XXIII Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2013
Oddział Gdański PTETiS
Referat nr 9

OCHRONA PRYWATNOŚCI W SYSTEMACH MONITORINGU WIZYJNEGO, PRZEGLĄD OPRACOWANYCH ARCHITEKTUR I ALGORYTMÓW

Janusz CICHOWSKI, Andrzej CZYŻEWSKI

Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki
Katedra Systemów Multimedialnych, ul. Narutowicza 11/12, 80-233, Gdańsk
tel: (+58) 347-13-01 fax: (+58) 347-11-14 e-mail: {jay, andcz}@sound.eti.pg.gda.pl

Streszczenie: Nieustannie rozwijające się technologie informacyjne związane z inteligentnym monitoringiem wizyjnym stwarzają ryzyko niewłaściwego wykorzystywania danych osobowych. W celu zapewnienia prawidłowej ochrony materiału wizyjnego, w ramach projektów realizowanych w Katedrze Systemów Multimedialnych WETI PG, opracowany został szereg architektur i algorytmów, które ułatwiają ochronę danych wrażliwych, takich jak: wizerunki osób, numery tablic rejestracyjnych, okna budynków i samochodów oraz prywatne posesje. W referacie opisano podstawy algorytmiczne rozwiązań stosowanych do celów detekcji oraz klasyfikacji obszarów wrażliwych w obrazach wizyjnych. Przedstawiono opracowane algorytmy anonimizacji, których zastosowanie w związku z zaproponowanymi architekturami przepływu informacji umożliwia odwracalną ochronę danych wrażliwych. Odwracalność procesu anonimizacji umożliwia osiągnięcie rozsądnego kompromisu pomiędzy osiąganym poziomem bezpieczeństwa i poszanowaniem prywatności osób postronnych.

Słowa kluczowe: anonimizacja, bezpieczeństwo, steganografia

1. WPROWADZENIE

Rozwój aglomeracji miejskich realizowany w zgodzie z paradygmatem „Inteligentnych Miast" powoduje ekspansję nowoczesnych technologii w obszarze funkcjonowania społeczeństwa. Rozwiązania, których zadaniem jest poprawianie jakości życia, wykorzystywane w niewłaściwy sposób przez niepowołane osoby lub instytucje mogą stanowić zagrożenie. Przykładem takiej technologii jest inteligentny monitoring, którego zadaniem jest ochrona i zapewnienie bezpieczeństwa obywateli. Niewłaściwe zarządzanie, przetwarzanie i przechowywanie pozyskanych danych wizyjnych, jest realnym zagrożeniem ograniczenia prywatności osób postronnych oraz wycieku danych osobowych. Zaprezentowane w niniejszym artykule algorytmy i architektury umożliwiające ochronę danych osobowych zostały opracowane w odpowiedzi na społeczne obawy przed utratą prywatności.

Społeczne zapotrzebowanie na ochronę prywatności nie powinno ingerować w poziom bezpieczeństwa świadczonego przez systemy monitoringu. Rosnąca liczba zagrożeń takich jak wandalizm czy terroryzm uzasadnia stosowanie rozproszonych inteligentnych systemów nadzoru wizyjnego. W celu osiągnięcia kompromisu pomiędzy prywatnością, a bezpieczeństwem Komisja Europejska rozszerzyła Kartę Podstawowych Praw Unii Europejskiej o regulacje związanie z monitoringiem wizyjnym i kwestiami pozyskiwania, przechowywania, zarządzania i usuwania danych wrażliwych. Regulacje definiują typy obiektów wizyjnych klasyfikowanych jako dane wrażliwe, określono również maksymalny okres przechowywania danych, który w zależności od lokalizacji systemu wizyjnego i jego zasięgu wynosi od 7 do 30 dni. Obszar objęty nadzorem wizyjnym powinien być odpowiednio oznaczony, aby osoby znajdujące się zasięgu kamer miały tego świadomość. Każda osoba ma prawo wglądu do materiału wizyjnego zawierającego jej wizerunek lub inne informacje pozwalające na identyfikację.

Opisane regulacje prawne umożliwiają ochronę prywatności od strony legislacyjnej, praktyczna ochrona danych osobowych w systemach monitoringu wizyjnego realizowana jest na poziomie technologii. Kompromis pomiędzy prywatnością i bezpieczeństwem realizowany jest poprzez zastosowanie steganografii [1]. W publicznym kanale transmisyjnym umieszczana jest ukryta wiadomość, którą może odtworzyć wyłącznie osoba znająca klucz szyfrujący. W kontekście ochrony prywatności proces ten nazywany jest anonimizacją odwracalną, gdzie ukrywanymi informacjami są obszary przedstawiające dane osobowe, a publicznym kanałem transmisyjnym jest strumień wizyjny. Podstawy algorytmiczne oraz opracowane architektury przepływu danych zostały opisane w kolejnych rozdziałach.

