

# Podstawy steganografii i stegoanalizy

Dominik Lau, Sebastian Kutny, Tomasz Lewandowski, Maciej Krzyżanowski

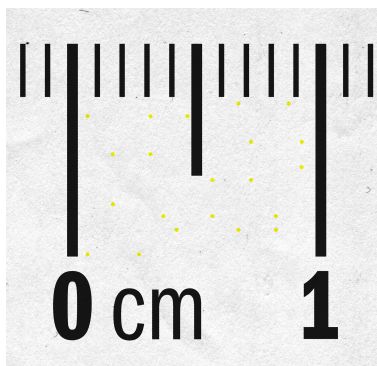
25 kwietnia 2023

## 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

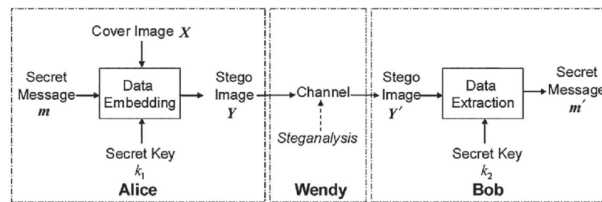
- steganografia czysta - nie jest stosowany żaden klucz, tekst jawny ukrywamy w pliku, jest to metoda Security through obscurity (nie spełnia zasady Kerckhoffs)
- steganografia z kluczem tajnym (symetrycznym) - przed komunikacją ustalany jest (np. algorytmem DH) klucz steganograficzny wykorzystywany 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 ramach różnych protokołów

## 3 Słowniczek

- stegosystem - połączenie metod i narzędzi służących do tworzenia ukrytego kanału do przekazywania informacji
- wiadomość - przesyłane dane



Rysunek 2: model steganografii

- kontener (stego-image) - 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

## 4 Historia steganografii

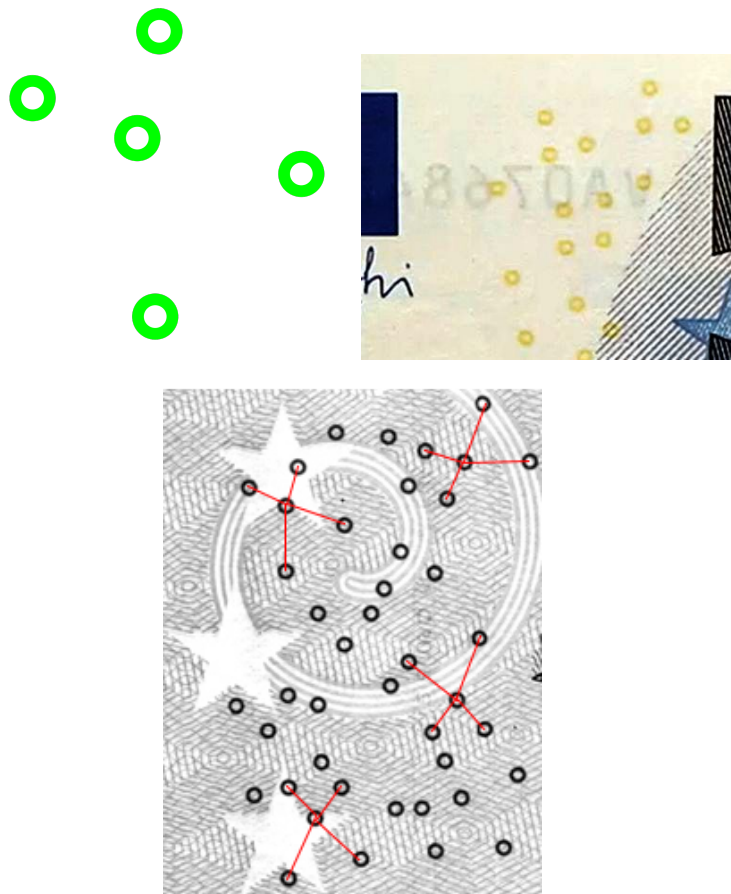
## 5 Algorytmy i przykłady steganografii w obrazach

W tej sekcji prezentujemy wybrane algorytmy steganografii na obrazach oraz przykładowe zastosowania

### 5.1 Modyfikacja LSB

### 5.2 Gamma trick\*

### 5.3 Eurion



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

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.

## 6 Algorytmy steganografii w plikach audio

## 7 Steganoanaliza

## 8 Źródła

- [https://pl.wikipedia.org/wiki/Steganografia\\_drukarkowa](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](https://www.researchgate.net/figure/The-model-of-steganography-and-steganalysis_fig1_333772050)
- <http://datagenetics.com/blog/september12015/index.html>