systems – CCTV surveillance systems for use in security applications, Part 5-1 Video transmission - General video transmission performance requirements,* 2012

[EN50132-5-2] PN-EN 50132-5-2:2012 Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 5-2. Transmisja wideo – Protokoły sieciowe (IP) dotyczące transmisji wideo, EN50132-5-2:2011 *Alarm systems – CCTV surveillance systems for use in security applications, Part 5-2 IP Video Transmission Protocols,* 2012

[EN50132-5-3] PN-EN 50132-5-3:2013 Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 5-3. Transmisja wideo – Analogowa i cyfrowa transmisja wideo, EN 50132-5-3:2012 *Alarm systems – CCTV surveillance systems for use in security applications – Part 5-3: Video transmission – Analogue and digital video transmission,* 2013

[EN50132-7] PN-EN 50132-7:2013 Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 7. Wytyczne stosowania, EN 50132-7:2012 *Alarm systems – CCTV surveillance systems for use in security applications – Part 5-3: Video transmission – Analogue and digital video transmission*, 2013

[CENELEC] European Committee for Electrotechnical Standardization homepage, www.cenelec.eu

[CHARTER] European Forum for Urban Security, Karta demokratycznego zastosowania monitoringu wizyjnego, *Charter for the democratic use of videosurveillance in European cities*, http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_EN.pdf

[WSDL] Web Services Description Language (WSDL) 1.1 W3C Note 15 March 2001 http://www.w3.org/TR/wsdl, 2001

[ANSI1] ANSI/INCITS 385-2004, "Information technology – Face Recognition Format for Data Interchange", 2004

[ISO1] ISO/IEC 19794-5:2005, "Information technology – Biometric data interchange formats – Part 5: Face image data", 2004

[ISO2] ISO/IEC JTC1/SC37 N506, "Biometric Data Interchange Formats Part 5: Face Image Data", 2004

[ISO3] ISO/IEC JTC1/SC37N 1477: Biometric Sample Quality Standard – Part1: Framework, 2006

[ISO4] ISO/IEC JTC1/SC37 N1477:Biometric Sample Quality – Part 5: Face Image Data Sample Quality, February12, 2007

[ISO5] ISO/IEC JTC 1/SC 37 N 1977, Text of Working Draft 29794-5, Biometric Sample Quality – Part 5: Face Image Data Sample Quality, 2007

[ISO6] ISO/IEC 19794-6:2005, Biometric data interchange formats – Part 6: Iris image data, 2005

[ISO7] ISO/IEC 19784-1:2006, Biometric application programming interface – Part 1: BioAPI specification

[JITA2009] Jitao S., Zhen L., S.Z. Li, *Face Image Quality Evaluation for ISO/IEC Standards 19794-5 and 29794-5*, Lecture Notes in Computer Science 2009, nr 5558