nedeljainformatike v9.0

Tajne sakrivene u fajlovima : Steganografija

Vuk Dolijanović

Matematička gimnazija

14. 05. 2024.

Agenda

1. Uvod
2. Metode
3. Primene

Kriptografija

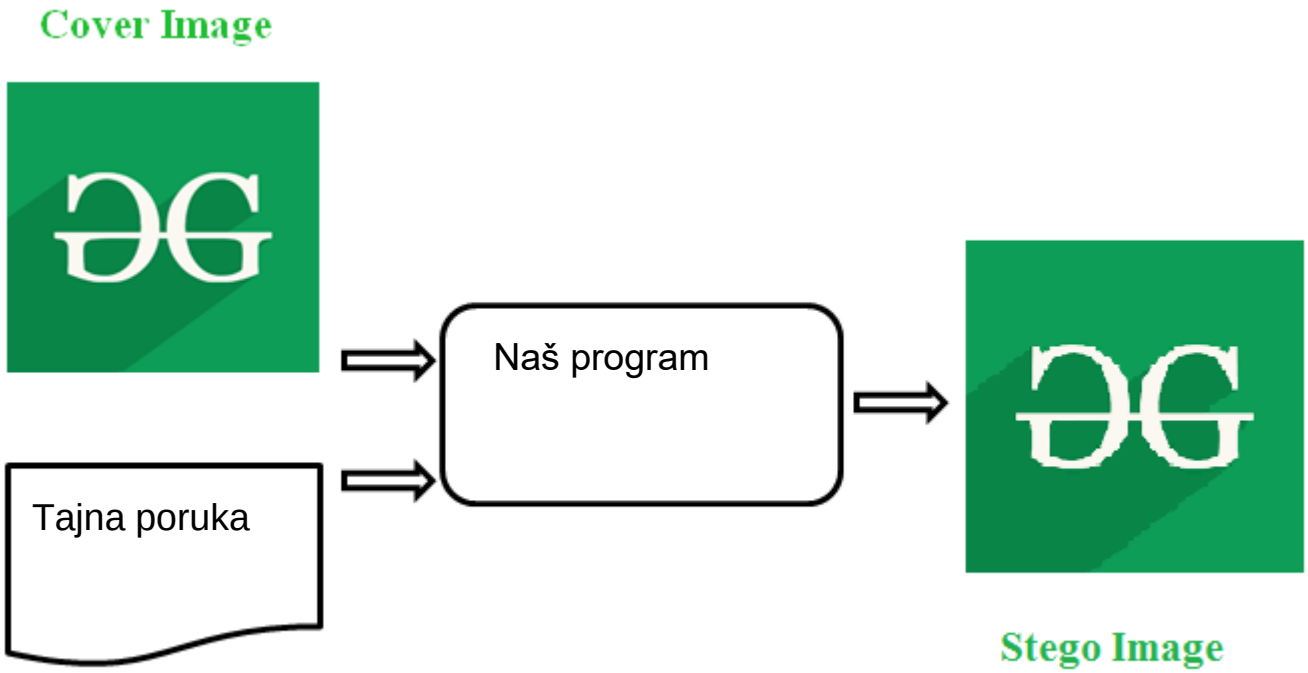
```
-----BEGIN PGP MESSAGE-----

hQIMA1OVm5qH5UWxARAAiSlIpmZVDEEgAP4J2nPZ32+F/1xI7ByZvGbC7O+DOu++
aHAExa0mtInhtpI3Q/NQq8lisSkeExodURMTA/ZHr5Q3xID+rItuev9MMT7/PeBM
QQKPH2f+TvYbJh+sjtjdahB0N8KmgHHjuZfN1My8MY+78SWT/NR5kHOF5XNFqBP2
kmFV67jxzpTPemzR8TFHZa8kOF6S7vAvlPej5msnSMMmJntTrWpbkKeJlTa3rQkp
0x35uLliOkZpHfIxTTFuhiomxIvMk5/N4QnIl6DzPddq0/mViiMMOadqJ2wYust5
CXZss4CfoslYy0qKDcUQTyW49Txd5dMuIFTR7aJmUkDjUQX1HB+v7BfAO9BcFSNC
CJhwBWUpSskdgXgyS1xzmZwcmsfBlYYQqAN5t2PrCnrSr4izgZWAiBzuSeoNJ/nS
CvclUmshvX+KuApYCPrJlfIDzWybEgAsvFRVAeqfmtxs6CfgGiTll/be/w8w7Wsz
BXALEkGYhEJknK+bGOO4wnE5KuOfSDkJ7iY6W3lyCk0AJow12ieWjWyn7sZJEOjw
uavhThXlhk6RXeFVnkxx5bLgnFZbdz4FySOz7R6B5w2PbXYjpFbpveA8LYXg8rqh
lRyomtMIPcURWQ2Y39f7xho2xXUf3ebdtgQQ7WLtl1sTM0BSHE0KFQwZU9rYhTTS
6QFoyactBhUqwfZmj0Rn5jVMzrzDR8Shy3/lc3Ii0jNSHnhjAW7825oZx1DfzFWO
RNq3hYl9uFwLqNM3O4ciwEC0VTxkskux6mS/FoeDJIb3JyFda1y4n6BrFFea3E4T
WxI2IFCq3s1n/75KtjuRKboNySsZpi0yfDKk8KrSNfGNk2lrqhF77S9vESDqRzsm
