

Audio steganografija: Direktno sekvencijalno širenje spektra

Mentor: prof. dr Bratislav Predić

Student: Milica Todorović, 1256

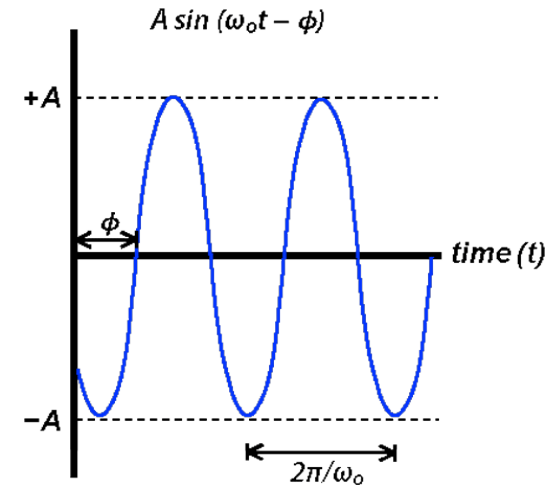
Digitalna reprezentacija zvuka

Karakteristike analognog signala (sinusni talas):

- Amplituda
- Frekvencija
- Faza

Karakteristike digitalnog signala:

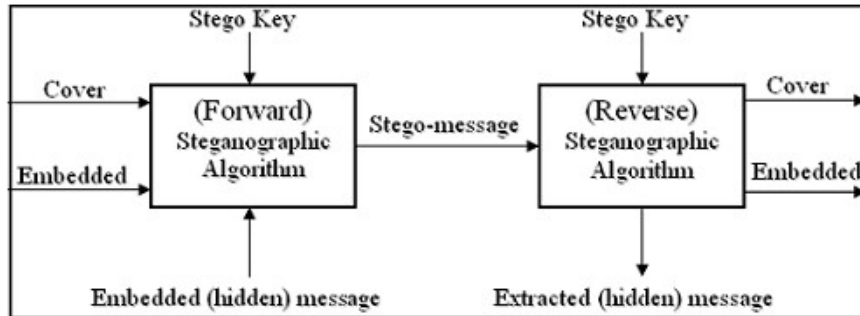
- Učestalost smplovanja (sampling rate)
- Bitska dubina/rezolucija (bit depth)



Steganografija

Umetnost skrivanja poruka u okviru drugih izvora informacija tako da ona nije vidljiva od strane neautorizovanog korisnika

Komponente steganografskog sistema:



Tipovi steganografije:

- Steganografija teksta
- Steganografija slika
- Steganografija mrežnih protokola
- Audio steganografija
- Video steganografija

Audio steganografija

Tipovi tehnika:

- Umetanje
- Zamena
- Generativne tehnike

Tehnike audio steganografije:

- Najmanje značajan bit (LSB)
- Skrivanje u ehu (Echo hiding)
- Kodiranje pomoću bita parnosti (Parity bit coding)
- Skrivanje u intervalima tišine (Silence hiding)
- Diskretna talasna transformacija (DWT)
- Kodiranje faze (Phase coding)
- Širenje spektra (Spread Spectrum)

Metrike evaluacije

- Učestalost bitske greške (BER)
- Srednja kvadratna greška (MSE):

$$MSE = \frac{1}{n} \sum_{i=0}^{n-1} (O(i) - S(i))^2$$

- Odnos maksimuma signala I šuma (PSNR):

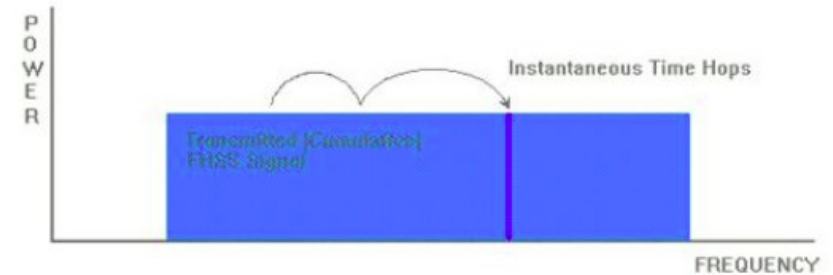
$$PSNR = 10 \log_{10} \left(\frac{\max(O)^2}{MSE} \right)$$

