STEGANOGRAPHY

COMP 597 – Computer Forensics

Steganography

- Hiding one or more data secretly in other forms of data

Basic Steganography

copy Maid.mp3 /b + d.zip /b hidMusic.mp3

Steganography

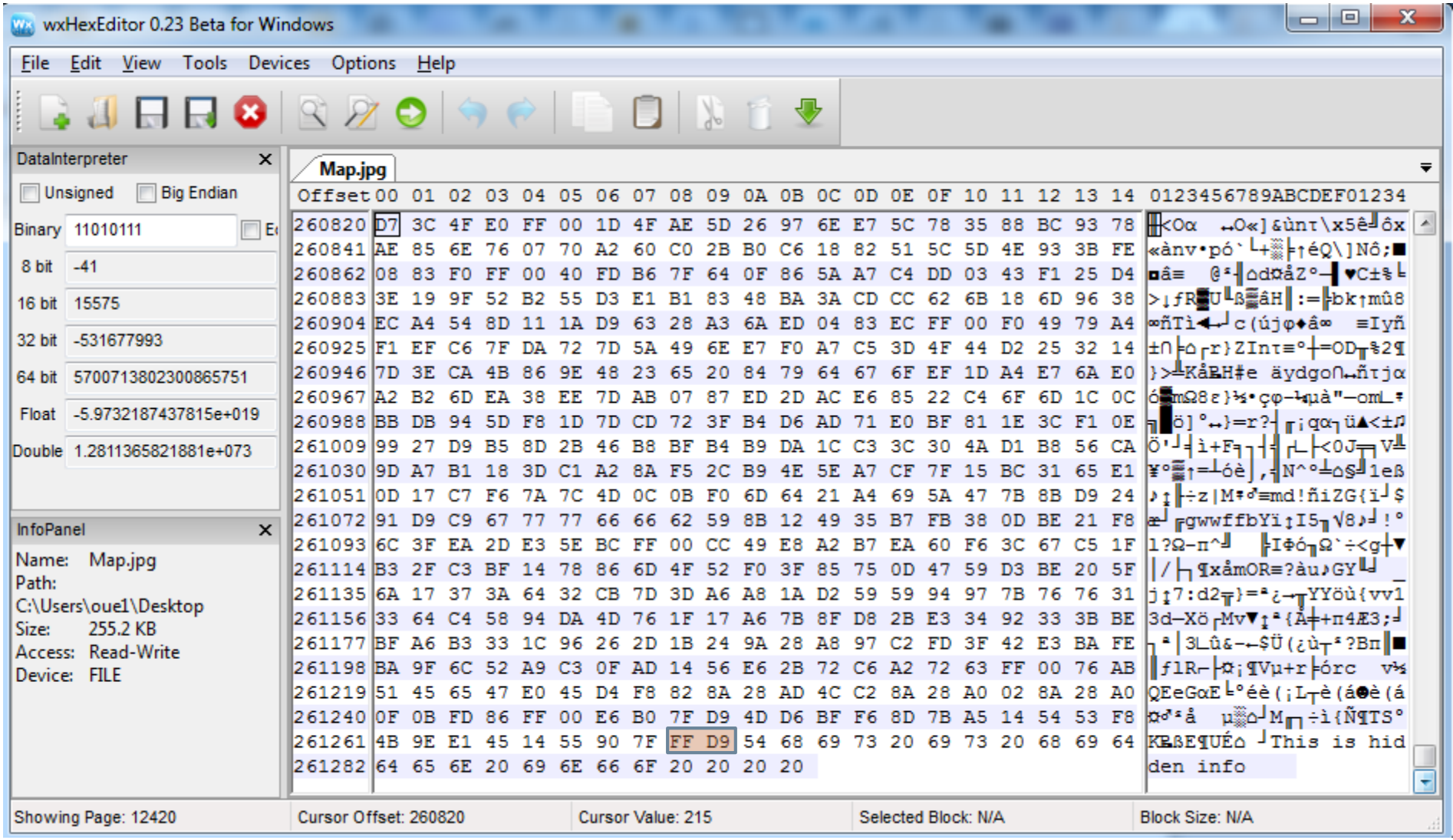
Main strategies:

