

Kodowanie i szyfrowanie sygnałów wizyjno- fonicznych

Andrzej Ciarkowski

Plan wykładu

- ▶ Szyfrowanie multimedialnych
- ▶ Ochrona praw autorskich
- ▶ Znakowanie wodne sygnałów cyfrowych

Zastosowanie szyfrowania w transmisji i magazynowaniu danych multimedialnych

- ▶ Ochrona prywatności w zastosowaniach typu VoIP (Voice & Video over IP – telefonia Internetowa, telekonferencje)
- ▶ Ochrona praw autorskich (i innych praw majątkowych) – telewizja cyfrowa (DVB), wideo na żądanie (VOD), filmy DVD i BD
- ▶ Ochrona danych wrażliwych – dokumentacja medyczna

Podstawowe pojęcia z dziedziny kryptografii

- ▶ Kryptosystem
- ▶ Plaintext
- ▶ Ciphertext
- ▶ Cipher
- ▶ Klucz
- ▶ Atak
- ▶ Kryptoanaliza

Cechy i wymagania kryptosystemu multimediiów

- ▶ Niewielka złożoność kryptosystemu: znaczna ilość danych do przetworzenia w czasie rzeczywistym, realizacja w urządzeniach przenośnych, o niewielkiej mocy obliczeniowej i małym poborze prądu
- ▶ Niewielki wpływ szyfrowania na jakość kompresji
- ▶ Odporność na utraty danych (pakietów)

Cechy i wymagania kryptosystemu multimediiów

- ▶ Skalowalność: adaptacja do różnych przepływności
- ▶ Wielopoziomowość: kolejne poziomy różniące się rozdzielczością, jakością itp.
- ▶ „Przezroczystość”: zgodność ze starszymi standardami/rozwiązaniami
- ▶ Dostęp swobodny do strumienia: przewijanie, zmiana punktu odtwarzania nie wymaga deszyfracji całego strumienia

Szyfrowanie a kompresja

- ▶ 3 podstawowe podejścia:
 - Najpierw szyfrowanie, potem kompresja: olbrzymia złożoność (szyfrowanie wielokrotnie większego strumienia nieskompresowanego), wymagania względem kompresji – musi być bezstratna, aby potem dało się odszyfrować dane, podatność na ataki
 - Najpierw kompresja, potem szyfrowanie: rozwiązanie aktualnie stosowane w transmisji czasu rzeczywistego, ale mało praktyczne w przypadku urządzeń przenośnych; podatność na ataki typu „known-plaintext”;
 - Zintegrowana kompresja/szyfrowanie: wymagane specjalne algorytmy kompresji, niekompatybilne z aktualnymi standardami, ale potencjalnie najlepsza efektywność

Szyfrowanie a kompresja

- ▶ Podejścia niestandardowe:
 - Szyfrowanie tylko części strumienia, reszta bezużyteczna bez części podstawowej – np. tylko ramki wideo typu I, ramki predykcyjne nieszyfrowane
 - Szyfrowanie tylko określonych bitów

Szyfrowanie transmisji online

- ▶ **Protokoły RTP i SRTP**
 - Protokół RTP (Realtime Transport Protocol) jest standardowym medium wykorzystywanym w transmisji strumieni multimedialnych
 - Typowe zastosowania: telefonia Internetowa (w połączeniu z SIP, Jingle lub IAX2), telewizja (w połączeniu z RTSP), monitoring
 - Dane multimedialne są kompresowane i dzielone pakiety o określonym rozmiarze oraz opatrywane nagłówkami umożliwiającymi odtworzenie oryginalnego strumienia
 - Istnieje rozszerzenie podstawowego protokołu RTP – Secure RTP, które umożliwia zastosowanie szyfrowania i kontroli poprawności pakietów

Realizacja szyfrowania i kontroli integralności w protokole SRTP

- ▶ Każdy skompresowany pakiet RTP jest szyfrowany osobno
- ▶ Stosowany jest szyfr DES w trybie CBC (Cipher Block Chaining), co umożliwia deszyfrację każdego pakietu bez znajomości poprzedzających
- ▶ Możliwe jest zaszyfrowanie całego pakietu RTP (wraz z nagłówkami) lub tylko „ładunku” multimedialnego
- ▶ Możliwe jest również stworzenie kryptograficznego podpisu cyfrowego umożliwiającego potwierdzenie autentyczności i integralności pakietu
- ▶ Typowo stosowany jest schemat: szyfrowanie multimediiów + weryfikacja nagłówków

