Podstawy steganografii i stegoanalizy

Dominik Lau, Sebastian Kutny, Tomasz Lewandowski, Maciej Krzyżanowski

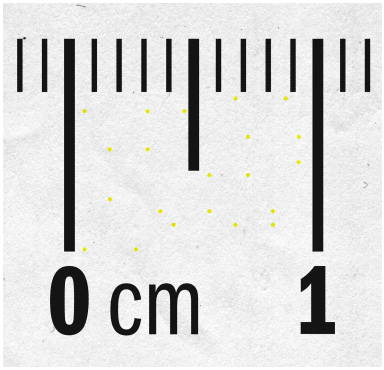
26 kwietnia 2023

1 Czym jest steganografia? Do czego służy?

Steganografia polega na ukrywaniu informacji przez ukrywanie komunikacji w innej formie transmisji danych np. w obrazkach, plikach dźwiękowych, tekstowych. Zastosowania steganografii

- omijanie cenzury/szpiegostwo
- umieszczanie znaków wodnych
- ukryta wymiana danych
- dodawanie metadanych do plików (np. znaki sterujące)
- numery seryjne drukarek (za pomocą małych kropek)
- wprowadzanie opóźnień w pakietach sieciowych
- zastosowania w VoIP (steganofonia)
- zabezpieczanie banknotów (np. EURion constellation)

Steganografia może zatem realizować następujące funkcje bezpieczeństwa



Rysunek 1: "kropki"zamieszczane przez drukarki

- poufność
- autentyczność
- niezaprzeczalność
- integralność

Porównanie kryptografii i steganografii

	kryptografia	steganografia
cel	zapewnienie poufności	ukrycie komunikacji
obecność klucza	tak	opcjonalna
widoczność danych	nie	tak
modyfikacja struktury przetwarzanych danych	nie	tak

2 Podział steganografii

Ze względu na sposób ukrywania danych

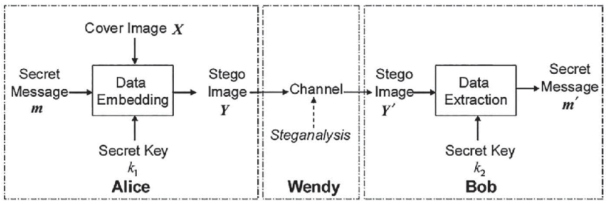
- steganografia czysta - nie jest stosowany żaden klucz, tekst jawny ukrywamy w pliku, jest to metoda Security through obscurity (nie spełnia zasady Kerckhoffsa)
- steganografia z kluczem tajnym (symetrycznym) - przed komunikacją ustalany jest (np. algorytmem DH) klucz steganograficzny wykorzystywany potem w algorytmie, następnie ukrywamy tekst jawny w pliku
- steganografia z kluczem publicznym - w pliku ukrywamy szyfrogram zaszyfrowany kluczem publicznym odbiorcy

Ze względu na kontener

- w plikach tekstowych
- w plikach audio
- w obrazach
- w ramkach różnych protokołów
- w plikach wykonawczych
- inne...

Ze względu na metodę modyfikacji nośnika

- **metody substytucji** - zamiana nadmiarowych danych nośnika
- **metody transformacyjne** - modyfikacja postaci falowej nośnika



Rysunek 2: model steganografii

- metody statystyczne - modyfikacja właściwości statystycznych nośnika
- metody generacji nośnika - ukrywanie informacji podczas tworzenia samego nośnika
- metody rozproszonego widma - ukrycie poprzez rozpraszanie danych
- metody zniekształceniowe - wprowadzenie zniekształceń do nośnika i pozyskanie informacji poprzez porównanie nośnika oryginalnego i zniekształconego

3 Steganoanaliza

4 Słowniczek

- stegosystem - połączenie metod i narzędzi służących do tworzenia ukrytego kanału do przekazywania informacji
- wiadomość (payload) - przesyłane dane
- kontener/nośnik (carrier) - to wszelkie dane służące do ukrycia tajnej wiadomości
- stegokontener - dane i ukryta w nich tajna wiadomość
- kanał steganograficzny (stegochannel) - kanał transmisji stegokontenera
- klucz (stegokey) - tajny klucz potrzebny do ukrycia stegokontenera

5 Algorytmy i zastosowania

W tej sekcji prezentujemy wybrane algorytmy steganografii oraz przykładowe zastosowania

5.1 Modyfikacja LSB

Zakodowanie
Jest to klasyczny algorytm steganografii, którego główną wadą jest łatwość w wykryciu/zniszczeniu wiadomości (np. przez wyzerowanie najmłodszych bitów). Przed niechcianym odczytem wiadomości możemy zapobiec poprzez zastosowanie kryptografii. Zasada działania algorytmu jest prosta:

1. wybierz, w którym kanale zapisać bity wiadomości (r,g,b, a, może obraz czarnobiały?)
2. zastąp stare wartości najmłodszych bitów określonego kanału obrazu kolejnymi bitami wiadomości

Analogiczna metoda jest możliwa na plikach dźwiękowych, tylko tam zmieniamy LSB próbek.