2. DETEKCJA OBSZARÓW WRAŻLIWYCH

Algorytmy anonimizacji przetwarzają strumień wizyjny w sposób analogiczny do filtracji, wybrane fragmenty obrazu zostają przetworzone tak, aby nie było możliwe ich rozpoznanie. Wynikiem działania algorytmu jest strumień wizyjny pozbawiony danych osobowych. Działanie algorytmów anonimizacji ma charakter binarny (włączony albo wyłączony), bardzo istotne jest przetwarzanie wstępne, którego głównym celem jest detekcja i klasyfikacja obszarów wrażliwych występujących w kolejnych ramkach strumienia wizyjnego.

Proces detekcji obszarów wrażliwych jest kluczowy dla skutecznej ochrony danych osobowych, błędna detekcja lub jej brak może powodować wyciek danych osobowych. W literaturze opisano wiele algorytmów stosowanych w

rzeczywistych systemach monitoringu do detekcji obiektów [2], śledzenia obiektów [3], klasyfikacji obiektów [4], detekcji twarzy [5], detekcji tablic rejestracyjnych [6], wykrywania zdarzeń niebezpiecznych [7].

Analiza strumieni wizyjnych w systemach monitoringu musi być realizowana bez opóźnień, a wyniki przetwarzania powinny być aktualizowane na bieżąco. Dobór optymalnego algorytmu detekcji jest kompromisem pomiędzy czasem trwania i jego skutecznością. Strumień wizyjny podlega przetwarzaniu, które ma na celu określić obszar występowania fragmentów zawierających twarze, tablice rejestracyjne oraz poruszające się obiekty. W celu skutecznej ochrony prywatności każdy z wymienionych obiektów powinien być wpierw wykryty.

Detekcja obiektów ruchomych z szczególnym uwzględnieniem detekcji pojazdów i osób została zrealizowana w oparciu o algorytm modelowania tła [4]. Wszystkie obiekty ruchome, niebędące tłem są wykrywane w strumieniu wizyjnym, następnie obiekty są klasyfikowane do jednej z trzech klas tj. pojazd, człowiek i inne. Klasyfikacja obiektów realizowana jest z wykorzystaniem właściwości geometrycznych (wysokość i szerokość) oraz cech fizycznych (prędkość) zamodelowanych obiektów. Jeżeli obiekt nie spełnia kryteriów przynależności do klas pojazd lub człowiek zostaje zaklasyfikowany jako inny i nie jest brany pod uwagę w trakcie anonimizacji.

Określanie położenia twarzy w ramkach strumieni wizyjnych realizowane jest z wykorzystaniem metody Viola-Jones [5]. Algorytm ten bazuje na cechach Haaro-podobnych oraz korzysta z klasyfikacji kaskadą słabych klasyfikatorów. Metoda ta polega na obliczaniu różnic jasności w przylegających do siebie obszarach w kierunkach horyzontalnym i wertykalnym. Ludzka twarz posiada charakterystyczny rozkład jaśniejszych i ciemniejszych obszarów, dlatego zastosowanie cech Haaro-podobnych umożliwia jej skuteczną detekcję. Obliczone parametry są porównywane ze zbiorem treningowym. Przeszukiwanie całej ramki obrazu w poszukiwaniu odpowiednich cech Haaro-podobnych dla różnych rozmiarów twarzy jest czasochłonne. Możliwe jest przyspieszenie przetwarzania poprzez zawężenie obszaru poszukiwań do fragmentów zaklasyfikowanych przez detektor obiektów ruchomych do klasy człowiek.

Ostatnim zaimplementowanym algorytmem jest detektor tablic rejestracyjnych. W ramach przetwarzania wstępnego realizowany jest szereg niskopoziomowych przekształceń m.in. korekcja obrotu i przeskalowanie. Przygotowana ramka zostaje poddana filtracji dolnoprzepustowej, a następnie realizowany jest splot z jądrem Sobela. Wynikiem przetwarzania jest obraz zawierający kontury obiektów. Ramka obrazu jest przeszukiwana w celu znalezienia skupisk energii tzn. obszarów, w których znajduje się największa liczba krawędzi. Wykryte obszary są analizowane pod kątem dopasowania do kształtu prostokątnego o rozmiarach proporcjonalnych do rzeczywistej tablicy rejestracyjnej. Analogicznie do detektora twarzy, możliwe jest zawężenie obszaru poszukiwań do obszarów zaklasyfikowanych jako pojazd przez detektor obiektów ruchomych.