x5SMR65nPuHBVvEdiSaGeML5It/SI4f2QVBOytrJf5APgl0XitV9KEH9O5UO2lLq
hEaUu7oRtFYXPfswo5yeaQf0Sld34wvhZ2dN06s6nfe+eEAe+Ar69Q03H+P8pD/r
srsLqdrLTrMvU6IWzbMdsbhExsqKtk2wpSZwNajR04pVOjh+m4RVhoRiBC3q9T3u
+hpimjM9xokfDcq9dv1ursSlTaERSpT7v2LieCYTIyOQpnh/cxbxm+/I3JHAMom8
15jS+3gvMFt9lm6oo1RANB+EuU00TelMFtKmWi5B2N6VV7UikOhZOWfDQap6Tpz3
nmwEpN9SHPQ8aufanhwjaAc7axlUFsbSdgBsM7SNW2fY1gbDQuo1dv5XbEaGIFbR
5Tevbt2wJfzzMujbMpy6H/DEr1AKmg98ntU6PIOEJutoTZfekzf4XPoOr5tAlSIS
BxQEWwu+lYZGtgZ0R8UjtaBR8oTK3iq4pBz8kZVb4gvZwTw85sKZD1a4XchuTbf7
ehCpz+F+mMQxdqmobGCi8UVoj6EE0noZTbzzoAV+gJd0TwQRg1MkJceq7H8f6f/p
8KLkFK3S4W5HZZXgC6hkE4PkGU6ZRprsQq8B381p7okcb4BbUs5ATfk9j8mCsIUD
qLR7z51IoM6+i3wmyB+KnjYVHcoVpDaWIdcUe/mK5oZNs14vIls1E0B1ZBK2kqAm
AF60joZqc3SsJUChotEhZd2cMGfhvdE2JQLSVkF+cAbuFhyQ4J5eNd0UM9Ker0f3
I3LDaIJPf1uzIVPj7a/zGg2uPCUSi+kVBgRRIYVrbAzWGUXAFzcwJFT8rgSoWC6o
7Ec+OL9h4EiE88PTb030O0ovZCZ4NMArT7sQbS/w2XzTpS5ij4sEKKN01PpNdR5I
shzo3H1+ctIpO2XvAnFxXVtM+uQy71qpI+pNkBjV6C3E5kMMr9nMW8AoQJMTvIU+
Dr4MDo6/AN1XnMJ85eR6YVXa63U/9lXI9eCtsNGHJdEpgmC83Ico/BY3UH+Y6cu2
SsKAJjdnUN4n6Gh9rLLStjCl9X4jg76dsNEfcY0wJq/bnP7X6tpC3m3UTDfgq6+E
fh99nVKkWKZpf3P6KYjQsPdv82UXA+3Bv/e+6SMpGGGOW6UljmUo+ZG8apzVxo7y
9fM3TmRe32MlZ6uqd8YF
=6Bif
-----END PGP MESSAGE-----
```

