BIAŁA KSIĘGA

Prywatność w dozorze wizyjnym

Narzędzia i technologie do ochrony prywatności

Grudzień 2023

AXIS COMMUNICATIONS

Streszczenie

Rozwiązania z zakresu dozoru muszą być zgodne z lokalnymi, regionalnymi lub innymi obowiązującymi przepisami dotyczącymi ochrony prywatności, które nakładają pewne ograniczenia dotyczące zbierania danych osobowych.

Jest parę narzędzi i technologii, które pomagają chronić prywatność osób w ramach dozoru.

- **Maski dynamiczne** anonimizują osoby lub pojazdy w materiale wizyjnym w czasie rzeczywistym. Aplikacja analityczna AXIS Live Privacy Shield oferuje wspomagane przez sztuczną inteligencję maskowanie dynamiczne w wybranych kamerach w celu wykrywania i maskowania osób bądź tablic rejestracyjnych. W przypadku wszystkich zgodnych kamer udostępnia też funkcję maskowania dynamicznego opartego na ruchu w celu maskowania wszystkich poruszających się obiektów.
- **Maskowanie statyczne** powoduje ukrywanie wybranego obszaru przez nałożenie trwałej maski na cały podgląd na żywo i nagrany materiał wizyjny. Jest to standardowa funkcja produktów Axis z zakresu sieciowych systemów wizyjnych i świetnie się sprawdza w przypadku scen wewnętrznych lub zewnętrznych ze stałymi obszarami, których nie wolno monitorować.
- Funkcji **edycji wideo** dostępnej w oprogramowaniu do zarządzania materiałem wizyjnym (VMS) można użyć, gdy trzeba wyeksportować materiał wizyjny, na przykład na potrzeby prac wyjaśniających, a jednocześnie zapewnić ochronę prywatności uwiecznionych na nagraniu osób postronnych.
- **Dozór za pomocą innych urządzeń**

  Kamery termowizyjne generują obrazy na podstawie ciepła emitowanego przez obiekty. Rejestrowane są tylko sylwetki — bez jakichkolwiek szczegółów umożliwiających identyfikację osób.

  Radary w systemach dozoru zapewniają detekcję, ale nie generują żadnych danych umożliwiających identyfikację osób.
- **Analizy** materiału wizyjnego lub audio mogą służyć do monitorowania sceny i wyzwalania działań, gdy coś odbiega od normy. Aplikacje analityczne mogą też wizualizować dane na monitorach bez zapisywania jakichkolwiek nagrań.

Właściciel systemu dozoru odpowiada za zapewnianie zgodności z przepisami dotyczącymi ochrony prywatności.

Spis treści

1 Wprowadzenie

Istnieją różne opcje ochrony prywatności w ramach dozoru wizyjnego. Można na przykład blokować pewne obszary w polu widzenia kamery, maskować osoby na obrazie wideo albo prowadzić dozór przy użyciu innych technologii.

W niniejszym dokumencie przedstawiono najważniejsze narzędzia i technologie służące do rozwiązywania problemów związanych z prywatnością podczas rejestrowania, zapisywania, przeglądania i eksportowania materiału wizyjnego z systemu dozoru.

2 Informacje podstawowe

Coraz częściej stosuje się dozór w miejscach publicznych, ponieważ obywatele zaczynają rozumieć, jak może on zwiększać ich bezpieczeństwo. Prywatność zawsze była priorytetem w branży dozoru, jednak świadomość ludzi na temat ich praw wzrosła dzięki takim inicjatywom jak RODO (Rozporządzenie o ochronie danych osobowych) w Europie czy FISMA (Federalna ustawa o zarządzaniu bezpieczeństwem informacji) w USA.

