HIDDEN IN PLAIN SIGHT

Steganography &
Digital Watermarking

Steganography

Στεγανός (*steganos*): covered

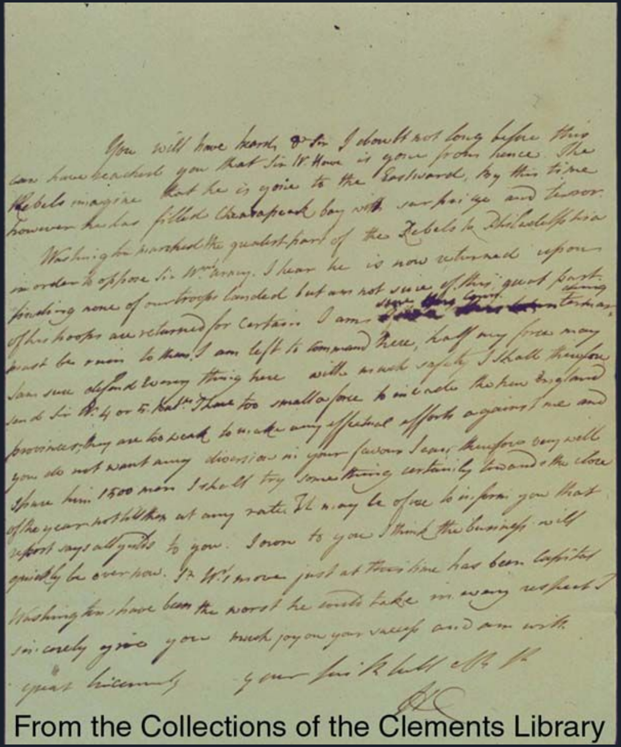
Steganography vs Cryptography

	Visible	Invisible
Insecure		
Secure		

Steganography vs Cryptography

	Visible	Invisible
Insecure	Plaintext	Noise
Secure*	Cryptography	Steganography

Mask Letter (1777)



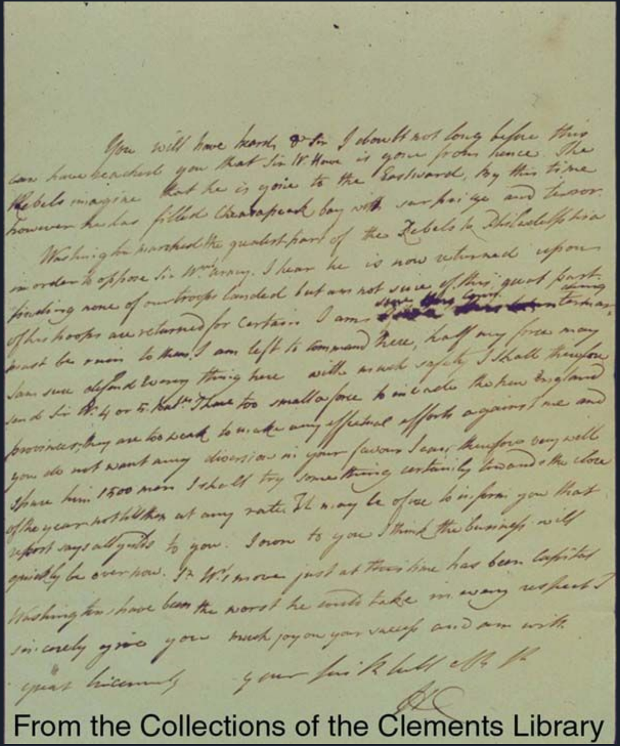
From the Collections of the Clements Library

You will have heard, Dr Sir I doubt not long before this / can have reached you that Sir W. Howe is gone from hence. The / Rebels imagine that he is gone to the Eastward. By this time / however he has filled Chesapeak bay with surprize and terror.