Szyfrowanie danych offline (plików)

- ▶ Zwykle stosowane w celu ochrony praw autorskich
- ▶ W zależności od przeznaczenia mogą być stosowane standardowe metody szyfrowania plików (bezpieczniejsze, bardziej złożone) lub optymalizowane dla multimediiów

Plan wykładu

- ▶ Szyfrowanie multimediiów
- ▶ Ochrona praw autorskich
- ▶ Znakowanie wodne sygnałów cyfrowych

Typowy system DRM (Digital Rights Management)

- ▶ Szyfrowanie materiału multimedialnego w celu uniemożliwienia dostępu bez prawidłowego klucza
- ▶ Podczas próby odtworzenia wyświetlany jest monit o dostarczenie licencji, która zawiera w sobie klucz deszyfrujący
- ▶ Różne rodzaje licencji: pojedyncze odtworzenie, pojedyncza kopia, 1 generacja kopii, ograniczenia geograficzne, ograniczenia czasowe
- ▶ Użytkownik zakupuje licencję na stronie wydawcy i dodaje ją do magazynu odtwarzacza
- ▶ Odtwarzacz weryfikuje licencję i deszyfruje strumień multimedialny

Skuteczność mechanizmów DRM

- ▶ Podatność na ataki – błędne założenia technologiczne, usterki programistyczne
- ▶ Organizacje usiłują cenzurować informacje o błędach i usterekach w systemach DRM za pomocą kroków prawnych

„Dziura analogowa”

- ▶ Brak kontroli na wyjściach analogowych odtwarzacza
- ▶ Nowsze rozwiązania eliminują „dziurę analogową” poprzez stosowanie tylko połączeń cyfrowych, wyposażonych w szyfrowane interfejsy (np. HDMI wraz z HDCP)
- ▶ Sygnał analogowy odtwarzany jest przy znacznie zdegradowanej jakości

Przykłady technologii DRM

Płyty DVD – system DCSS (Digital Content Scrambling System)

- ▶ Służy ochronie modelu biznesowego polegającego na wypuszczaniu nośników w różnych terminach w różnych rejonach geograficznych
- ▶ Wymuszenie licencjonowania odtwarzaczy DVD (dodatkowe \$\$\$ dla producentów płyt)
- ▶ Uniemożliwienie przewinięcia reklam itp.
- ▶ Złamany w 1998, Jon Lech Johansen ☺

Płyty Blu-ray i HD-DVD – system AACSS (Advanced Access Content System)

- ▶ Złamany w 2007 za pomocą ataku „known plaintext”, hacker muslix64 ☺

Port HDMI – system HDCP (High-bandwidth Digital Content Protection)

- ▶ Transmisja szyfrowanych multimediiów pomiędzy kompatybilnymi urządzeniami
- ▶ Specyfikacja prawnie zastrzeżona – wymagany zakup licencji
- ▶ Licencjobiorca musi zgodzić się na szereg ograniczeń, w tym możliwość unieważnienia swego klucza (i eliminację z rynku)
- ▶ Złamany w 2001 (przed praktyczną implementacją w jakimkolwiek urządzeniu) przez naukowców–kryptologów
- ▶ W 2010 upubliczniono odtworzony poprzez kryptoanalizę klucz główny HDCP, efektywnie niszcząc cały system ☺

Plan wykładu

- ▶ Szyfrowanie multimediiów
- ▶ Ochrona praw autorskich
- ▶ Znakowanie wodne sygnałów cyfrowych

Co to jest znakowanie wodne?