- Insertion
  - Append
  - Prepend
- Substitution

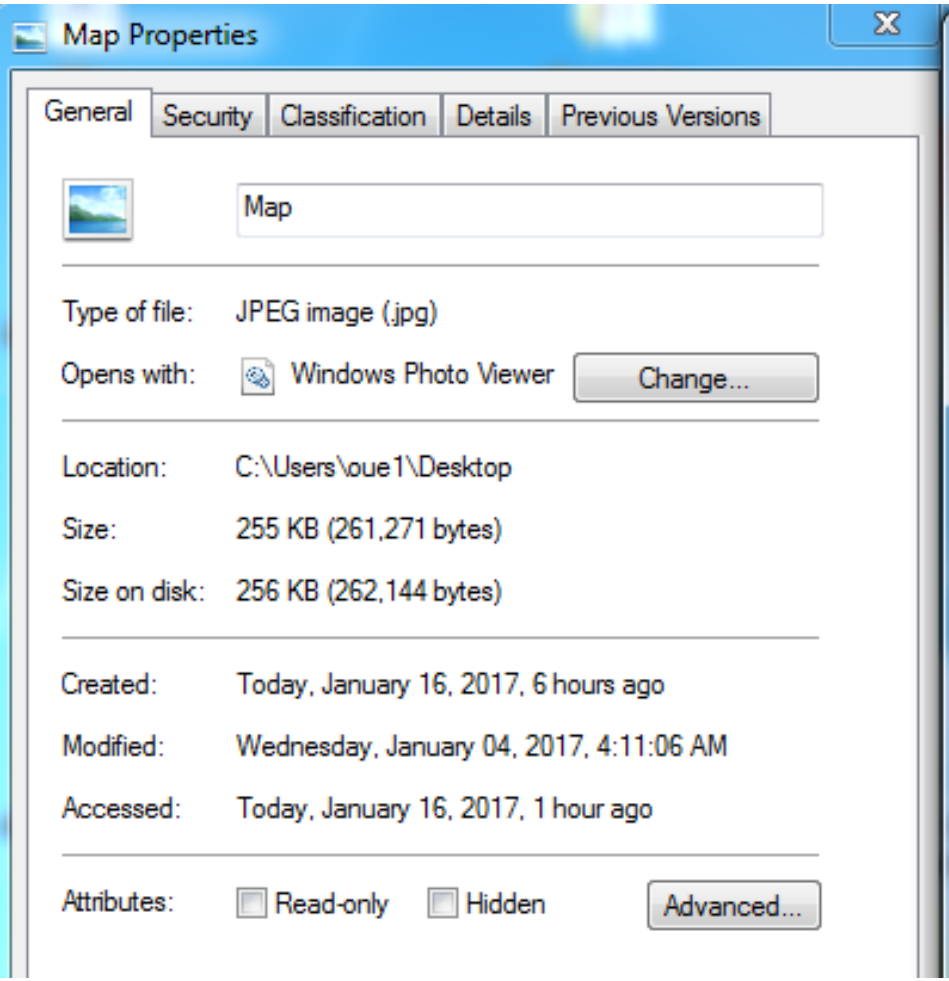
Steganography - JFIF

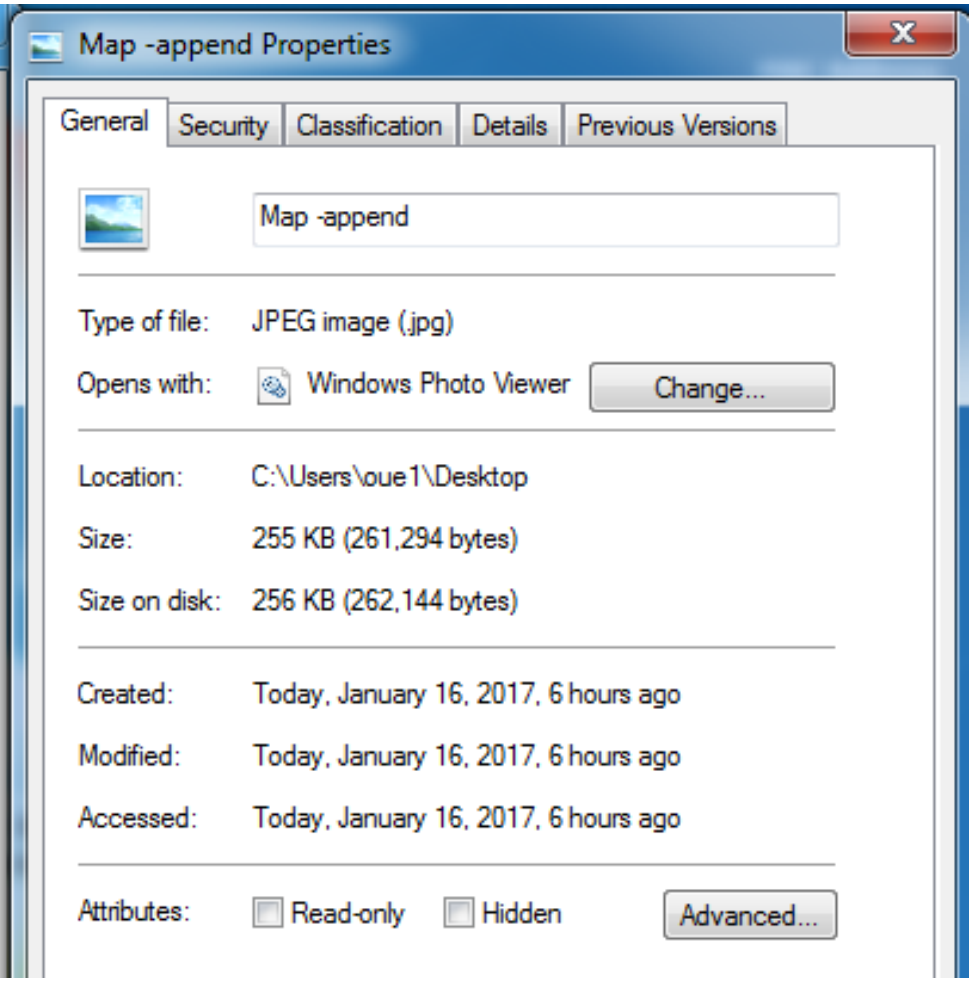
File Marker	Value
SOI	FF D8
APPO	FF E0
SOFO	FF C0
SOS	FF DA
EOI	FF D9