Detekcja
Prosta metoda wykrycia, czy obraz zawiera zakodowaną wiadomość

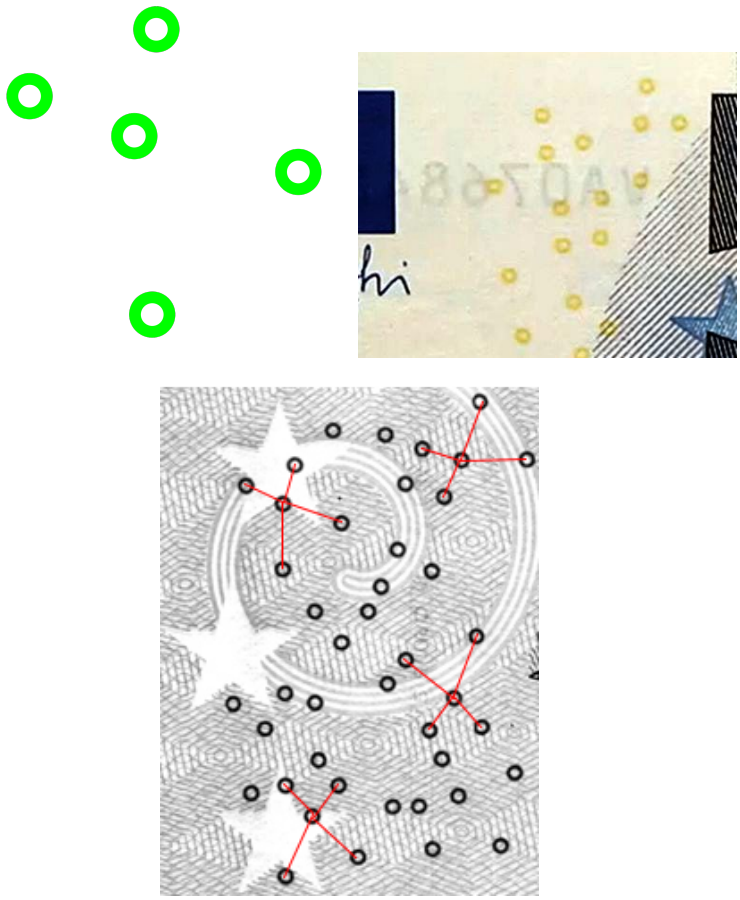
1. dzielimy piksele na bloki
2. dla każdego bloku liczymy wartość średnią LSB

Jeżeli w obrazie ukryto **zaszyfrowaną** wiadomość, to niektóre regiony bloków powinny mieć średnią ≈ 0.5 (ze względu na losowy charakter szyfrów). Możliwe są oczywiście false positives, gdy piksele w niezmodyfikowanym obrazie mają taką charakterystykę.

5.2 Gamma trick*

5.3 Ukrywanie obrazów w spektrogramach

5.4 Eurion



Rysunek 3: EURion, przykładowy układ na banknocie euro, dollarze

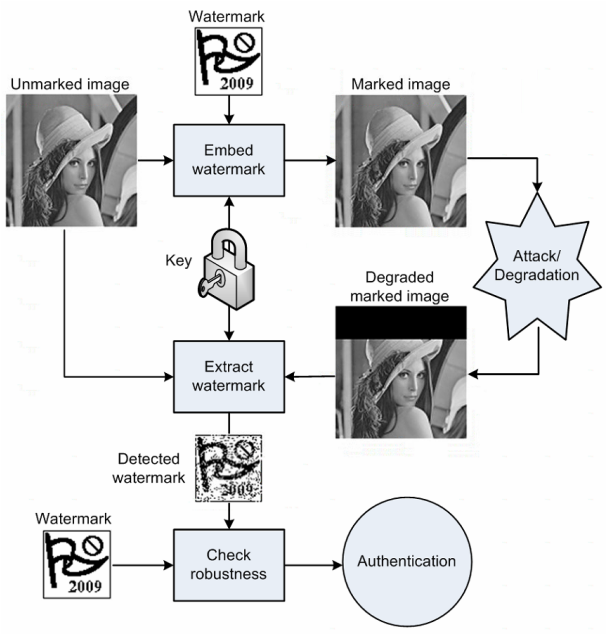
EURion jak i inne podobne zabiegi stanowią metodę przeciwdziałania fałszerstwom. Na banknotach umieszczane są zbiory kropek o różnych średnicach i względnych pozycjach (te parametry są sekretem). Kropki te tworzą fingerprint, który jest wykrywany przez oprogramowanie do skanowania (za pomocą metod detekcji wzorca) i wszelkie próby kopiowania banknotów są blokowane.

5.5 Znaki wodne

Umieszczanie znaków wodnych w plikach ma na celu zamieszczenie informacji o właścicielu praw autorskich. Wykorzystujemy różnych metod steganografii w celu zapewnienia:

- trudności w usunięciu
- odporności na transformacje (**robustness**)
- niedostrzegalności (**perceptibility**)
- przepustowość

z czego najważniejszą cechą jest odporność na transformacje



Rysunek 4: schemat zamieszczania znaku wodnego

Rysunek 5: CAP(Coded Anti Piracy) - przykład znaku wodnego zamieszczanego w filmach do identyfikacji źródła nielegalnych kopii

6 Narzędzia steganograficzne i steganoanalityczne

7 Źródła

- https://pl.wikipedia.org/wiki/Steganografia_drukarkowa
- https://royalprice.ru/pl/setting/steganografiya-i-stegoanaliz-obzor-sushchestvuyushchih-programm-i-algoritmov/
- https://www.researchgate.net/figure/The-model-of-steganography-and-steganalysis_fig1_333772050
- http://datagenetics.com/blog/september12015/index.html