- ▶ Nazwa „znakowanie wodne” wywodzi się z techniki drukarskiej polegającej na umieszczeniu zwykle niezauważalnego znaku w papierze w celu poświadczenia autentyczności (np. banknotu)
- ▶ Znakowanie wodne (watermarking) – proces (nieodwracalnego) osadzania informacji w sygnale cyfrowym (zwykle fonicznym lub wizyjnym)
- ▶ Informacja pod postacią „znaku wodnego” pozostaje zakodowana w sygnale pomimo poddaniu go przekształceniom i kopiowaniu

Znakowanie widoczne (visible)

- ▶ Znak wodny pozostaje widoczny (jest wprost lokalizowany) w sygnale, w którym został osadzony
- ▶ Typowo jest to tekst lub logo, osadzone w obrazie wizyjnym w celu wyraźnego oznaczenia właściciela treści



Znakowanie niewidzialne (invisible)

- ▶ Znak wodny jest niezauważalny przez odbiorcę – wykorzystane są własności psychofizjologiczne słuchu lub wzroku
- ▶ Obecność i/lub treść znaku może zostać wykryta np. poprzez analizę statystyczną sygnału (w zależności od zastosowanej metody i intencji)



Zastosowanie znakowania wodnego

- ▶ Ochrona praw autorskich
 - Identyfikacja właściciela
 - Systemy DRM – odtwarzacz wykrywa obecność znaku wodnego i uniemożliwia odtworzenie bez pasującej licencji
- ▶ Identyfikacja źródła (fingerprinting)
 - Każdy z adresatów wiadomości otrzymuje ją z innym znakiem wodnym („odciskiem palca”) – w przypadku „wycieku” pozwala na ustalenie źródła
- ▶ Monitorowanie mediów
- ▶ Tajna komunikacja (steganografia)

Cechy systemu znakującego

- ▶ Odporność (robustness)
- ▶ Zauważalność/Przezroczystość (perceptability/transparency)
- ▶ Pojemność (capacity)
- ▶ Złożoność (complexity)
- ▶ Odwracalność (reversibility)

Odporność (robustness)

- ▶ Określa stopień odporności osadzonego znaku na modyfikacje sygnału (w tym celowe ataki zmierzające do zniszczenia znaku wodnego)
- ▶ Typowe modyfikacje:
 - Przekształcenia liniowe (filtracja)
 - Dodanie sygnału (w tym szumu)
 - Kompresja stratna
 - Konwersja A/C i C/A

Zauważalność/Przezroczystość (perceptability/transparency)

- ▶ Określa, czy proces znakowania wprowadza percypowalne zniekształcenia sygnału znakowanego
- ▶ Wyznaczane przy pomocy testów subiektywnych (odsłuchowych) i obiektywnych (np. PESQ)

Pojemność (capacity)

- ▶ Ilość informacji, którą algorytm znakujący jest w stanie zakodować w przeliczeniu na pojedynczy bit sygnału znakowanego (zwykle wyrażona w procentach)
- ▶ Inne miary: bity na ramkę, bit/kB

Złożoność (complexity)

- ▶ Koszt numeryczny związany z procesem osadzania i detekcji znaku wodnego – im niższy tym lepiej
- ▶ Również koszt związany z przeprowadzeniem skutecznego ataku na znak wodny – im wyższy tym lepiej

Odwracalność (reversibility)

- ▶ Czy znak wodny może zostać całkowicie usunięty z sygnału, tak aby uzyskać wierną kopię sygnału oryginalnego?

Podstawy i metody znakowania sygnałów fonicznych i wizyjnych

- ▶ Własności słuchu wykorzystywane w znakowaniu
- ▶ Własności wzroku wykorzystywane w znakowaniu
- ▶ Metody ogólne
- ▶ Metody znakowania sygnałów fonicznych
- ▶ Metody znakowania sygnałów wizyjnych

Własności słuchu wykorzystywane w znakowaniu

- ▶ Pasmo częstotliwości 20–20000Hz – umieszczenie znaku wodnego poza tym pasmem jest mało praktyczne
- ▶ Dynamika 120dB – trudno umieścić znak wodny który byłby wprost niesłyszalny
- ▶ Przebieg krzywych progowych głośności zależy od częstotliwości
- ▶ Niska wrażliwość na zmiany fazy
- ▶ Występowanie maskowania w dziedzinie czasu i częstotliwości
- ▶ Model psychoakustyczny wskazuje na 5–10 krotną nadmiarowość pełnopasmowego sygnału akustycznego – dużo miejsca na ukrywanie znaku wodnego
- ▶ Zastosowanie kodowania stratnego zmniejsza nadmiarowość i utrudnia wprowadzenie znaku wodnego