Zarówno w sferze publicznej, jak i prywatnej obowiązują wytyczne oraz przepisy władz lokalnych i regionalnych, a także związków zawodowych i stowarzyszeń, dotyczące dozoru wizyjnego i ochrony prywatności. Regulacje te mają na celu ochronę praw człowieka przez dbanie o poszanowanie praw ludzi do prywatności. Dlatego wprowadzane są mechanizmy kontroli, które trzeba wdrażać — w zakresie rejestrowania, przechowywania i udostępniania danych wizyjnych.

To właściciel systemu dozoru musi dbać, by jego system dozoru był zgodny ze wszystkimi obowiązującymi lokalnymi i międzynarodowymi przepisami dotyczącymi ochrony prywatności. Jednak producenci i dostawcy mogą pomagać klientom być na bieżąco z najlepszymi praktykami w zakresie dozoru. Dotyczy to też prawidłowego i etycznego korzystania z zebranych danych oraz podejmowania niezbędnych kroków w celu zapewnienia zgodności z przepisami.

3 Maskowanie materiału wizyjnego

Dostępne są różne techniki ukrywania wybranych obszarów lub anonimizacji osób w materiale wizyjnym z systemu dozoru.

W przypadku dostępności wszystkich rodzajów maskowania można wybrać maskowanie w postaci jednolitego koloru lub mozaiki (pikselowe). Maskowanie przy użyciu jednolitego koloru zapewnia najlepszą ochronę prywatności, ponieważ umożliwia jednoczesne obserwowanie ruchów. W przypadku maskowania

w postaci mozaiki poruszające się obiekty lub ludzie są widoczni w bardzo niskiej rozdzielczości, co pozwala na lepsze rozróżnianie form przez obserwację rzeczywistych kolorów obiektów.

Maska w postaci koloru i w postaci mozaiki.

3.1 Maskowanie dynamiczne

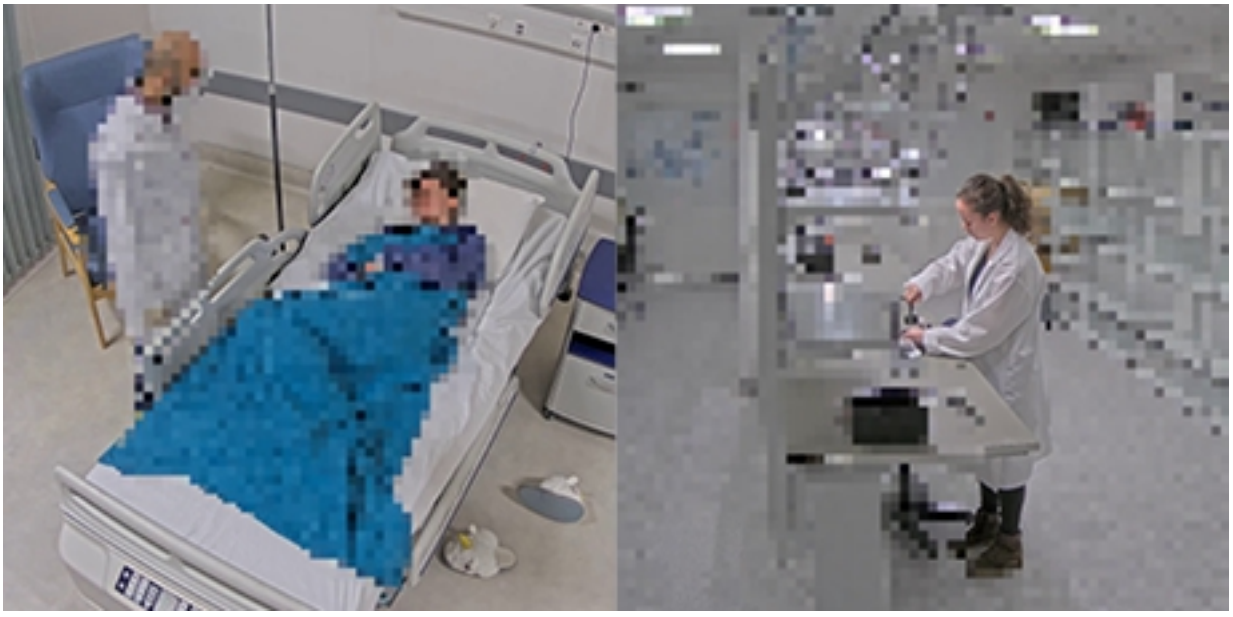
Dzięki tej technice funkcje analiz wideo automatycznie anonimizują osoby znajdujące się w polu widzenia kamery. Odbywa się to w czasie rzeczywistym, ponieważ funkcje analiz monitorują działania i ruchy w ramach sceny.