Washington marched the greater part of the Rebels to Philadelphia / in order to oppose Sir Wm's. army. I hear he is now returned upon / finding none of our troops landed but am not sure of this, great part / of his troops are returned for certain. I am sure this countermarching / must be ruin to them. I am left to command here, half of my force may / I am sure defend everything here with much safety. I shall therefore / send Sir W. 4 or 5 Bat [talio]ns. I have too small a force to invade the New England / provinces; they are too weak to make any effectual efforts against me and / you do not want any diversion in your favour. I can, therefore very well / spare him 1500 men. I shall try some thing certainly towards the close / of the year, not till then at any rate. It may be of use to inform you that / report says all yields to you. I own to you that I think the business will / quickly be over now. **Sr. W's move just at this time has been capital. / Washingtons have been the worst he could take in every respect.** / sincerely give you much joy on your success and am with / great Sincerity your [ ] / HC

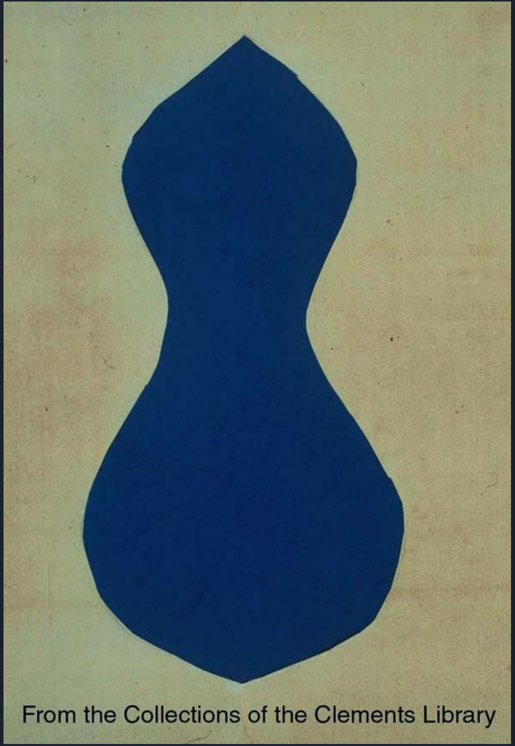
http://clements.umich.edu/exhibits/online/spies/methods-mask.html

Mask Letter (1777)

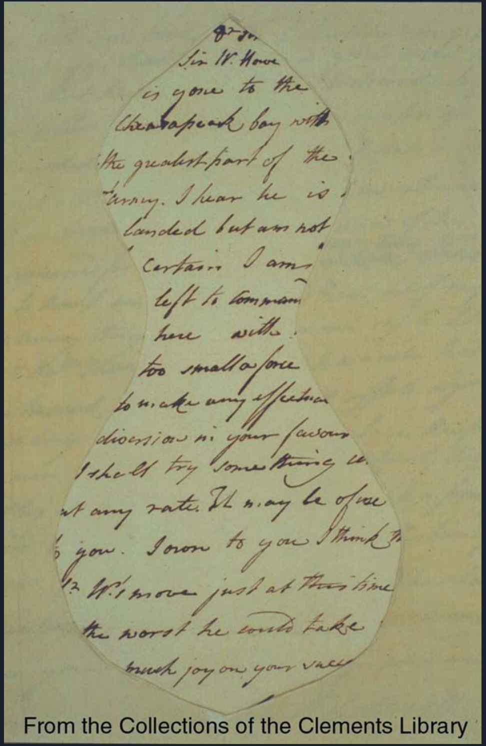


You will have heard, Dr Sir I doubt not long before this
can have reached you that Sir W. Howe is gone from hence. The
Rebels imagine that he is gone to the Eastward. By this time
however he has filled Chesapeak bay with surprize and terror.
Washington marched the greatest part of the Rebels to Philadelphia
in order to oppose Sir Wm's army. I hear he is now returned upon
finding none of our troops landed but am not sure of this, great part
of his troops are returned for certain. I am ~~[illegible]~~ certain
must be ruin to them. I am left to command here, half my force may
I am sure defend every thing here with much safety I shall therefore
send Sir W. 4 or 5 Batns. I have too small a force to invade the New England
provinces; they are too weak to make any effectual efforts against me and
you do not want any diversion in your favour I can therefore very well
spare him 1500 men I shall try something certainly towards the close
of the year not till then at any rate. It may be of use to inform you that
report says all yields to you. I own to you I think the business will
quickly be over now. Sr W's move just at this time has been Capital
Washington's have been the worst he could take in every respect
sincerely give you much joy on your success and am with
great sincerity your faithful [illegible]
H C