Steganography - Append

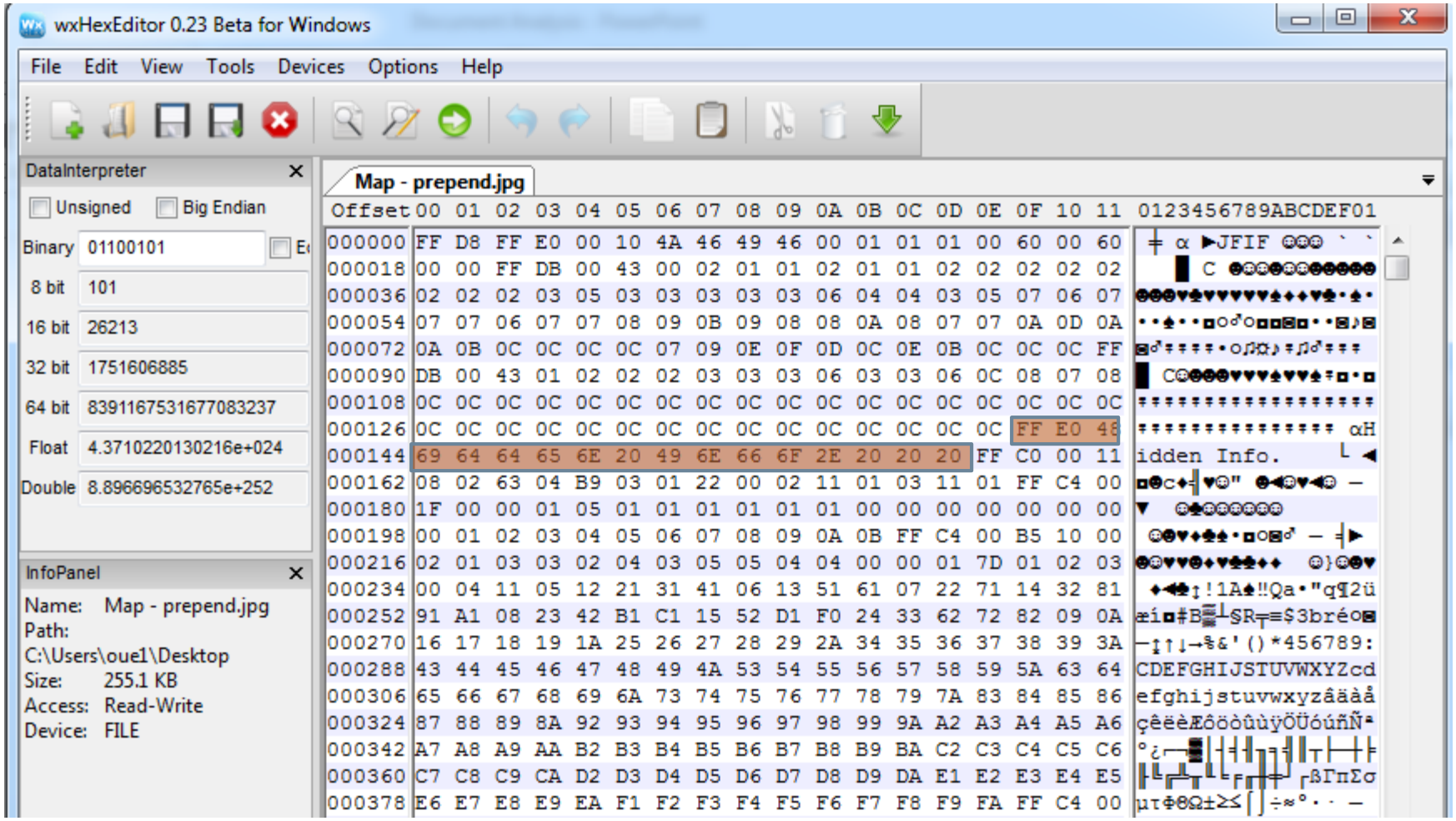


Steganography - Append





Steganography – Prepend



Least Significant Bit - RGB

00000000
00000000
00000000
11111111
00000000
00000000
00000000
11111111

Least Significant Bit

Steganography

Available tools:

- Clotho
- Our Secret
- S-Tools
- wbStego

wbStego

f3.txt | f4.txt

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	0123456789ABCDEF012345678
000000	73	65	63	72	65	74	20	6D	65	73	73	61	67	65	20	69	73	20	68	69	64	64	65	6E	20	secret message is hidden
000025	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	20	6D	65	73	73	61	67	65	20	69	73	20	here.♪◙secret message is
000050	68	69	64	64	65	6E	20	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	20	6D	65	73	73	hidden here.♪◙secret mess
000075	61	67	65	20	69	73	20	68	69	64	64	65	6E	20	68	65	72	65	2E	0D	0A	73	65	63	72	age is hidden here.♪◙secr
000100	65	74	20	6D	65	73	73	61	67	65	20	69	73	20	68	69	64	64	65	6E	20	68	65	72	65	et message is hidden here
000125	2E	0D	0A	73	65	63	72	65	74	20	6D	65	73	73	61	67	65	20	69	73	20	68	69	64	64	.♪◙secret message is hidd
000150	65	6E	20	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	20	6D	65	73	73	61	67	65	20	en here.♪◙secret message
000175	69	73	20	68	69	64	64	65	6E	20	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	20	6D	is hidden here.♪◙secret m
000200	65	73	73	61	67	65	20	69	73	20	68	69	64	64	65	6E	20	68	65	72	65	2E	0D	0A	73	essage is hidden here.♪◙s
000225	65	63	72	65	74	20	6D	65	73	73	61	67	65	20	69	73	20	68	69	64	64	65	6E	20	68	ecret message is hidden h
