

Podstawy steganografii

Dominik Lau, Sebastian Kutny, Tomasz Lewandowski, Maciej Krzyżanowski

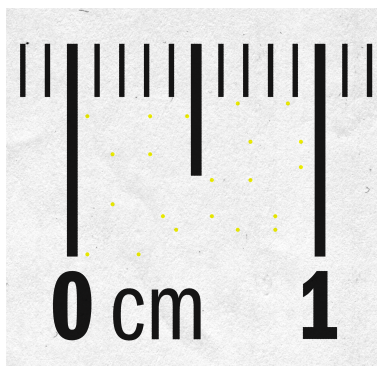
25 kwietnia 2023

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



Rysunek 2: EURion - układ kropek przypominających konstelację Oriona umieszczany na wielu banknotach

- poufność
- autentyczność
- niezaprzeczalność
- integralność

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 prywatnym - 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 medium komunikacji

- w plikach tekstowych
- w plikach audio
- w obrazach

- 3 Słowniczek
- 4 Historia steganografii
- 5 Algorytmy steganografii w obrazach
 - 5.1 Modyfikacja LSB
 - 5.2 Gamma trick*
- 6 Algorytmy steganografii w plikach audio
- 7 Steganoanaliza
- 8 Źródła

- https://pl.wikipedia.org/wiki/Steganografia_drukarkowa