Algorytmy detekcji obszarów wrażliwych są newralgicznym punktem systemów ochrony prywatności. Skuteczność algorytmów detekcji determinuje skuteczność całego systemu. Istotne jest odpowiednie dobranie algorytmów oraz ich parametrów tak, aby możliwe było przetwarzanie bez opóźnień z zachowaniem wysokiej skuteczności detekcji.

3. ALOGRYTMY ANONIMIZACJI

Procedura anonimizacji polega na usunięciu lub ukryciu danych wrażliwych w taki sposób, aby osoby postronne nie miały możliwości identyfikacji chronionych obiektów. Anonimizacja realizowana w sposób manualny (chroniony obszar jest ręcznie zaznaczany przez operatora) jest powszechnie stosowana w środkach masowego przekazu np. gazetach i telewizji. Zastosowanie analogicznych algorytmów w systemach monitoringu wymusza automatyzację procesu. Bezobsługowa anonimizacja jest możliwa poprzez wykorzystanie informacji pochodzących z modułów detekcji.

Algorytmy anonimizacji można podzielić na dwie grupy: anonimizacja nieodwracalna (prosta) polega na trwałym zniszczeniu fragmentu obrazu, anonimizacja odwracalna (krypto-anonimizacja), umożliwia odzyskanie pierwotnego obrazu pod warunkiem znajomości klucza szyfrującego. Oba typy algorytmów mogą być zastosowane do ochrony prywatności w systemach monitoringu wizyjnego, właściwości poszczególnych algorytmów zostały omówione w kolejnych podrozdziałach.

3.1. Anonimizacja nieodwracalna

Pierwszą grupę algorytmów pozwalających na zapewnienie prywatności w systemach monitoringu wizyjnego stanowią algorytmy anonimizacji prostej. Procedura anonimizacji prostej polega na permanentnym zniekształceniu wybranego fragment obrazu w taki sposób, aby identyfikacja obszaru wrażliwego była niemożliwa. Wycinanie jest najprostszą metodą realizującą powyższe założenia poprzez trwałe wycięcie całego obszaru wrażliwego, reguła matematyczna przedstawiająca proces wycinania dana jest wzorem (1)

$$I_{out}(x,y)=\begin{cases} I_{in}(x,y) & \text{gdy } I_{mask}(x,y)=0 \\ 0 & \text{gdy } I_{mask}(x,y)\neq 0 \end{cases} \quad (1)$$

gdzie: I_{in} – obraz wejściowy, I_{out} – obraz wynikowy, I_{mask} – obraz zawierający maski wykrytych obiektów, x – numer kolumny, y – numer wiersza

I(x,y) prezentuje wartość piksela umieszczonego w dwuwymiarowej przestrzeni w punkcie *(x,y)*. W przypadku, gdy przetwarzany obraz jest reprezentowany w skali szarości to wartość piksela jest związana ze składową luminancji, w przypadku obrazów kolorowych wartość piksela w punkcie *(x,y)* jest wektorem złożonym ze składowych barwnych (np. RGB, YUV). W miejscach występowania binarnej maski piksele obrazu wejściowego są zerowane. Bardziej złożoną metodą anonimizacji prostej jest filtracja Gaussowska przedstawiona wzorem (2).

$$I_{out}(x,y)=\begin{cases} I_{in}(x,y) & \text{gdy } I_{mask}(x,y)=0 \\ I_{in}(x,y)*\left(\frac{1}{2\pi\sigma^2}\cdot e^{\frac{\left(x^2+y^2\right)}{2\sigma^2}}\right) & \text{gdy } I_{mask}(x,y)\neq 0 \end{cases} \quad (2)$$

gdzie: σ – parametr odpowiedzialny za wartość odchylenia standardowego rozkładu Gaussowskiego

Procedura rozmywania Gaussowskiego bazuje na obliczeniu splotu wejściowego obrazu z dwuwymiarowym filtrem Gaussa. Modyfikacja wartości parametru σ wpływa na stopień rozmycia, mniejsze wartości odchylenia standardowego powodują gorszą anonimizację. Kolejnym algorytmem wykorzystywanym w celu ochrony strumieni wizyjnych w sposób nieodwracalny jest algorytm mozaikowania realizowany zgodnie ze wzorem (3).