000250	65	72	65	2E	0D	0A	73	65	63	72	65	74	20	6D	65	73	73	61	67	65	20	69	73	20	68	ere.♪◙secret message is h

f4.txt

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	0123456789ABCDEF012345678
000000	73	65	63	72	65	74	00	6D	65	73	73	61	67	65	00	69	73	00	68	69	64	64	65	6E	20	secret message is hidden
000025	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	00	6D	65	73	73	61	67	65	20	69	73	20	here.♪◙secret message is
000050	68	69	64	64	65	6E	00	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	00	6D	65	73	73	hidden here.♪◙secret mess
000075	61	67	65	00	69	73	00	68	69	64	64	65	6E	00	68	65	72	65	2E	0D	0A	73	65	63	72	age is hidden here.♪◙secr
000100	65	74	00	6D	65	73	73	61	67	65	00	69	73	00	68	69	64	64	65	6E	00	68	65	72	65	et message is hidden here
000125	2E	0D	0A	73	65	63	72	65	74	00	6D	65	73	73	61	67	65	00	69	73	00	68	69	64	64	.♪◙secret message is hidd
000150	65	6E	00	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	00	6D	65	73	73	61	67	65	00	en here.♪◙secret message
000175	69	73	00	68	69	64	64	65	6E	00	68	65	72	65	2E	0D	0A	73	65	63	72	65	74	00	6D	is hidden here.♪◙secret m
000200	65	73	73	61	67	65	20	69	73	20	68	69	64	64	65	6E	20	68	65	72	65	2E	0D	0A	73	essage is hidden here.♪◙s
000225	65	63	72	65	74	00	6D	65	73	73	61	67	65	20	69	73	00	68	69	64	64	65	6E	00	68	ecret message is hidden h
000250	65	72	65	2E	0D	0A	73	65	63	72	65	74	00	6D	65	73	73	61	67	65	20	69	73	20	68	ere.♪◙secret message is h

S-Tools - GIF

S-Tools - GIF

Attacks on Steganography

1. File Only
2. File and Original Copy
3. Destroy Everything Attack
4. Reformat Attack

Secret Sharing

What do we do when the secret is too important?