From the Collections of the Clements Library



From the Collections of the Clements Library

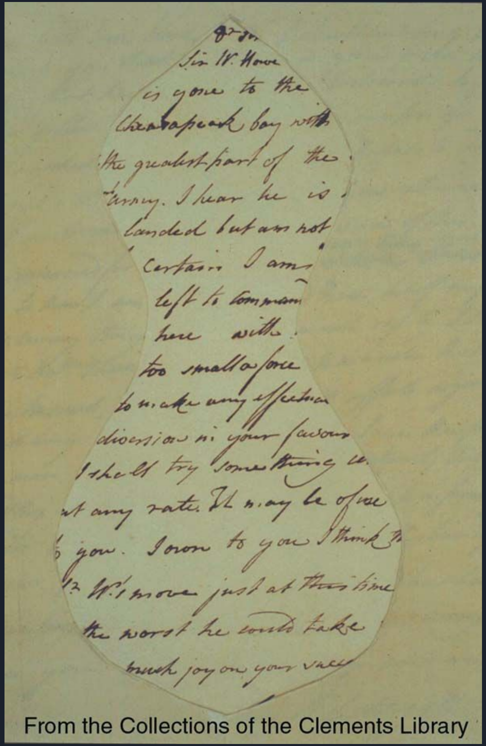


Dr Sir
Sir W. Howe
is gone to the
Chesapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain I am
left to command
here with
too small a force
to make any effectual
diversion in your favour
I shall try something ce
at any rate. It may be of use
to you. I own to you I think th
Sr W's move just at this time
the worst he could take
much joy on your succ

From the Collections of the Clements Library

http://clements.umich.edu/exhibits/online/spies/methods-mask.html

Mask Letter (1777)



D. Sir
Sir W. Howe
is gone to the
Chesapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain. I am
left to command
here with
too small a force
to make any effectual
diversion in your favour
I shall try something at
at any rate. It may be of use
to you. I own to you I think S
Sr W's move just at this time
the worst he could take
Much joy on your succ

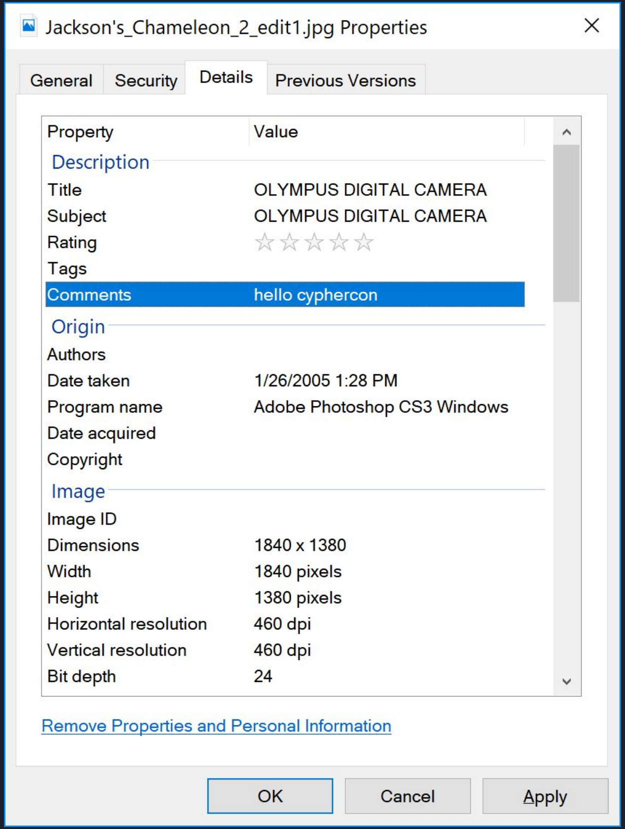
From the Collections of the Clements Library