$$I_{out}(x,y)=\begin{cases} I_{in}(x,y) & \text{gdy } I_{mask}(x,y)=0 \\ \dfrac{1}{m\cdot n}\displaystyle\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} I_{in}\left(\left\lfloor\frac{x}{m}\right\rfloor+i,\left\lfloor\frac{y}{n}\right\rfloor+j\right) & \text{gdy } I_{mask}(x,y)\neq 0 \end{cases} \quad (3)$$

gdzie: m – szerokość ziarna mozaiki, n – wysokość ziarna mozaiki

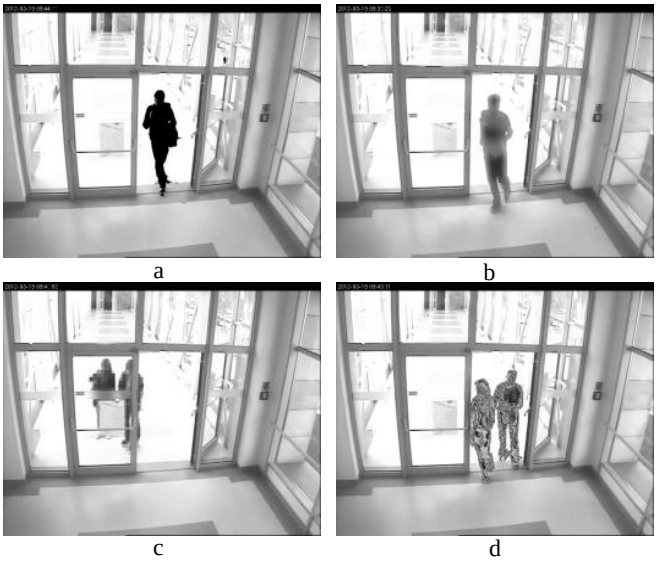
Pierwszym etapem algorytmu jest podział obszaru chronionego na przyległe prostokątne bloki. Rozmiar bloku (ziarno mozaiki) decyduje o jakości anonimizacji, mniejsze ziarno powoduje słabsze zniekształcenia i gorszą anonimizację. W każdym bloku obliczana jest wartość średnia ze wszystkich wartości pikseli znajdujących się w danym bloku. Otrzymana wartość średnia zostaje przypisana do wszystkich pikseli w danym bloku. Ostatnim algorytmem realizującym anonimizację prostą jest opracowany przez autorów algorytm przesuwania bitowego przedstawiony wzorem (4).

$$I_{out}(x,y)=\begin{cases} I_{in}(x,y) & \text{gdy } I_{mask}(x,y)=0 \\ I_{in}(x,y)<<b & \text{gdy } I_{mask}(x,y)\neq 0 \end{cases} \quad (4)$$

gdzie: b – liczba przesuwanych bitów, << – operator przesunięcia bitowego w lewo

Przesunięciu bitowemu podawane są wartości pikseli, będące w zasięgu maski detektora. Zaproponowana metodologia wymaga przetwarzania strumienia wizyjnego przedstawionego z uwzględnieniem przestrzeni barw RGB. Jakość anonimizacji zależna jest od wartości parametru b, który definiuje liczbę bitów przesunięcia, zbyt mała liczba przesuwanych bitów, może powodować wyciek danych osobowych. W wyniku przeprowadzonych eksperymentów empirycznie stwierdzono, że przesunięcie wartości składowych RGB poszczególnych pikseli obrazu o co najmniej dwa bity jest wystarczające do skutecznej ochrony danych osobowych. Przeprowadzenie operacji opisanej wzorem (4) w przestrzeni barw YUV nie jest zalecane, ze względu na możliwość przecieku danych wrażliwych. W przypadku przetwarzania w przestrzeni YUV istotne jest przesunięcie kanału luminancji (Y) o co najmniej sześć bitów, przy jednoczesnym przesunięciu składowych chrominancji (U i V) o co najmniej trzy bity. Algorytm został zaprojektowany z myślą o systemach wbudowanych, gdzie cześć obliczeń może być realizowana po stronie kamery.

Algorytmy opisane w niniejszym rozdziale z wyłączeniem algorytmu przesuwania bitowego są powszechnie znane, jednak zastosowanie ich w połączeniu z autorskimi architekturami przepływu danych pozwalają na realizację odwracalnej ochrony prywatności. Działanie poszczególnych algorytmów przedstawiono na rysunku 1.

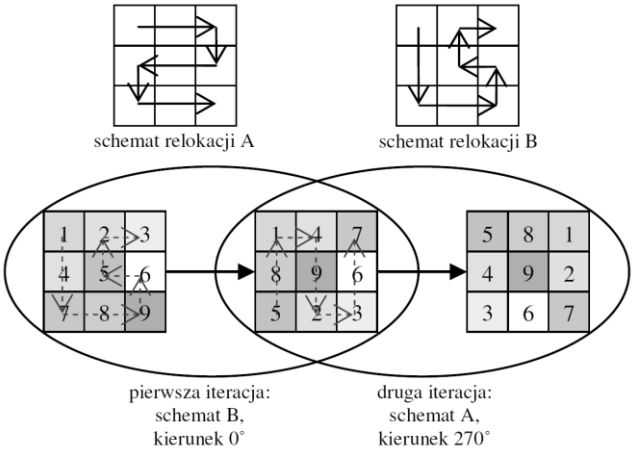


Rys. 1. Anonimizacja prosta obiektów ruchomych z wykorzystaniem algorytmów: a) wycinania, b) rozmywania, c) mozaikowania i d) przesuwania bitowego.

