Znakowanie wodne sygnałów fonicznych i wizyjnych

Wykład: Systemy i Terminale Multimedialne, sem. 6

mgr inż. A. Ciarkowski

Plan wykładu

- Co to jest znakowanie wodne?
- Zastosowanie znakowania wodnego
- Cechy i klasyfikacja systemów znakowania sygnałów cyfrowych
- Podstawy i metody znakowania sygnałów fonicznych i wizyjnych
- Metoda eliminacji echa akustycznego z wykorzystaniem znakowania cyfrowego

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)

Steganografia

- Tajna komunikacja z zastosowaniem techniki znakowania wodnego
- Oryginalny sygnał stanowi medium dla niewidzialnego znaku wodnego
- W założeniu tylko „wtajemniczony” (dysponujący kluczem) odbiorca jest w stanie odczytać zakodowaną informację

Znakowanie a metadane

- Znak wodny może pełnić podobną rolę co metadane – przenosić dodatkowe informacje opisujące treść itp.
- W przeciwieństwie do metadanych jest on zapisany bezpośrednio w sygnale, a nie „załączony” do niego

Zastosowanie znakowania wodnego

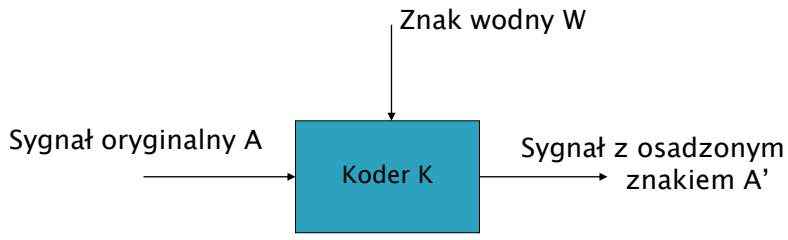
- Ochrona praw autorskich
  - Identyfikacja właściciela
  - Systemy DRM – odtwarzacz wykrywa obecność znaku wodnego i uniemożliwia odtworzenie bez pasującej licencji
- Identyfikacja źródła (fingerprinting)
  - Każdy z adresatów wiadomości otrzymuje ją z innym znakiem wodnym („odciskiem palca”) – w przypadku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

Cechy i klasyfikacja systemów znakowania sygnałów cyfrowych

- Zasada działania systemu znakującego
- Cechy systemu znakującego
- Klasyfikacja ze względu na odporność
- Klasyfikacja ze względu na weryfikowalność

Zasada działania systemu znakującego

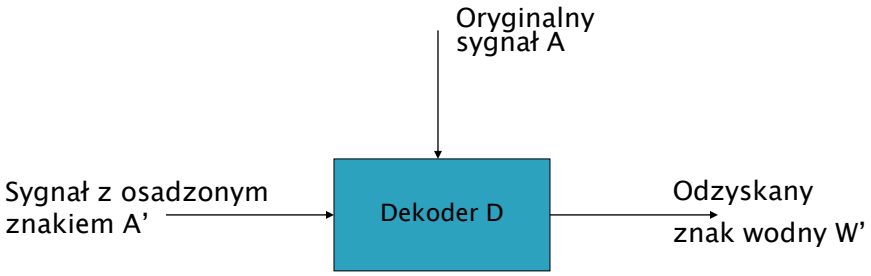
- Kodowanie



$K(A,W)=A'$

Zasada działania systemu znakującego

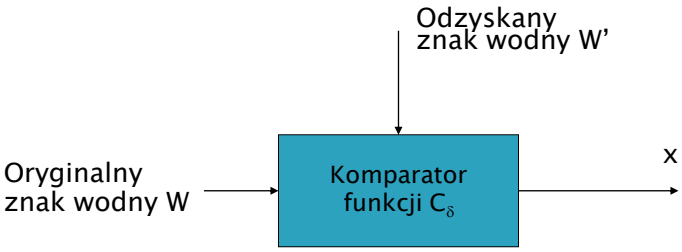
- Dekodowanie



$$D(A',A)=W'$$

Zasada działania systemu znakującego

- Rozpoznawanie znaku wodnego



$$C_\delta(W',W)=\begin{cases}1, & c\geq\delta\\ 0, & \text{w przeciwnym razie}\end{cases}$$

C – współczynnik korelacji pomiędzy W i W'

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?