Aplikacja analityczna AXIS Live Privacy Shield zainstalowana na kamerze udostępnia wspomagane przez sztuczną inteligencję maskowanie dynamiczne w przypadku kamer wideo.

3.1.1 Maskowanie wspomagane przez sztuczną inteligencję

Funkcja ta jest obsługiwana przez wybrane kamery wyposażone w jednostkę głębokiego uczenia (deep learning processing unit — DLPU). Dzięki maskowaniu wspomaganemu przez sztuczną inteligencję aplikacja analizuje przekazywany na żywo obraz wideo w celu wykrywania osób lub tablic rejestracyjnych. Można

wybrać maskowanie osób (zarówno poruszających się, jak i nieruchomych), twarzy lub tablic rejestracyjnych. Metodę maskowania można też odwrócić, aby zamiast osób lub twarzy było maskowane tło.



Maskowanie osób i maskowanie tła w narzędziu AXIS Live Privacy Shield.

AXIS Live Privacy Shield umożliwia dynamiczne maskowanie wspomagane przez sztuczną inteligencję z prędkością do 10 klatek na sekundę. Nadaje się to do wewnętrznych i zewnętrznych scen bliskiego zasięgu w takich miejscach jak zakłady produkcyjne, szpitale, domy opieki, hotele, szkoły, biura czy sklepy.

Dzięki funkcji maskowania wspomaganego przez sztuczną inteligencję maski będą aktywne nawet wtedy, gdy znajdujące się w polu dozoru osoby nie ruszają się przez długi czas.

3.1.2 Strumienie z maskowaniem i bez maskowania

Maskowanie za pomocą narzędzia AXIS Live Privacy Shield jest trwałe, tj. nie można go usunąć z materiału wizyjnego po nagraniu. Można jednak skonfigurować aplikację tak, aby przesyłała strumień wideo z maskowaniem, a osobno również strumień bez maskowania. W niektórych programach do zarządzania materiałem wizyjnym (video management software — VMS) można skonfigurować prawa dostępu do poszczególnych strumieni.

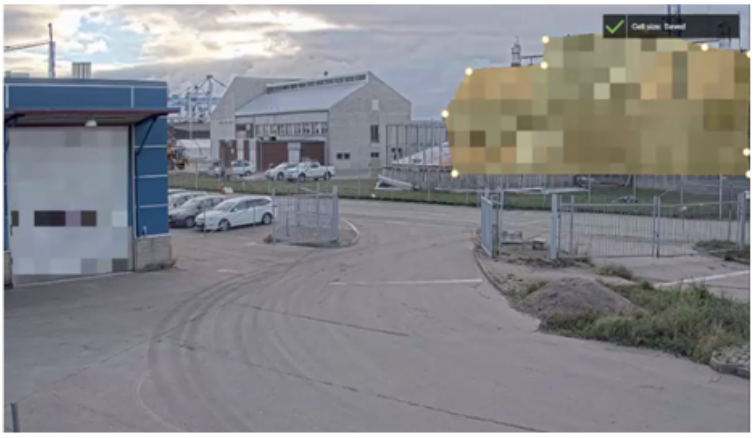
Można zatem zapisać strumień bez maskowania, ale będą mogli go zobaczyć tylko upoważnieni pracownicy. Jeśli tożsamość osób uchwyconych na nagraniu okaże się kluczowa dla jakiegoś śledztwa, będzie można uzyskać dostęp do takich informacji. Równoległe rejestrowanie takich strumieni nie tylko ułatwia ochronę osób fizycznych z poszanowaniem ich praw do prywatności, ale też pozwala na wywiązywanie się z obowiązków właściciela systemu dozoru w zakresie zapewnienia bezpieczeństwa osobom, zwłaszcza w otwartych przestrzeniach publicznych.