3.2. Anonimizacja odwracalna

Algorytmy anonimizacji prostej są jednokierunkowe co oznacza, że nie istnieje procedura, która umożliwia odzyskiwanie chronionych danych. Ze względu na konieczność zapewnienia bezpieczeństwa i ochrony danych osobowych, został zaimplementowany algorytm anonimizacji odwracalnej. Głównym założeniem było stworzenie algorytmu, który w sposób efektywny realizowałby ukrywanie fragmentów obrazu z zachowaniem możliwości jego późniejszego odtworzenia. Procedura deanonimizacji (odszyfrowania) realizowana jest w przypadku wystąpienia zdarzenia niebezpiecznego.

Zaimplementowany algorytm [8, 9] bazuje na przemieszczeniu pikseli w obrębie całego chronionego obszaru zgodnie z konkretnym schematem relokacji. Możliwe jest zastosowanie kaskady złożonej z kilku realizowanych kolejno schematów relokacji. Metoda realizuje permutacje pikseli w całym przetwarzanym obszarze, wynikowy fragment obrazu po szyfrowaniu przyjmuje charakter kolorowego szumu. Poglądowy przebieg relokacji pikseli z wykorzystaniem dwóch schematów relokacji w obszarze o rozmiarach 3×3 przedstawiono na rysunku 2.



Rys. 2. Algorytm relokacji pikseli

Znajomość schematów relokacji przestrzennej umożliwia zastosowanie odwrotnej procedury i ustawienie wszystkich pikseli na ich początkowych pozycjach. Zaimplementowany algorytm realizuje anonimizację w obszarach prostokątnych, informacja o rozmiarach obszaru, kolejności wykonania relokacji i ich kierunku umożliwia odzyskanie danych wizyjnych, które były ukryte. Szczegóły implementacyjne algorytmu oraz analiza wpływu kompresji stratnej obrazu na jakość chronionych danych zostały opisane w literaturze [8]. Odwracalna anonimizacja twarzy osób oraz tablic rejestracyjnych została przedstawiona na rysunku 3.

a b

Rys. 3. Krypto-anonimizacja: a) twarzy, b) tablic rejestracyjnych

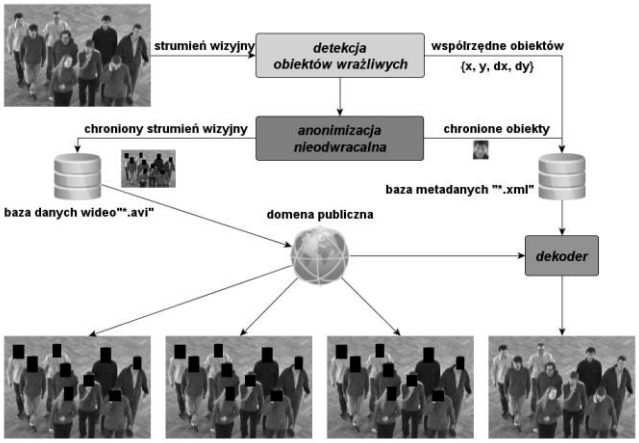
Istotny wpływ na proces ochrony danych wrażliwych ma rozdzielczość kamer wykorzystywanych w systemie monitoringu.. Czas przetwarzania strumienia wizyjnego wysokiej rozdzielczości (ang. High Definition) jest znacznie dłuższy od przetwarzania strumieni niskiej rozdzielczości. Analiza czasu przetwarzania w zależności od rozmiaru obiektu oraz liczby wykrywanych obiektów została przedstawiona przez autorów w literaturze [9].

4. ARCHITEKTURY BEZPIECZNEGO PRZEPŁYWU DANYCH

Zaprezentowane algorytmy realizują ochronę prywatności na poziomie strumieni wizyjnych. Dane wizyjne w systemach monitoringu są zapisywane i przechowywane, z tego względu istotna jest kontrola dostępu oraz ochrona danych na poziomie architektury systemu. Przepływ informacji i rodzaj stosowanych zabezpieczeń jest istotny z punktu widzenia ochrony danych osobowych. Skomplikowanie architektury systemu jest zależne od zastosowanych algorytmów anonimizacji. Poniżej zostały omówione trzy zaproponowane architektury systemów monitoringu wizyjnego, które umożliwiają ochronę prywatności nie wpływając negatywnie na poziom świadczonego bezpieczeństwa.