Klasyfikacje mechanizmów znakowania – odporność

- Znakowanie odporne (robust)
  - wysoka odporność na ataki i zniekształcenia
- Znakowanie delikatne (fragile)
  - niewielka odporność
  - niewielka manipulacja prowadzi do zniszczenia znaku
  - zastosowanie w wykrywaniu prób manipulacji (tampering)
- Znakowanie widoczne, lokalizowalne (visible, localized)
  - niewielka odporność na ataki
  - znak może zostać łatwo zniszczony, gdyż jest jawnie lokalizowalny

Klasyfikacja mechanizmów znakowania – weryfikowalność

- Klasyfikacja uwzględniająca, jakie informacje są niezbędne do odczytania osadzonego w sygnale znaku
  - Prywatne (private, nonblind)
  - Półprywatne (semiprivate, semiblind)
  - Publiczne (public, blind, oblivious)

Prywatne (private, nonblind)

- Tzw. znakowanie z użyciem pewnych informacji
- Weryfikacja obecności znaku wodnego wymaga posiadania oryginalnego sygnału

Półprywatne (semiprivate, semiblind)

- Tzw. znakowanie z użyciem szczątkowych informacji
- Detekcja znaku nie wymaga znajomości oryginalnego sygnału
- Potrzebny jest jedynie sygnał ze znakiem
- Wykorzystywane głównie w zabezpieczeniach przed kopiowaniem, np. DVD-Video
- Również *fingerprinting*

Publiczne (public, blind, oblivious)

- Tzw. znakowanie „świadome”
- Nie wykorzystuje ani oryginalnych danych ani wzorca znaku wodnego
- Weryfikacja wzorca polega na odczycie odpowiednich bitów sygnału

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 zależny 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

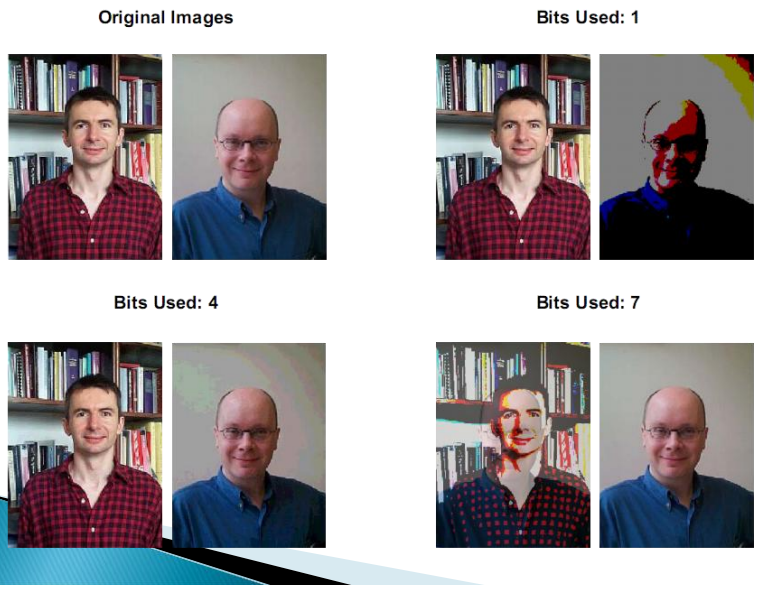
Własności wzroku wykorzystywane w znakowaniu

- Bezwładność wzroku – 0,1s; 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)



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

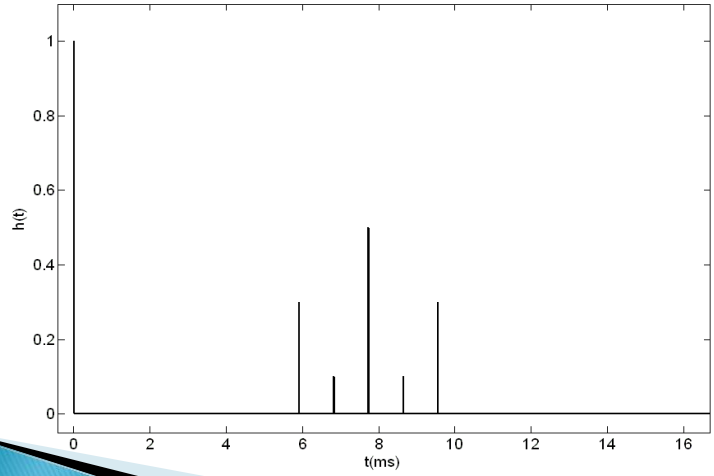
Kodowanie falkowe

- 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

Ciekawe przykłady steganografii
(niezwiązane z sygnałami cyfrowymi)