Własności wzroku wykorzystywane w znakowaniu

- ▶ Bezwładność wzroku – 0,1 s; możliwość ukrywania informacji „podprogowej” w obrazie ruchomym
- ▶ Dynamika 50dB

Kodowanie LSB

- ▶ Ukrywanie informacji w najmniej znaczących bitach próbek
- ▶ Większa skuteczność dla obrazu ze względu na mniejszą dynamikę narządu wzroku
- ▶ Metoda nieodporna na ataki, kompresję, filtrację itp.
- ▶ Znak wodny jest możliwy do wykrycia w zasadzie tylko w przypadku wykonania kopii cyfrowej 1:1
- ▶ Dodanie znaku wodnego powoduje pojawienie się szumu znakowania

Kodowanie LSB (superpozycja)

Original Images



Bits Used: 1



Bits Used: 4



Bits Used: 7



Kodowanie fazowe

- ▶ Kodowanie informacji w dziedzinie widma, poprzez modyfikację widma fazowego sygnału
- ▶ Aby znak wodny pozostał niezauważony i nie spowodować znacznych zniekształceń konieczne jest zachowanie ciągłości fazy
- ▶ Odczyt znaku wodnego wymaga znajomości długości bloku i precyzyjnego określenia punktu początkowego
- ▶ Istnieją modyfikacje tej metody wykorzystujące modulację fazy w podpasmach sygnału
- ▶ Metoda jest nieco bardziej odporna na ataki od LSB

Rozpraszanie widma (spread-spectrum)

- ▶ Kodowanie w dziedzinie widma
- ▶ Technika polega na modyfikacji widma amplitudowego poprzez wstawienie do sygnału wąskopasmowego fragmentów o szerszym paśmie (zwykle o charakterze szumowym)
- ▶ Metoda odporna na zakłócenia i ataki
- ▶ W przypadku sygnałów fonicznych znak jest łatwo zauważalny ze względu na dużą dynamikę słuchu

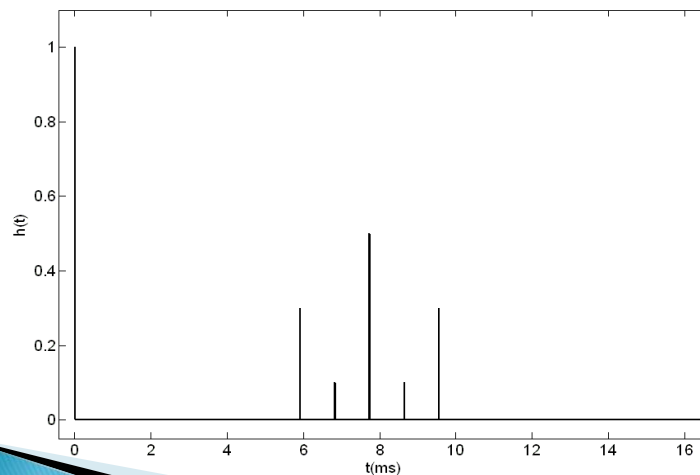
Kodowanie falkowe

- ▶ Kodowanie polega na dekompozycji falkowej sygnału i przeskalowaniu odpowiednich współczynników „pseudowidma” falkowego
- ▶ Wykrycie znaku wodnego zwykle wymaga posiadania oryginalnego sygnału
- ▶ Metoda dość odporna na ataki

Ukrywanie echa

- ▶ Metoda znakowania sygnału fonicznego wykorzystująca zjawisko pre- i post-maskowania (w dziedzinie czasu)
- ▶ Znakowanie polega na wstawieniu echa o opóźnieniu mniejszym niż próg percepcji
- ▶ Detekcja znaku polega na wyznaczeniu funkcji autokorelacji lub cepstrum sygnału
- ▶ Metoda odporna na przekształcenia liniowe oraz konwersję A/C i C/A
- ▶ Brak odporności na kompresję stratną opartą o model psychoakustyczny

Ukrywanie echa



Rozdzielanie kolorów

- ▶ Metoda bazująca na kodowaniu LSB, ale w stosunku do poszczególnych składowych koloru
- ▶ Znak wodny jest trudniejszy do wykrycia niż w podstawowej metodzie LSB