

Podstawy kryptografii

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2024/2025

inf.ug.edu.pl/~amb/

Steganografia i znaki wodne

Definicje

- Dzieło
 - fotografia, film, utwór muzyczny, kod programu, obwód scalony, kod html, ...
 - ma swój zapis w postaci pliku w komputerze (??)
- Treść (content)
 - to co jest przekazywane drogą elektroniczną i inną
 - wszystkie możliwe dzieła, istniejące i potencjalne
- Nośnik
 - sposób zapisu i przenoszenia dzieł
 - płyty CD/DVD, transmisja telewizyjna/internetowa, ...
 - w wersji klasycznej druk i fotografia

Steganografia a znaki wodne

- Znakowanie (watermarking)
 - dodanie do dzieła dodatkowej treści
 - związanej z samym dziełem (autor, właściciel, prawa odtwarzania, znacznik śledzenia użycia)
 - nie przeszkadzającej w odbiorze, przynajmniej nie przeszkadzającej w stopniu znacznym
 - niełatwej do usunięcia
- Steganografia
 - dodanie do dzieła dodatkowej treści
 - niezwiązanej z dziełem
 - niezauważalnej, w szczególności gdy nie jest aktywnie szukana
 - być może tajnej

Dwie operacje

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Steganografia
i znaki
wodne

Steganografia
Znaki wodne
Przykłady
implementacji

- Zanurzanie: $E(c, m)$ *embedding, cover work, message*
- Wykrywanie/wyodrębnianie: $D(w)$ *detecting/extracting, watermarked work*
 - $D(E(c, m)) = m$
 - być może konieczny będzie klucz tajny
 - $D(k, E(k, c, m)) = m$
 - być może są dwa klucze, publiczny p i prywatny s
 - $D(s, E(p, c, m)) = m$
 - być może konieczne będzie oryginalne dzieło
 - $D(c, E(c, m)) = m$

Zastosowania znaków wodnych

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Steganografia
i znaki
wodne

Steganografia
Znaki wodne
Przykłady
implementacji

- Identyfikacja autora/właściciela
 - informacja, że prawa kopiowania są ograniczone: ©
 - możliwe zidentyfikowanie właściciela praw
 - w przypadku muzyki/filmu/itp wersja pisana na nośniku
- Dowód autorstwa
 - <http://www.copyright.gov/docs/fees.html>
 - znak wodny w dziele
 - zabezpieczony hasłem (= trudniejszy do usunięcia)
 - czy można fałszywie dowodzić, że jest umieszczony w dziele?
- Identyfikacja kolejnego właściciela
 - by odkryć kto nielegalnie kopiuje
 - by uniemożliwić autorowi nadmierne kopiowanie

Zastosowania znaków wodnych c.d.

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Steganografia
i znaki
wodne

Steganografia
Znaki wodne
Przykłady
implementacji

- Uwierzytelnianie dzieła
 - podpis cyfrowy (w wersji dosłownej łatwy do stracenia)
- Monitorowanie rozpowszechniania dzieł
 - kontrola reklam
- Uniemożliwienie kopiowania
 - tzn. dzieło zmodyfikowane nie da się skopiować
 - ale sprzęt kopiujący musi respektować ograniczenia
 - wymaganie prawne
 - lub część licencji
- Wielokrotne i/lub modyfikowalne znaki wodne
 - np. znak autora, dystrybutora, numerowanej kopii dzieła
 - znak oryginalności, pierwszej kopii, nielegalnej kopii
- Zmiana standardów
 - nowe rozwiązania są traktowane jako znak wodny

Własności systemów znaków wodnych

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Steganografia
i znaki
wodne

Steganografia
Znaki wodne
Przykłady
implementacji

- Efektywność
 - wykrywalność znaku wodnego (założenie: brak zakłóceń)
- Wierność
 - odczucie odbiorcy, że dzieło jest oryginalne
 - również jeśli ma dostęp do oryginału
- Nośność
 - wielkość bezwzględna lub względna znaku wodnego
- Wykrywanie ślepe (publiczne) vs. z oryginałem (prywatne)
- Czułość/ odporność
 - prawdopodobieństwo, że znak wodny zostanie wykryty
 - również po pewnych zaburzeniach
- Specyficzność
 - prawdopodobieństwo, że znak nie zostanie wykryty tam gdzie go nie ma