4.1. Zastosowanie metadanych

Pierwsza zaproponowana architektura wykorzystuje dodatkowy generowany przez system strumień metadanych, który jest zapisywany niezależnie od strumienia wizyjnego. Podejście bazujące na metadanych wymaga oddzielenia danych wrażliwych od strumienia wizyjnego. Obszary przedstawiające dane osobowe są anonimizowane z wykorzystaniem algorytmów anonimizacji nieodwracalnej, następnie dane wrażliwe są transkodowane ze strumienia wizyjnego do strumienia metadanych. W strumieniu metadanych umieszczane są również informacje o zależnościach przestrzenno czasowych pomiędzy dwoma strumieniami. Ideowy schemat blokowy architektury zaprezentowano na rysunku 4.

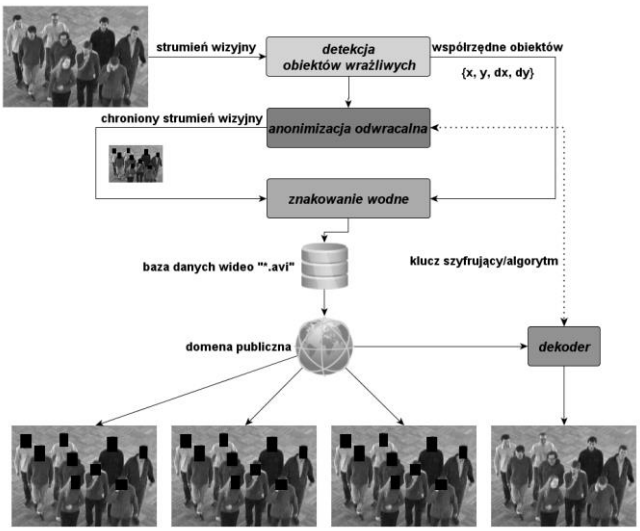


Rys. 4. Architektura systemu monitoringu wizyjnego wykorzystująca metadane do ochrony prywatności

Osoby niepowołane mają dostęp do strumienia wizyjnego pozbawionego danych wrażliwych. W przypadku zajścia zdarzenia niebezpiecznego istnieje możliwość ponownego scalenia danych jedynie przez osoby uprawnione, które mają dostęp do bazy metadanych. Mocną stroną przedstawionego podejścia jest bardzo duże bezpieczeństwo informacji wrażliwych, ponieważ są one całkowicie odseparowane. Wadą tej architektury jest duża ilość generowanych danych.

4.2. Zastosowanie cyfrowego znakowania wodnego

Ze względu na konieczność stosowania dwóch baz danych w pierwszym zaprezentowanym podejściu opracowano alternatywne rozwiązanie, które umożliwia ochronę prywatności jedynie z wykorzystaniem bazy danych wizyjnych. Wykryte obszary wrażliwe zostają poddane procesowi anonimizacji odwracalnej, a informacje o przestrzennej lokalizacji i rozmiarach zaszyfrowanych obiektów ukrywane są w postaci znaków wodnych [8]. Schemat blokowy systemu wykorzystującego cyfrowe znakowanie wodne został przedstawiony na rysunku 5.



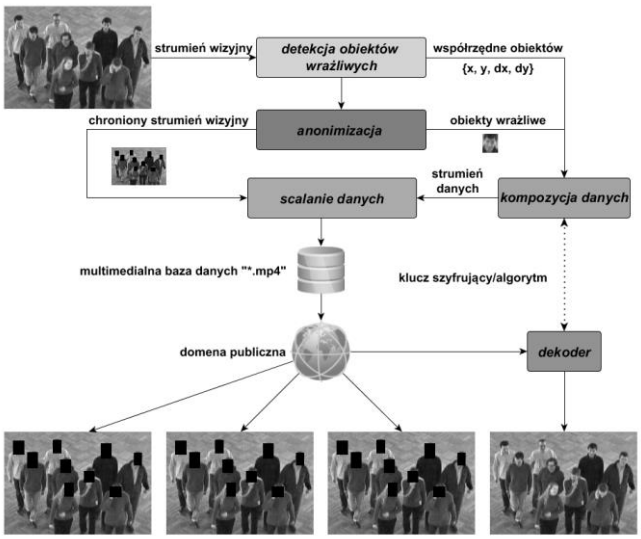
Rys. 5. Architektura systemu monitoringu wizyjnego wykorzystująca znakowanie wodne do ochrony prywatności