Sir. W. Howe / is gone to the / Chesapeak bay with / the greatest part of the / army. I hear he is / landed but am not / certain. I am / left to command / here with / too small a force / to make any effectual / diversion in your favour. / I shall try something / at any rate. It may be of use / to you. I own to you I think / **Sr W's move just at this time / the worst he could take.** / Much joy on your success.

http://clements.umich.edu/exhibits/online/spies/methods-mask.html

Steganography Channels - Metadata

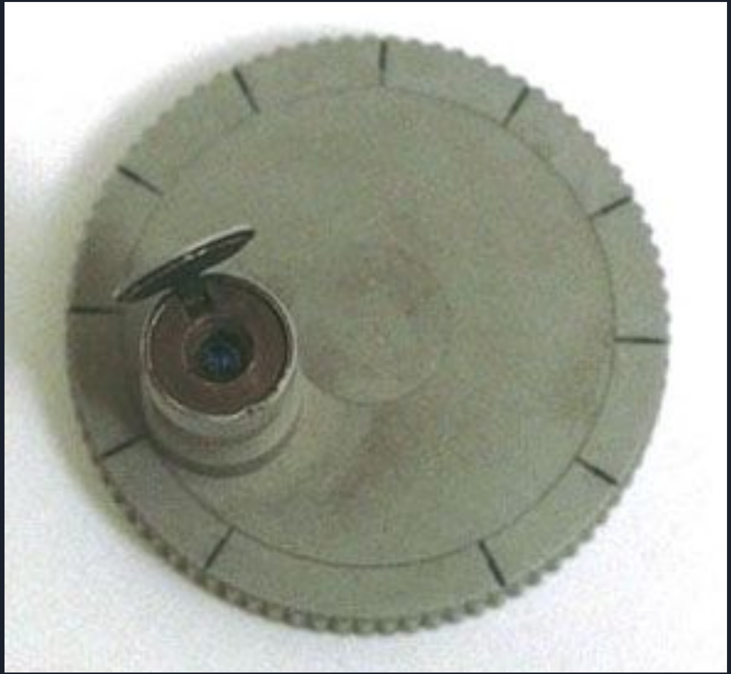
Steganography Channels - Metadata

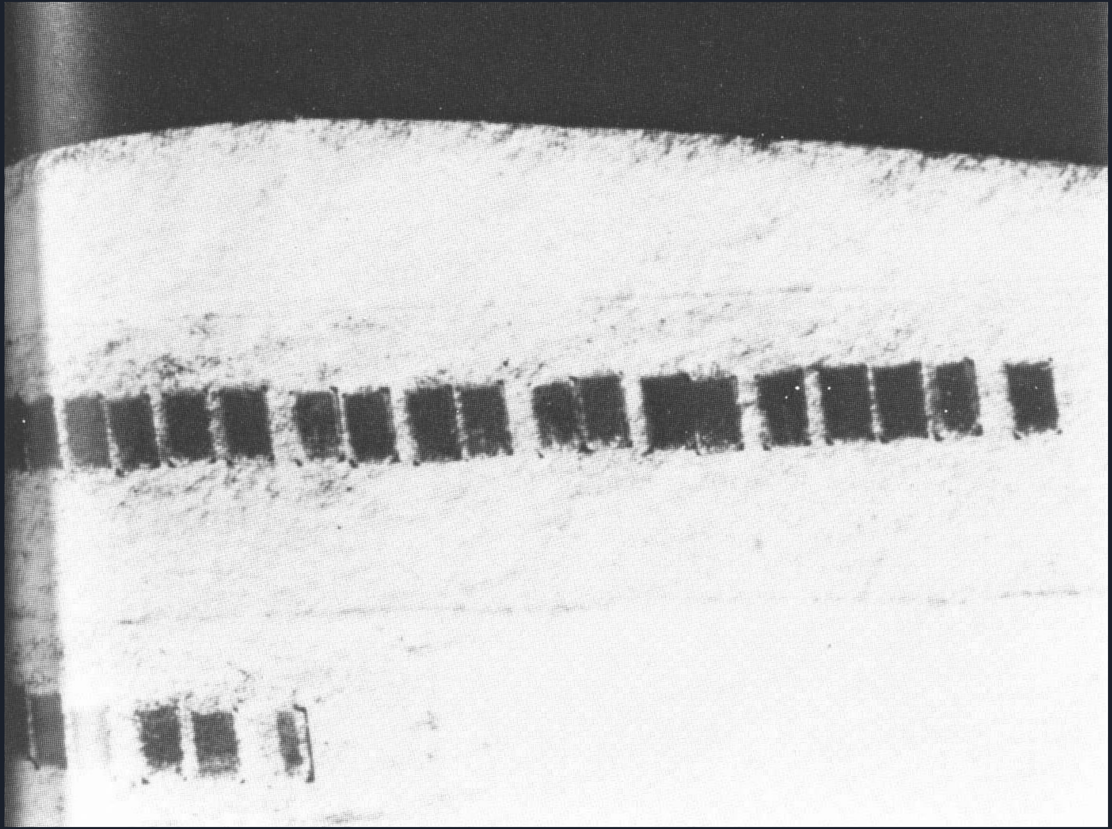


Jackson's_Chameleon_2_edit1.jpg Properties

Property	Value
Description	
Title	OLYMPUS DIGITAL CAMERA
Subject	OLYMPUS DIGITAL CAMERA
Rating	☆☆☆☆☆
Tags	