Bezpieczeństwo steganografii

Podstawy kryptografii

Andrzej Borzyszkowski

Steganografia i znaki wodne

Steganografia
Znaki wodne
Przykłady implementacji

- Możliwe ataki
 - atak wyłącznie z dziełem ze znakiem wodnym
 - atak z oryginalnym nośnikiem
 - atak z zanurzoną wiadomością, celem jest odkrycie algorytmu zanurzania dla celów przyszłej analizy
 - atak z wybraną wiadomością, atakujący ma prawo żądać zanurzenia wybranej wiadomości i ma zamiar odkryć algorytm zanurzania (być może z tajnym kluczem)
- Atak na pojedyncze dzieło
 - próba usunięcia
 - znika ślad, że był znak wodny
 - nie znika, ale znak jest nieczytelny
 - próba nieuprawnionego wstawienia (fałszerstwo)
 - próba nieuprawnionego odczytania

Przykłady implementacji – grafika

Podstawy kryptografii

Andrzej Borzyszkowski

Steganografia i znaki wodne

Steganografia
Znaki wodne
Przykłady implementacji

- najmniej znaczący bit (LSB): każdy piksel jest reprezentowany przez 3 bajty dla każdego z kolorów – każdy bajt jest natężeniem jednego z kolorów – niewielka zmiana natężenia nie będzie odczuwalna dla odbiorcy
- tzw. dyskretna transformata kosinusowa



przykłady przekształceń obrazu "Lena" różnymi metodami

źródło: *Data hiding based on extended turtle shell matrix construction method* Springer Nature

Przykłady implementacji– html

Podstawy kryptografii

Andrzej Borzyszkowski

Steganografia i znaki wodne

Steganografia
Znaki wodne
Przykłady implementacji

- spacje
 - spacje na końcu wiersza nie grają roli – dodatkowe spacje
 - liczba spacji nie gra roli – spacje pojedyncze i podwójne na oznaczenie bitów
 - spacje i tabulacje są traktowane identycznie
- tagi
 - nieznane tagi w html są opuszczane podczas renderowania
 - fałszywe literówki w nazwach atrybutów
 - tagi z kilkoma atrybutami pozwalają na dowolność w kolejności tych atrybutów
 - wielkość liter w nazwach tagów nie gra roli, można stosować dowolną wielkość
 - spacje wewnątrz tagów nie grają roli
- otwarcie i natychmiastowe zamknięcie środowiska

Przykłady implementacji – tekst zwykły

Podstawy kryptografii

Andrzej Borzyszkowski

Steganografia i znaki wodne

Steganografia
Znaki wodne
Przykłady implementacji

- spacje na końcu linii są niewidoczne
 - celowe literówki mogą służyć jako dowód autorstwa tekstu
 - słownik synonimów
 - gramatyki generujące tekst, tekst ma pozorny sens a decyzje podejmowane w generowaniu konkretnych zwrotów ukrywają informację (<https://www.spammimic.com/>)
- Dear Decision maker , This letter was specially selected to be sent to you . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1625 ; Title 5 , Section 305 ! THIS IS NOT A GET RICH SCHEME ! Why work for somebody else when you can become rich as few as 87 weeks ! Have you ever noticed most everyone has a cellphone & more people than ever are surfing the web ! Well, now is your chance to capitalize on this ! WE will help YOU sell more and decrease perceived waiting time by 180% . You can begin at absolutely no cost to you ! But don't believe us . Mrs Jones of Idaho tried us and says "My only problem now is where to park all my cars" . This offer is 100% legal ! etc. ukrywa tekst „kryptografia”