Tehnika širenja spektra

- Energija generisana u određenm opsezima ciljano se širi u okviru frekventnog domena, rezultujući signalom sa širim opsegom frekvencija
- Tajna komunikacija korišćena u vojne svrhe

Tehnike širenja spektra:

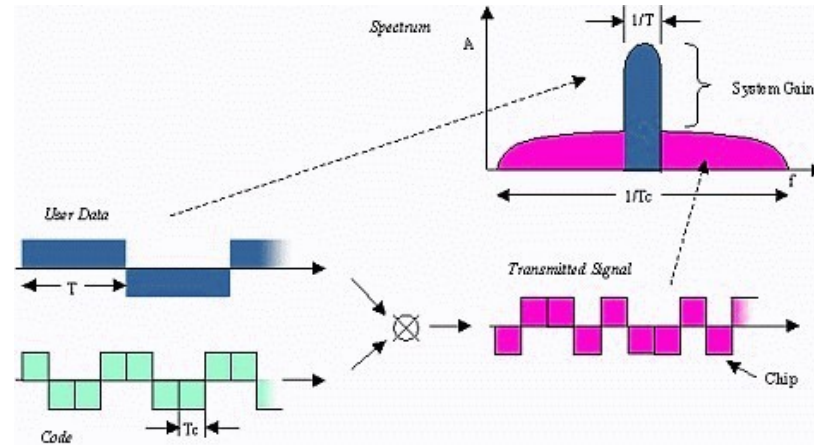
- Skokovito frekventivno širenje spektra (FHSS)
- Diskretno sekvencijalno širenje spektra (DSSS)
- Skokovito vremensko širenje spektra (THSS)



FHSS

Direktno sekvencijalno širenje spektra

- Moduliranje tajne poruke pseudo slučajnom sekvencom više frekvencije
- Umetanje generisanog šuma u originalni signal



Direktno sekvencijalno širenje spektra

- 1) Pripremiti tajnu poruku koju je potrebno raširiti
- 2) Pripremiti PN sekvencu koja će se iskoristiti za modulaciju date poruke
- 3) Izvršiti modulaciju poruke sa PN sekvencom, pri čemu frekvencija sekvence mora biti veća od frekvencije signala tajne poruke
- 4) Umetnuti modulirani signal u prenosni audio fajl
- 5) Prijemnik za dekodiranje poruke mora imati istu PN sekvencu
- 6) Modulirati dobijeni signal sa istom PN sekvencom
- 7) Rezultujući signal je tajna poruka

Direktno sekvencijalno širenje spektra

Enkodiranje:

- **A** – signal (bitstream) tajne poruke, amplituda $\{-1, 1\}$, frekvencija **n**
- **PN** – pseudo slučajna sekvenca, amplituda $\{-1, 1\}$, frekvencija **cr**
- **B** – distribuirani signal A, frekvencija **n x cr**
- **V** – prenosni audio signal, amplitude skalirane na $[-1, 1]$
- **α** – faktor jačine

$$v'_i = v_i + \alpha \cdot b_i \cdot p_i$$

Direktno sekvencijalno širenje spektra

Dekodiranje:

- Množenje stego signala istom PN sekvencom

$$\sum_{i=j \cdot cr}^{(j+1) \cdot cr - 1} p_i v'_i = \sum_{i=j \cdot cr}^{(j+1) \cdot cr - 1} p_i v_i + \sum_{i=j \cdot cr}^{(j+1) \cdot cr - 1} \alpha b_i p_i^2$$

- Prvi sabirak ~ 0 – posledica prirode PN sekvence za veliku učestalost smplovanja
- Drugi sabirak postaje $\sum_{i=j \cdot cr}^{(j+1) \cdot cr - 1} \alpha b_i$ - posledica $\{-1, 1\}$ vrednosti PN sekvence
- Ukoliko je vrednost izraza manja od 0, originalni bit – 1, u suprotnom originalni bit - 0
- α se mora pažljivo odabrati da bi αb_i bilo iznad određenog praga

Direktno sekvencijalno širenje spektra

Prednosti:

- Robustan
- Otporan na napade šumom

Nedostaci:

- Generisani pseudo slučajni šum se potencijalno može čuti u stego objektu

Hvala na pažnji!