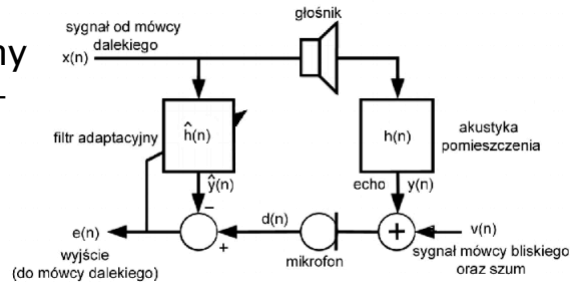
- Kodowanie białych znaków – polega na manipulacji szerokością białych znaków w tekście – stosowane w dystrybucji tajnych materiałów (pozwala zidentyfikować źródło „przecieku”)
- XML – kodowanie pojedynczego bitu poprzez zastosowanie form <tag/> i <tag></tag>
- Kodowanie informacji w sekwencjach DNA – synteza łańcuchów DNA, które mogą być np. przesłane zwykłą pocztą

Eliminacja echa akustycznego z wykorzystaniem znakowania

- Echo akustyczne jest istotnym problemem w systemach komunikacji głosowej (a zwłaszcza w VoIP ze względu na znaczne opóźnienia)
- Do zwalczania echa akustycznego wykorzystuje się systemy eliminacji echa akustycznego (AEC), składające się z:
  - Detektora mowy równoczesnej
  - Filtru adaptacyjnego
  - Procesora nieliniowego

Eliminacja echa akustycznego

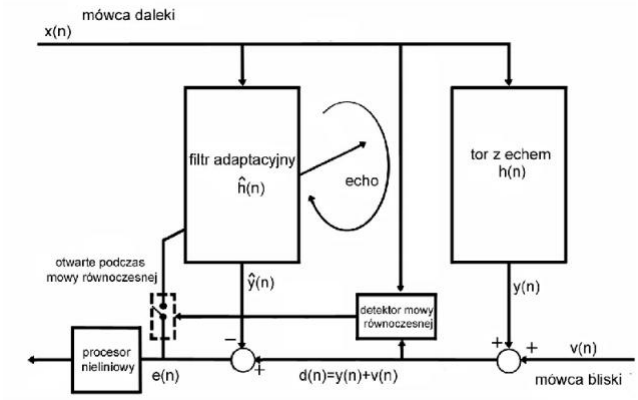
- Filtr adaptacyjny dokonuje estymaty charakterystyki „toru echa” h(n)
- Sygnał od mówcy dalekiego x(n) poddany filtracji jest odejmowany od sygnału zarejestrowanego
- Wynikiem jest sygnał e(n) wolny od echa akusty-cznego



Detekcja mowy równoczesnej

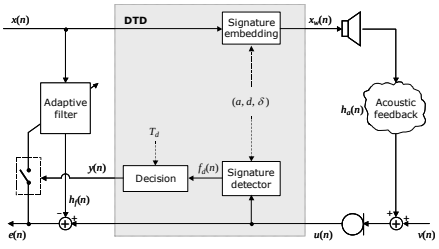
- W sytuacji gdy obecny jest sygnał od mówcy lokalnego należy zatrzymać proces adaptacji filtra, aby zapobiec jego rozstrojeniu
- W tym celu wykorzystuje się układ DTD – detektor mowy równoczesnej
- Typowe układy DTD bazują na metodach:
  - porównywania energii sygnałów – niska skuteczność, niewielka złożoność
  - obliczanie korelacji skrośnej – wysoka skuteczność, bardzo wysoka złożoność

Detekcja mowy równoczesnej



Zastosowanie znakowania sygnałów akustycznych do detekcji mowy równoczesnej

- „Zakłócenie” sygnału mówcy odległego poprzez dodanie do niego sygnału mówcy lokalnego (wystąpienie mowy równoczesnej) uniemożliwia wykrycie sygnatury znakującej w sygnale odbieranym



Wybór metody znakowania

- Niezbędne jest zastosowanie znakowania odpornego na konwersję A/C i C/A oraz charakteryzującego się dużym stopniem „przezroczystości” (*transparency*)
- Zastosowano metodę „ukrywania echa” (*echo hiding*) – dodanie do sygnału nadawanego krótkiego (kilka ms) echa, które dla słuchacza odczuwalne jest jako lekka zmiana barwy dźwięku
- Detekcja sygnatury wykorzystuje cepstrum mocy sygnału odbieranego