Secret Sharing – Information Splitting

1. We split the secret into *n* parts
2. Each part on its own look like noise
3. We combine the *n* parts to recreate the secret

Secret Sharing – Information Splitting

Approach 1:

$f(k_1, f(k_2, f(k_3, \ldots f(k_n, X) \ldots)))$

Secret Sharing – Information Splitting

Approach 2:

$$X_1 + X_2 + X_3 + \cdots + X_n = X$$

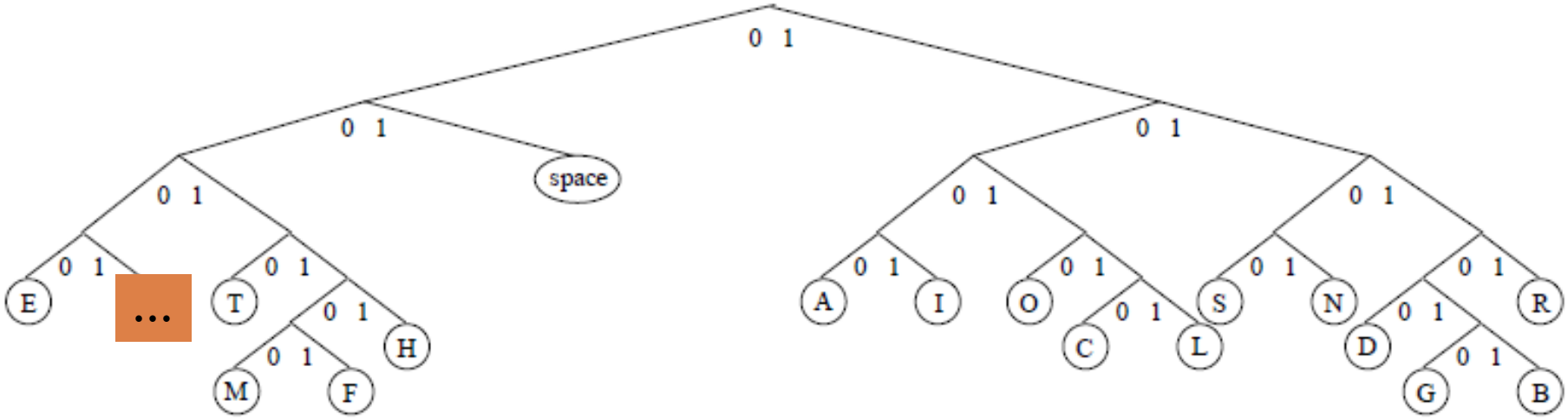
Text Steganography based on Mimicry

- source text *S*
- hidden message *H*
- Based on Huffman Coding

Huffman Coding

Letter	Frequency	Letter	Frequency
space	26974	A	6538
B	1275	C	3115
D	2823	E	9917
F	1757	G	1326
H	3279	I	6430
J	152	K	317
L	3114	M	1799
N	5626	O	6261
P	2195	Q	113
R	5173	S	5784
T	8375	U	2360
V	928	W	987
X	369	Y	1104
Z	60		

Huffman Coding



Huffman Coding

- 01110011 s
- 01100101 e
- 01100011 c
- 01110010 r
- 01100101 e
- 01110100 t

- 1100 s
- 0000 e
- 10110 c
- 1111 r
- 0000 e
- 0010 t

Mimicry n=2

Thy etheren' ante esthe ales. icone thers the ase omsictorm s iom. wactere cut le ce s mo be t Me. Y whes ine odofuion os thore cctherg om tt s d Thm & tthamben tin'ssthe, co westitit odecra fugon tucod. liny Eangem o wen il ea bionBulivethe ton othanstoct itaple

Mimicry n=25

The letter compression or video is only to generate a verbatim> followed by 12 whiter ‘H’ wouldn’t design a perfective reconomic data. This to simple hardware. These worked with encodes of the data list of the diction in the most come down in depth in a file decome down in adds about of character first.

References

- Michael T. Raggo, Chet Hosmer, Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols, 2012.
- Peter Wayner, Disappearing Cryptography, 3rd edition, 2008.