3.2 Maskowanie statyczne

Stosowanie statycznych masek prywatności świetnie się sprawdza w przypadku dozoru we wnętrzach budynków lub na zewnątrz, jeśli obejmuje on stałe obszary, których nie wolno monitorować. Funkcja ta ukrywa wybrany obszar, nakładając trwałą (nieprzezroczystą lub mozaikową) maskę na wszystkie obrazy rejestrowane na żywo oraz zarejestrowany materiał. W przypadku maski mozaikowej dany obszar jest

widoczny w bardzo niskiej rozdzielczości, dzięki czemu można obserwować aktywność, ale nie widać szczegółów umożliwiających identyfikację.

Stosowanie statycznych masek prywatności od dawna jest standardem w produktach Axis. Można je łączyć ze stosowaniem masek dynamicznych za pomocą narzędzia AXIS Live Privacy Shield.



Zastosowanie statycznej maski prywatności w postaci wielokątnej mozaiki w celu trwałego zablokowania dozoru budynku.

Maskowanie określonych obszarów w celu zapobiegania niezamierzonemu dozorowi jest szczególnie przydatne w przypadku kamer PTZ (z funkcją obrotu, pochylenia i zbliżenia) ze względu na ich duży zasięg i szeroki kąt widzenia. W przypadku kamer PTZ statyczne maski prywatności są powiązane z układem współrzędnych kamery. Dzięki temu maskowanie pozostaje na tym samym obszarze sceny nawet wtedy, gdy zmienia się pole widzenia kamery.

4 Edycja materiału wideo

W przypadku udostępniania nagranego materiału wizyjnego może być konieczne zapewnienie zgodności z wszelkimi obowiązującymi przepisami chroniącymi prywatność osób postronnych. Narzędzie do edycji wideo dostępne w pakiecie AXIS Camera Station umożliwia łatwe maskowanie osób lub obszarów widocznych w scenie. Można na przykład zamaskować tylko wybrane poruszające się obiekty lub wszystkie nieruchome i poruszające się obiekty, z wyjątkiem osób będących przedmiotem zainteresowania.

Należy pamiętać, że edycja wideo nie jest możliwa w przypadku podglądu na żywo.

5 Dozór za pomocą innych urządzeń

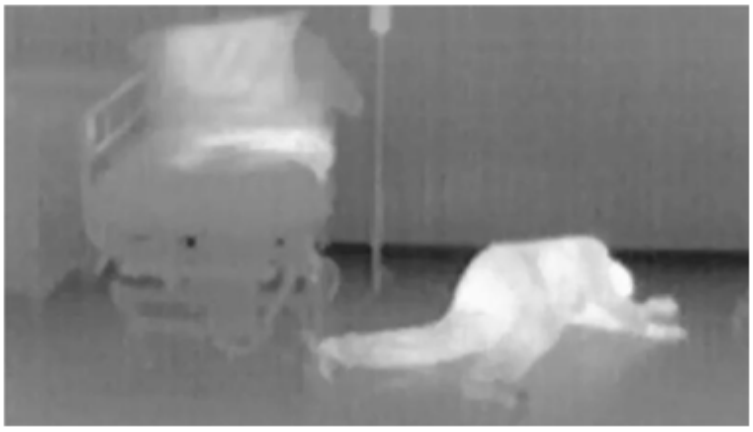
Czasem najlepszą gwarancją ochrony prywatności w systemach dozoru jest stosowanie innych detektorów zamiast zwykłych kamer. Takie rozwiązania sprawdzają się w każdych warunkach pogodowych i przy każdym oświetleniu.