Ochrona prywatności realizowana jest przez algorytm krypto-anonimizacji, osoby uprawnione mogą odtworzyć pierwotny strumień wizyjny, jeśli dysponują prawidłowym kluczem szyfrującym. W celu automatycznej deanonimizacji

wymagana jest ekstrakcja znaku wodnego, który zawiera informacje o przestrzennym rozmieszczeniu i rozmiarach obiektów chronionych. Informacje te są niezbędne do poprawnego odszyfrowania chronionych obszarów, jednak są one podatne na zniszczenie poprzez np. zastosowanie silnej kompresji stratnej. Uszkodzenie znaku wodnego powoduje bezpowrotną utratę możliwości odszyfrowania chronionych danych.

4.3. Zastosowanie kontenera multimedialnego

Połączenie funkcjonalności obu omówionych rozwiązań przyczyniło się do powstania architektury wykorzystującej rozbudowany kontener multimedialny. Omówione dotychczas rozwiązania przechowują wyłącznie materiał wizyjny. Zaobserwowano, że w systemach monitoringu wizyjnego, niewykorzystywane są pozostałe modalności dostępne w nowoczesnych kontenerach multimedialny np. MPEG4, który umożliwia transport danych wizyjnych, fonicznych oraz dowolnych metadanych. Strumienie wizyjne poddawane są przetwarzaniu w celu detekcji obszarów wrażliwych. Wykryte obszary są anonimizowane dowolnym typem algorytmu. Symultanicznie informacje wrażliwe są transkodowane do modalności audio [9] lub metadanych. Jeżeli zastosowany algorytm anonimizacji był odwracalny możliwe jest umieszczenie tylko informacji o zależnościach przestrzenno czasowych poszczególnych obszarów chronionych. Oba strumienie danych umieszczane są w jednym kontenerze multimedialnym i składowane w bazie danych. Procedura odzyskania chronionych danych jest możliwa, ale wymagana jest znajomość procesu anonimizacji. Dekoder powinien znać parametry transkodowania, rodzaj wykorzystanej modalności oraz klucz szyfrujący. Schemat blokowy architektury przedstawiono na rysunku 6.



Rys. 6. Architektura systemu monitoringu wizyjnego wykorzystująca rozbudowany kontener multimedialny do ochrony prywatności

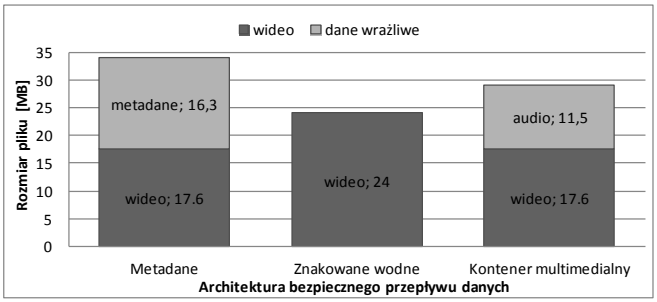
4.4. Porównanie

Przedstawione architektury realizują skuteczną ochronę danych osobowych jednocześnie zachowując możliwość ich odtworzenia przez uprawnione osoby. Zaprezentowane rozwiązania nie są uniwersalne, charakteryzują je różne wymagania sprzętowe, różne złożoności obliczeniowe i niejednakowa pojemność danych. Porównanie architektur zostało zestawione w tablicy 1.

Tablica 1. Porównanie architektur realizujących ochronę danych osobowych w systemach monitoringu wizyjnego

	Metadane	Znakowanie wodne	Kontener danych
złożoność obliczeniowa	mała	duża	bardzo duża
ochrona danych osobowych	bardzo skuteczna	skuteczna	skuteczna
ryzyko utraty danych	małe	duże	małe
odporność na kompresję stratną	bardzo duża	mała	średnia
ilość generowanych danych	bardzo duża	średnia	duża
max. liczba chronionych obiektów	bez ograniczeń	max. 20 obiektów	max. 8 obiektów
przepływność danych multimedialnych	średnia 1500 kbps	duża 3000 kbps	bardzo duża 4500 kbps

Wyniki przedstawione w tablicy 1 zostały otrzymane poprzez wykonanie eksperymentów i analizę czasów przetwarzania oraz ilości generowanych danych dodatkowych z użyciem ujednoliconego zbioru testowego. Dane wizyjne były przetwarzane w każdej z zaproponowanych architektur bezpiecznego przepływu danych. Ilość danych dodatkowych generowanych w procesie anonimizacji strumienia wizyjnego przedstawiono na rysunku 7.