Kriptografija

- Ne može se dekriptovati sadržaj naše poruke
- ALI neko ko nadzire kanal komunikacije može videti da je tajna poruka poslata

```
-----BEGIN PGP MESSAGE-----

hQIMA1OVm5qH5UWxARAAiSlIpmZVDEEgAP4J2nPZ32+F/1xI7ByZvGbC7O+DOu++
aHAExa0mtInhtpI3Q/NQq8lisSkeExodURMTA/ZHr5Q3xID+rItuev9MMT7/PeBM
QQKPH2f+TvYbJh+sjtjdahB0N8KmgHHjuZfN1My8MY+78SWT/NR5kHOF5XNFqBP2
kmFV67jxzpTPemzR8TFHZa8kOF6S7vAvlPej5msnSMMmJntTrWpbkKeJlTa3rQkp
0x35uLliOkZpHfIxTTFuhiomxIvMk5/N4QnIl6DzPddq0/mViiMMOadqJ2wYust5
CXZss4CfoslYy0qKDcUQTyW49Txd5dMuIFTR7aJmUkDjUQX1HB+v7BfAO9BcFSNC
CJhwBWUpSskdgXgyS1xzmZwcmsfBlYYQqAN5t2PrCnrSr4izgZWAiBzuSeoNJ/nS
CvclUmshvX+KuApYCPrJlfIDzWybEgAsvFRVAeqfmtxs6CfgGiTll/be/w8w7Wsz
BXALEkGYhEJknK+bGOO4wnE5KuOfSDkJ7iY6W3lyCk0AJow12ieWjWyn7sZJEOjw
uavhThXlhk6RXeFVnkxx5bLgnFZbdz4FySOz7R6B5w2PbXYjpFbpveA8LYXg8rqh
lRyomtMIPcURWQ2Y39f7xho2xXUf3ebdtgQQ7WLtl1sTM0BSHE0KFQwZU9rYhTTS
6QFoyactBhUqwfZmj0Rn5jVMzrzDR8Shy3/lc3Ii0jNSHnhjAW7825oZx1DfzFWO
RNq3hYl9uFwLqNM3O4ciwEC0VTxkskux6mS/FoeDJIb3JyFda1y4n6BrFFea3E4T
WxI2IFCq3s1n/75KtjuRKboNySsZpi0yfDKk8KrSNfGNk2lrqhF77S9vESDqRzsm
x5SMR65nPuHBVvEdiSaGeML5It/SI4f2QVBOytrJf5APgl0XitV9KEH9O5UO2lLq
hEaUu7oRtFYXPfswo5yeaQf0Sld34wvhZ2dN06s6nfe+eEAe+Ar69Q03H+P8pD/r
srsLqdrLTrMvU6IWzbMdsbhExsqKtk2wpSZwNajR04pVOjh+m4RVhoRiBC3q9T3u
+hpimjM9xokfDcq9dv1ursSlTaERSpT7v2LieCYTIyOQpnh/cxbxm+/I3JHAMom8
15jS+3gvMFt9lm6oo1RANB+EuU00TelMFtKmWi5B2N6VV7UikOhZOWfDQap6Tpz3
nmwEpN9SHPQ8aufanhwjaAc7axlUFsbSdgBsM7SNW2fY1gbDQuo1dv5XbEaGIFbR
5Tevbt2wJfzzMujbMpy6H/DEr1AKmg98ntU6PIOEJutoTZfekzf4XPoOr5tAlSIS
BxQEWwu+lYZGtgZ0R8UjtaBR8oTK3iq4pBz8kZVb4gvZwTw85sKZD1a4XchuTbf7
ehCpz+F+mMQxdqmobGCi8UVoj6EE0noZTbzzoAV+gJd0TwQRg1MkJceq7H8f6f/p
8KLkFK3S4W5HZZXgC6hkE4PkGU6ZRprsQq8B381p7okcb4BbUs5ATfk9j8mCsIUD
qLR7z51IoM6+i3wmyB+KnjYVHcoVpDaWIdcUe/mK5oZNs14vIls1E0B1ZBK2kqAm
AF60joZqc3SsJUChotEhZd2cMGfhvdE2JQLSVkF+cAbuFhyQ4J5eNd0UM9Ker0f3
I3LDaIJPf1uzIVPj7a/zGg2uPCUSi+kVBgRRIYVrbAzWGUXAFzcwJFT8rgSoWC6o
7Ec+OL9h4EiE88PTb030O0ovZCZ4NMArT7sQbS/w2XzTpS5ij4sEKKN01PpNdRSI
shzo3H1+ctIpO2XvAnFxXVtM+uQy71qpI+pNkBjV6C3E5kMMr9nMW8AoQJMTvIU+
Dr4MDo6/AN1XnMJ85eR6YVXa63U/9lXI9eCtsNGHJdEpgmC83Ico/BY3UH+Y6cu2
SsKAJjdnUN4n6Gh9rLLStjCl9X4jg76dsNEfcY0wJq/bnP7X6tpC3m3UTDfgq6+E
fh99nVKkWKZpf3P6KYjQsPdv82UXA+3Bv/e+6SMpGGGOW6UljmUo+ZG8apzVxo7y
9fM3TmRe32M1Z6uqd8YF
=6Bif
-----END PGP MESSAGE-----
```