Comments	hello cyphercon
Origin	
Authors	
Date taken	1/26/2005 1:28 PM
Program name	Adobe Photoshop CS3 Windows
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	1840 x 1380
Width	1840 pixels
Height	1380 pixels
Horizontal resolution	460 dpi
Vertical resolution	460 dpi
Bit depth	24

Steganography Channels - Side Channels





Robustness and Perceptibility

	Fragile	Robust
Obvious		
Subtle		

Robustness and Perceptibility

	Fragile	Robust
Obvious	Caption	Watermark
Subtle	Noise	

Robustness and Perceptibility

https://www.flickr.com/photos/cafecredit/30931037323

Robustness and Perceptibility

https://www.flickr.com/photos/cafecredit/30931037323

Robustness and Perceptibility

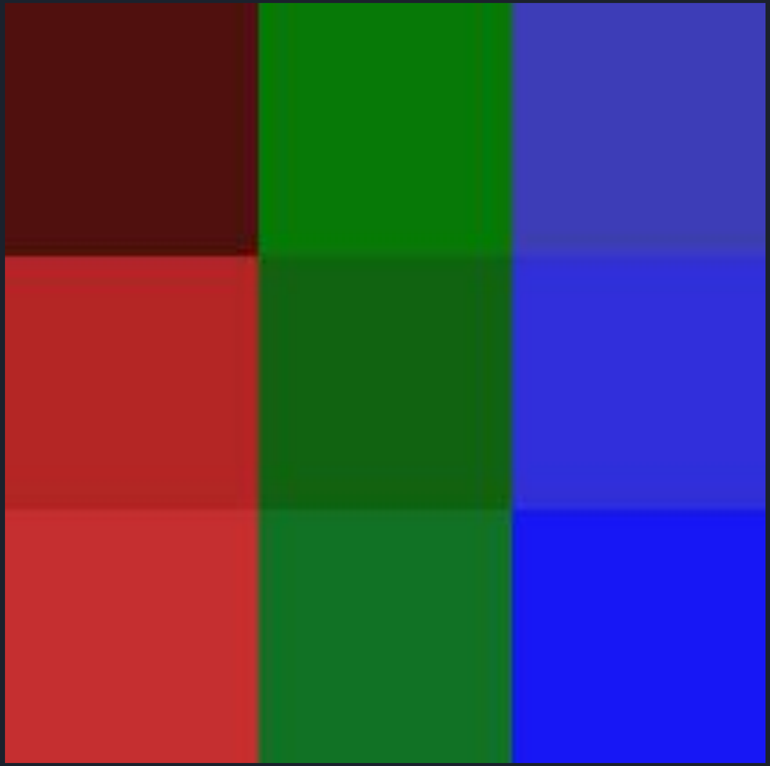
	Fragile	Robust
Obvious	Caption	Watermark
Subtle	Noise	Watermark