Rys. 7. Objętość plików wyjściowych powstałych w wyniku anonimizacji strumienia wizyjnego przy wykorzystaniu zaproponowanych architektur przepływu danych

Plik testowy, na którym została przeprowadzona powyższa analiza zawierał strumień wizyjny o długości 60 sekund zapisany z w rozdzielczości PAL (704×576). Strumień został zarejestrowany z szybkością 15 ramek na sekundę, objętość pliku wejściowego wynosiła 17.6 MB.

5. PODSUMOWANIE

Zaprezentowane algorytmy i architektury dają możliwość zwiększenia poczucia prywatności w miejscach publicznych oraz ograniczenie społecznej awersji do systemów nadzoru wizyjnego. Odpowiednia konfiguracja zaprezentowanych algorytmów umożliwia skuteczną ochronę danych osobowych. Istotnym aspektem dotyczącym projektowania systemów monitoringu jest odpowiednie zaplanowanie i uwzględnienie kwestii dotyczących prywatności osób postronnych. Lokalizacja systemu monitoringu, zasoby sprzętowe i dostępna moc obliczeniowa będą miały wpływ na dobór zastosowanych algorytmów.

Ochrona prywatności w miejscach publicznych nie może wpływać negatywnie na bezpieczeństwo osób i mienia. Zaprezentowane wyniki prac badawczo rozwojowych dowodzą, że aktualny stan techniki pozwala na implementację mechanizmów ochrony prywatności będących rozszerzeniem istniejących systemów monitoringu.

5. BIBLIOGRAFIA

1 J. A. Bloom, I. J. Cox, J. Fridrich, T. Kalker, M. L. Miller, "Digital Watermarking and Steganography" Boston 2008, ISBN: 9780123725851

2 A. Czyżewski, P. Dalka, "Moving Object Detection and Tracking for the Purpose of Multimodal Surveillance System in Urban Areas", New Directions in Intelligent Interactive Multimedia: Studies in Computational Intelligence, pp. 75–84, 2008, ISSN: 1860-949X, ISBN: 978-3-540-68126-7

3 Z. Han, Q. Ye, J. Jiao, "Online feature evaluation for object tracking using Kalman filter", 19th International Conference on Pattern Recognition, pp. 1–4, 2008, ISBN 978-1-4244-2174-9

4 D. Ellwart, A. Czyżewski, "Viewpoint independent shape-based object classification for video surveillance", 12th International Workshop on Image Analysis for Multimedia Interactive Services, Delft, Netherlands, 2011, ISBN: 978-94-90818-00-5

5 P. Viola, M. Jones, "Robust Real-Time Face Detection" International Journal of Computer Vision, vol. 57, no. 2, pp. 137-154, Netherlands 2004

6 H. Sheng, C. Li, Q. Wen, Z. Xiong, "Real-Time Anti-Interference Location of Vehicle License Plates Using High-Definition Video" IEEE Intelligent Transportation Systems Society, vol. 1, issue 4, pp. 17-23, Winter 2009, ISSN: 2229-5518 4

7 P. Zhang, T. Thomas, S. Emmanuel, M. S. Kankanhalli, "Privacy Preserving Video Surveillance Using Pedestrian Tracking Mechanism", Proceedings of the 2nd ACM workshop on Multimedia in Forensics, Security and Intelligence (MiFor '10), pp. 31-36, October 2010, ISBN: 978-1-4503-0157-2

8 J. Cichowski, A. Czyżewski, "Reversible Video Stream Anonymization for Video Surveillance Systems Based on Pixels Relocation and Watermarking", IEEE 13th International Conference on Computer Vision Workshops (ICCV2011), Workshop on Visual Surveillance, pp. 1971-1977, November 2011, ISBN: 978-1-4673-0062-9

9 J. Cichowski, A. Czyżewski, B. Kostek, "Visual Data Encryption for Privacy Enhancement in Surveillance Systems", Proceedings of the 15th International Conference on Advanced Concepts for Intelligent Vision Systems (ACIVS 2013), Lecture Notes in Computer Science. Vol. 8192, pp 13-24, October 2013, ISBN: 978-3-319-02895-8

PRIVACY ENHANCEMENT METHODS FOR SURVEILLANCE SYSTEMS, AN OVERVIEW OF THE DEVELOPED ARCHITECTURES AND ALGORITHMS

Key-words: anonymization, security, steganography

The main focus of the paper concerns methods and algorithms for enhancing privacy in visual surveillance systems. Analysis of possible approaches to smart surveillance systems architectures with regards to personal data protection was made. A balance between privacy and security is searched for employing three possible solutions presented, each of them using a different hardware and software setup. The proposed system architectures accompanied by descriptions of algorithmic background and applied specific mechanisms explaining were included. Summarizing remarks pertaining implementation and research results were added.