Steganografija 101



Agenda

1. Uvod
2. Metode
3. Primene

LSB steganografija

Originalna slika

```
11111111 00000000
00000000 00000000
00000000 00000000

11111111 00000000
11111111 00000000
00000000 11111111
```

LSB steganografija u kojoj menjamo dva poslednja bita kako bi ugradili reč "cat" u našu sliku

Slika sa ugrađenom porukom

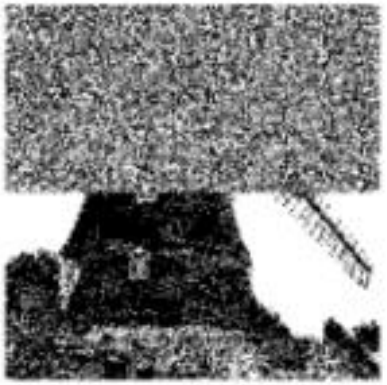
```
11111101 00000011
00000010 00000001
00000000 00000010

11111100 00000011
11111101 00000001
00000001 11111100
```

c	a	t
01 10 00 11	01 10 00 01	01 11 01 00

Steganaliza

Original

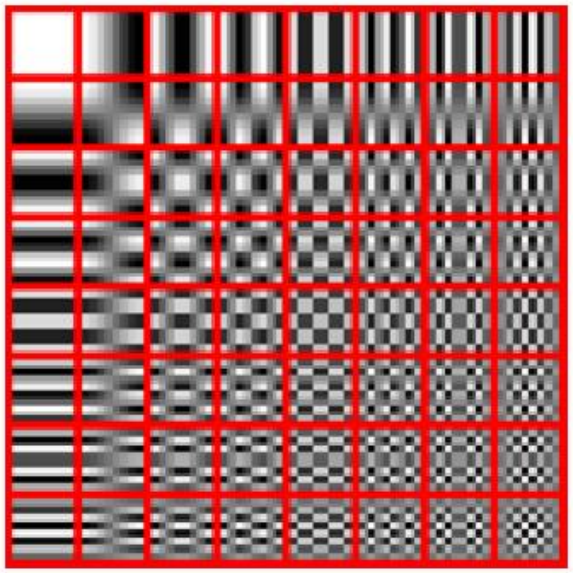
LSBs of Original



LSBs of Steganographed Version

Drugi formati slika

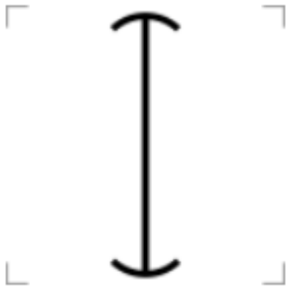
- Neki formati koriste kompresiju - na primer JPEG
- Videti predavanje sa Nedelje informatike 2022 o JPEG kompresiji
- Ne možemo koristiti LSB steganografiju
- Postoje druge metode steganografije u ovom slučaju
- Za JPEG - DCT koeficijenti



$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}.$$

Steganografija u tekstu

- Unicode standard definiše dva karaktera koji se koriste u arapskom jeziku za spajanje reči - Zero width joiner i zero width non joiner