Least Significant Bits

006	000	000
166	000	000
179	000	000

000	094	000
000	052	000
000	121	000

000	000	142
000	000	201
000	000	249



Least Significant Bits

006	000	000
166	000	000
179	000	000

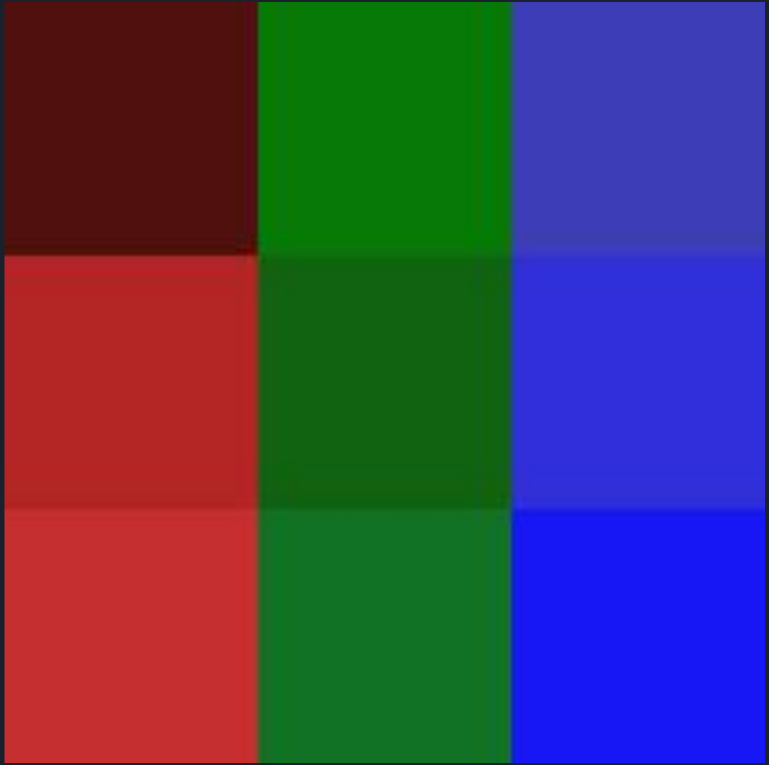
00000110	00000000	00000000
01110100	00000000	00000000
10110011	00000000	00000000

Least Significant Bits

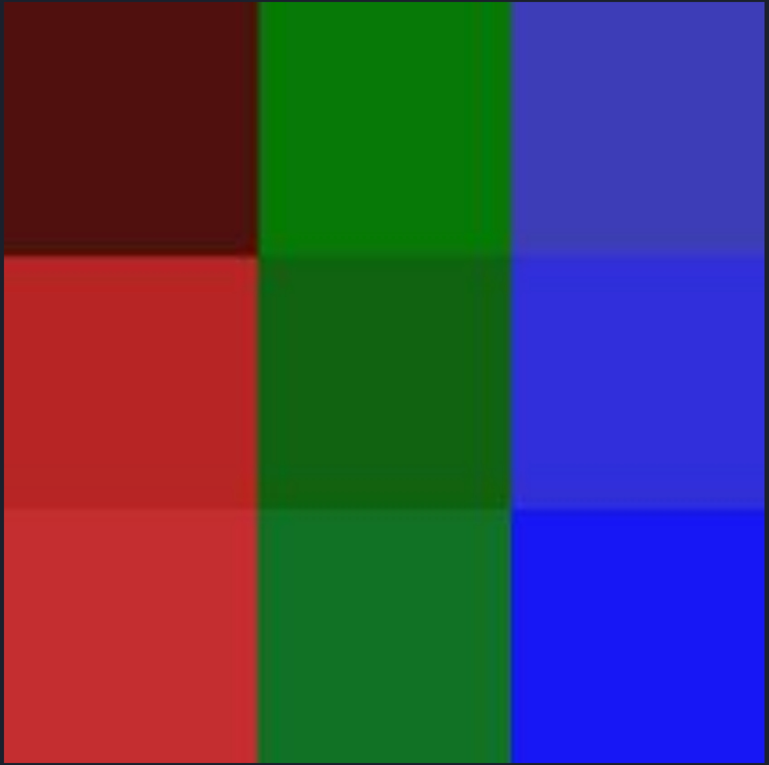
00000110	00000000	00000000
01110100	00000000	00000000
10110011	00000000	00000000

