

Steganografija

Vsebina

- Skrivanje sporočila
 - Algoritem F5
- Ekstrakcija sporočila
 - Inverzni postopek

Skrivanje sporočila

- Poljubno tekstovno sporočilo
 - Omejitev dolžine zaradi velikosti slike
- Binarizacija sporočila
 - Na začetku dodajte 4 zloge za dolžino sporočila v bitih

Skrivanje sporočila

- Razdelitev slike na bloke velikosti 8x8
- DCT ali Haar
- Cik-cak
- Kvantizacija
- Faktor stiskanja

Skrivanje sporočila – Algoritem F5

- Imamo $64 - N$ koeficientov
 - Uporabimo koeficiente na indeksih od 4 do 32
 - Če je N večji, se ta razpon zmanjša (npr. $N = 40$, uporabimo koeficiente na indeksih od 4 do 23)
- Vzamemo M naključnih trojic koeficientov AC1, AC2 in AC3
 - Zaporedni indeksi (npr. 5, 6, 7 ali 28, 29, 30 ali 15, 16, 17)
 - Brez prekrivanja (npr. 10, 11, 12 in 12, 13, 14 – to je prepovedano)
- Seme za generirane naključnih števil za izbiro trojic je $N * M$
 - Enako pri skrivanju in ekstrakciji sporočila

Skrivanje sporočila – Algoritem F5

- Pri vsakem koeficientu uporabimo najmanj pomemben bit
 - LSB (angl. least significant bit)
 - $C1 = \text{LSB}(AC1)$, $C2 = \text{LSB}(AC2)$ in $C3 = \text{LSB}(AC3)$
- Za vsako trojico ($C1$, $C2$ in $C3$) uporabimo dva bita $x1$ in $x2$ iz binariziranega sporočila

Skrivanje sporočila – Algoritem F5

- Imamo C_1 , C_2 in C_3 ter x_1 in x_2
- Uporabimo naslednje operacije za skrivanje

$x_1 = C_1 \oplus C_2$	&&	$x_2 = C_2 \oplus C_3$	– ni sprememb
$x_1 \neq C_1 \oplus C_2$	&&	$x_2 = C_2 \oplus C_3$	– NEGACIJA LSB AC_1
$x_1 = C_1 \oplus C_2$	&&	$x_2 \neq C_2 \oplus C_3$	– NEGACIJA LSB AC_3
$x_1 \neq C_1 \oplus C_2$	&&	$x_2 \neq C_2 \oplus C_3$	– NEGACIJA LSB AC_2

Skrivanje sporočila

- Uporaba RLE nad koeficienti
- Zapis v binarno datoteko

Ekstrakcija sporočila

- Preberemo binarno datoteko in izvedemo RLE, da pridobimo koeficiente
- Ekstrakcija sporočila
 - $x1 = C1 \text{ XOR } C2$
 - $x2 = C2 \text{ XOR } C3$
- Inverzni cik-cak
- DCT ali Haar
- Sestavimo sliko iz blokov 8x8
- Shranimo sliko na disk in prikažemo skrito sporočilo

Poročilo

- Prikažite graf ali tabelo
 - PSNR metrika
 - Shannonova entropija
 - Blokovnost med originalno in modificirano sliko
- Uporabite kombinacijo parametrov $N = \{1, 20, 40\}$ in $M = \{1, 3, 5\}$
- Prikažite dva histograma za intenziteto vseh slikovnih pik pred in po modifikaciji pri $N = 20$ in $M = 3$
 - Uporabite smiselno število košev

Zaključek

- Vrednost 15%
 - Skrivanje sporočila 6%
 - Ekstrakcija sporočila 6%
 - Poročilo 3%
- Ni ustnega zagovora