- Njih možemo iskoristiti za ugrađivanje naše tajne poruke u tekst



(а) *ISO* симбол за *ZWJ*

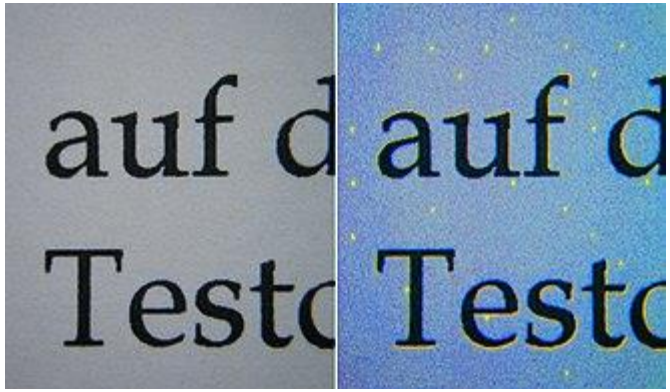
(б) *ISO* симбол за *ZWNJ*

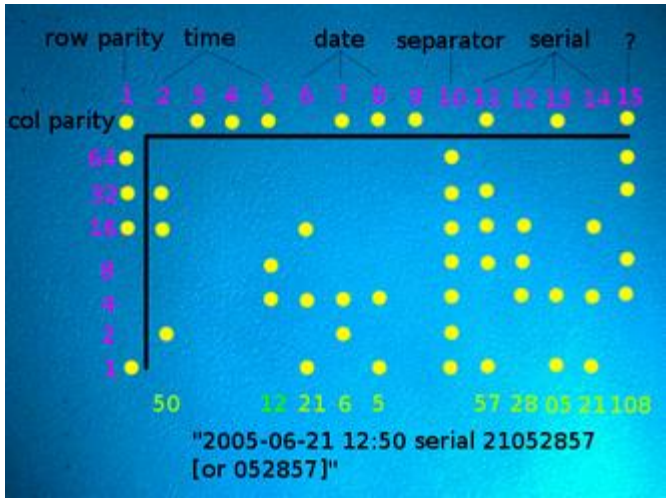
Agenda

1. Uvod
2. Metode
3. Primene

Digitalni štampači

- Štampači u svaki papir ugrađuju mikroskopske žute tačke koje služe da bi forenzički identifikovale dokument na jedinstven način
- Na ovaj način može se ukoliko dođe do potrebe identifikovati ko je odgovoran za štampanje lažnog novca, krivotvorenje dokumenata...





Watermarking i *Coded Anti Piracy*

- Watermarking predstavlja ugrađivanje poruke koja jednoznačno određuje nečije vlasništvo nad autorskim pravima digitalnog dela
- Coded Anti Piracy je tip watermarkinga pomoću kog možemo zaključiti koja osoba u lancu produkcije nekog digitalnog dela je odgovorna za širenje tog dela u širu javnost

Stegomalware

- Stegomalware predstavlja maliciozan kod ugrađen u neki fajl, koji je sakriven kako bi izbegao detekciju od strane antivirusa
- Taj maliciozni kod mora da bude aktiviran od strane nekog eksternog koda

Hvala na pažnji!

Pitanja?