00000101	00000000	00000000
01110111	00000001	00000001
10110010	00000001	00000000

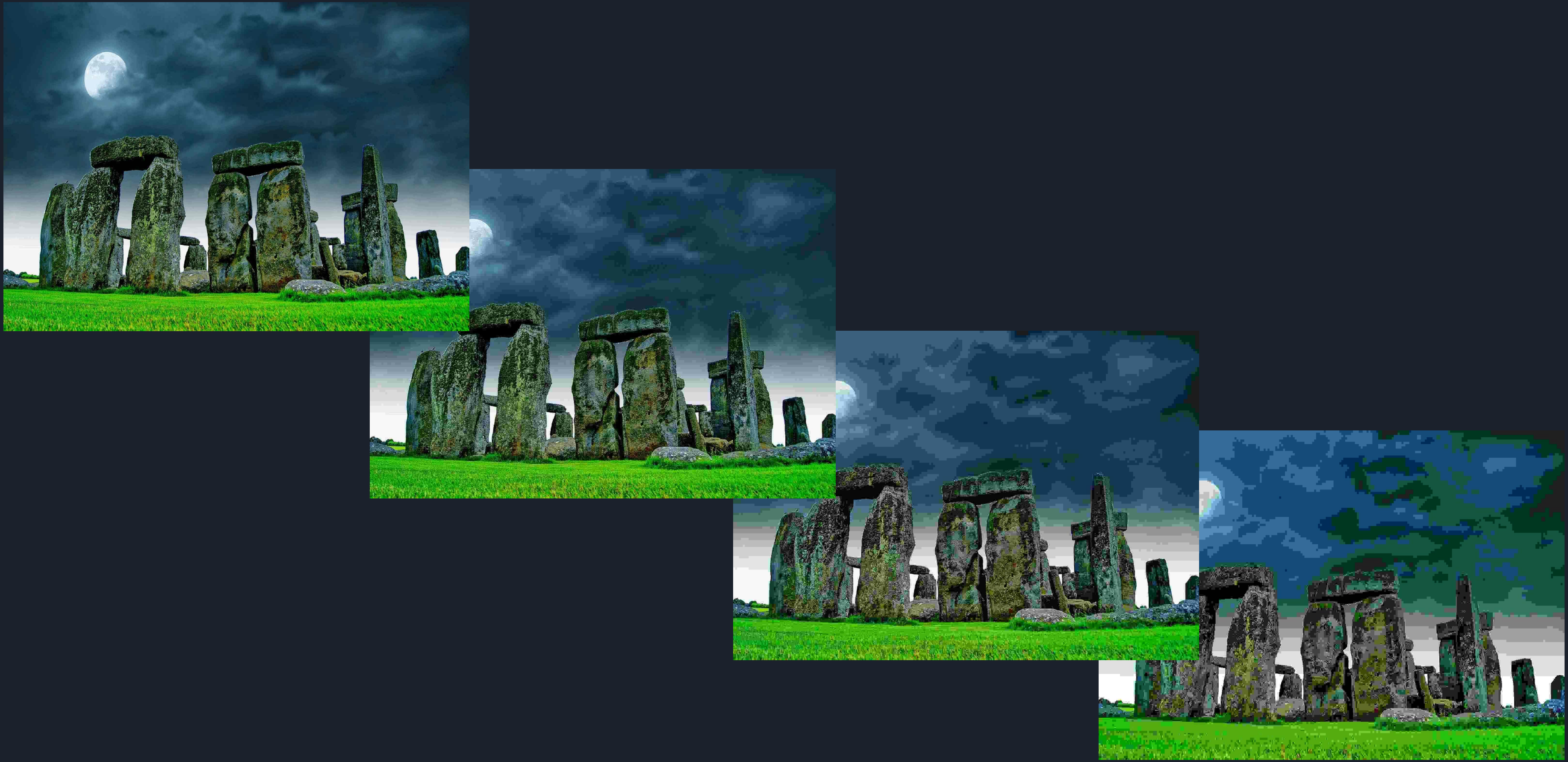
Least Significant Bits



“CYPHER”