5.1 Obrazowanie termowizyjne

Kamery termowizyjne wykrywają ciepło, a nie światło widzialne. Tworzą obraz na podstawie ciepła emitowanego przez obiekty znajdujące się w polu widzenia kamery, co pozwala na prowadzenie zdalnego

dozoru bez zbierania danych osobowych. Rejestrowane są tylko kształty ruchomych lub nieruchomych obiektów.

Kamery termowizyjne z wbudowanymi funkcjami detekcji i analiz ruchu są przydatne w środowiskach o wysokich wymaganiach dotyczących ochrony prywatności. W takich miejscach jak ośrodki opieki zdrowotnej czy domy opieki dla osób starszych kamery termowizyjne chronią prywatność, a jednocześnie szybko alarmują pracowników o niespodziewanych ruchach. Jeśli pacjent upadnie lub będzie potrzebować pomocy medycznej, personel będzie mógł szybko zareagować.



Kamery termowizyjne umożliwiają zdalny dozór bez szczegółów umożliwiających identyfikację osób.

5.2 Radar

Radar zapewnia pełną ochronę prywatności, ponieważ korzysta z technologii radarowej, a nie wizyjnej.

Radar działa na zasadzie nadawania fal radiowych, ich odbioru i analizy fal odbitych od obiektów znajdujących się w polu detekcji urządzenia. Technologia radarowa w połączeniu z narzędziami analitycznymi zapewnia detekcję ruchu i wyzwalanie alarmów bez zbierania danych osobowych. Znakomicie się nadaje do wykrywania intruzów na dużych przestrzeniach otwartych. Radar może następnie automatycznie powiadamiać pracowników ochrony i uruchamiać komunikaty przez głośniki.

5.3 Narzędzia analityczne

Narzędzia do analizy materiału wizyjnego i audio mogą ułatwiać dozór sceny w czasie rzeczywistym i reakcję w sytuacjach, gdy coś odbiega od normy. Narzędzia analityczne generują metadane, które umożliwiają zrozumienie sceny bez uzyskiwania dostępu do strumienia wideo bądź audio czy zapisywania nagrań. Dane mogą być przedstawiane wizualnie w arkuszach kalkulacyjnych lub na pulpitach albo wyzwalać alarmy w czasie rzeczywistym. Może to pomagać w eliminowaniu obaw dotyczących danych osobowych. Narzędzia do analiz materiału audio mogą wyzwalać alarmy, gdy mikrofon wychwyci określone dźwięki, na przykład krzyki osób, stłuczenie szkła lub inne nietypowe dźwięki.

6 Ochrona danych

Ochrona danych nie wchodzi w zakres zagadnień omawianych w niniejszym dokumencie. Ważnym aspektem ochrony prywatności jest jednak sposób przetwarzania danych pochodzących z systemów dozoru wizyjnego. Więcej informacji można znaleźć na stronie *www.axis.com/about-axis/cybersecurity*.

T10194474/PL/M1.5/2312

O firmie Axis Communications

Axis umożliwia tworzenie mądrzejszego i bezpieczniejszego świata, tworząc rozwiązania zwiększające bezpieczeństwo i wydajność biznesową. Jako firma z branży technologicznej będąca liderem na rynku, Axis oferuje systemy dozoru wizyjnego, kontroli dostępu, domofonowe i rozwiązania audio. Rozwiązania te są wzbogacone o inteligentne aplikacje analityczne i wysokiej jakości szkolenia

Firma Axis zatrudnia około 4000 zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami z sektora technologii oraz integracji systemów na całym świecie, aby dostarczać rozwiązania dla klientów. Firma Axis powstała w 1984 roku, a jej siedziba znajduje się w Lund w Szwecji