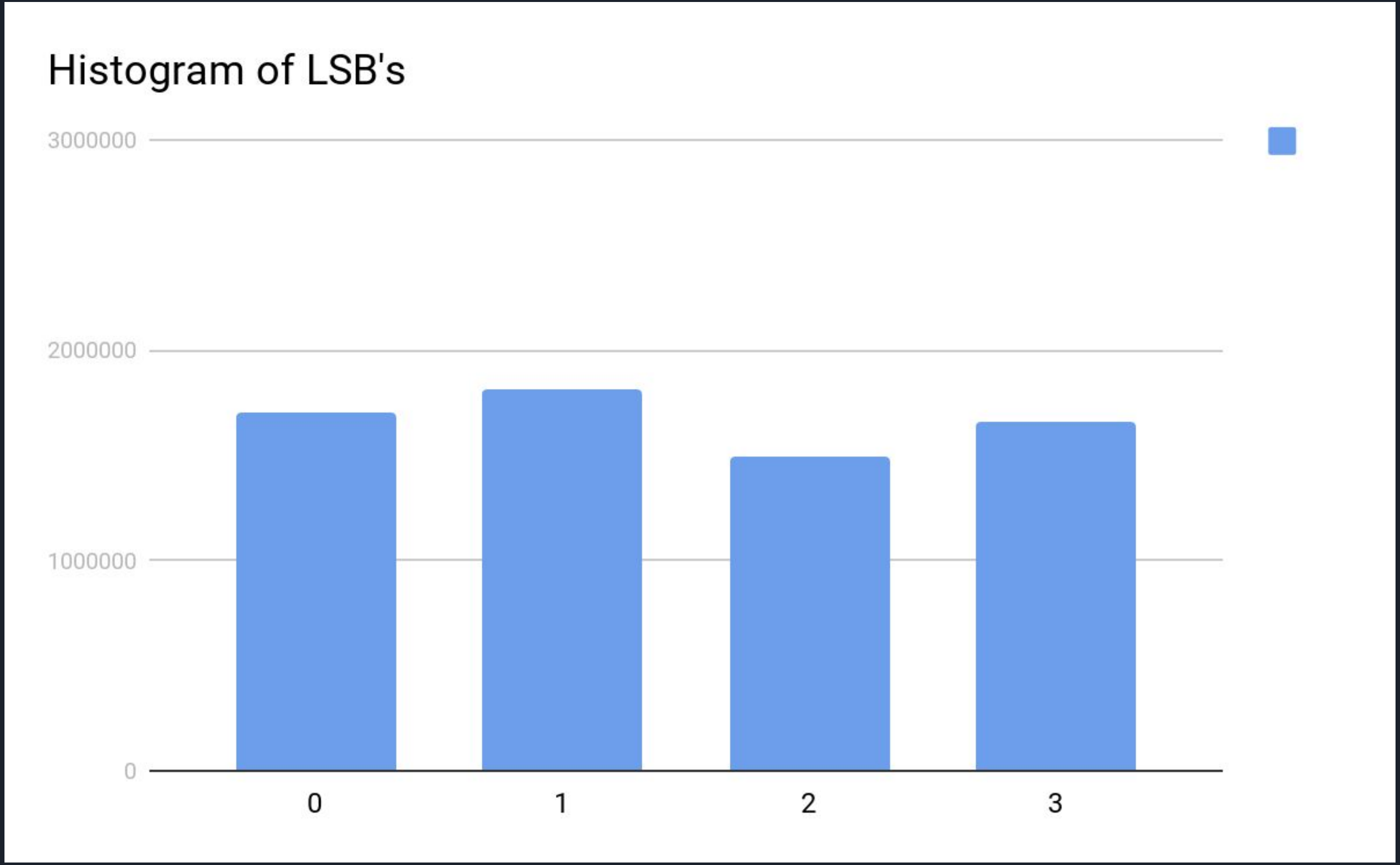


Lossy Compression

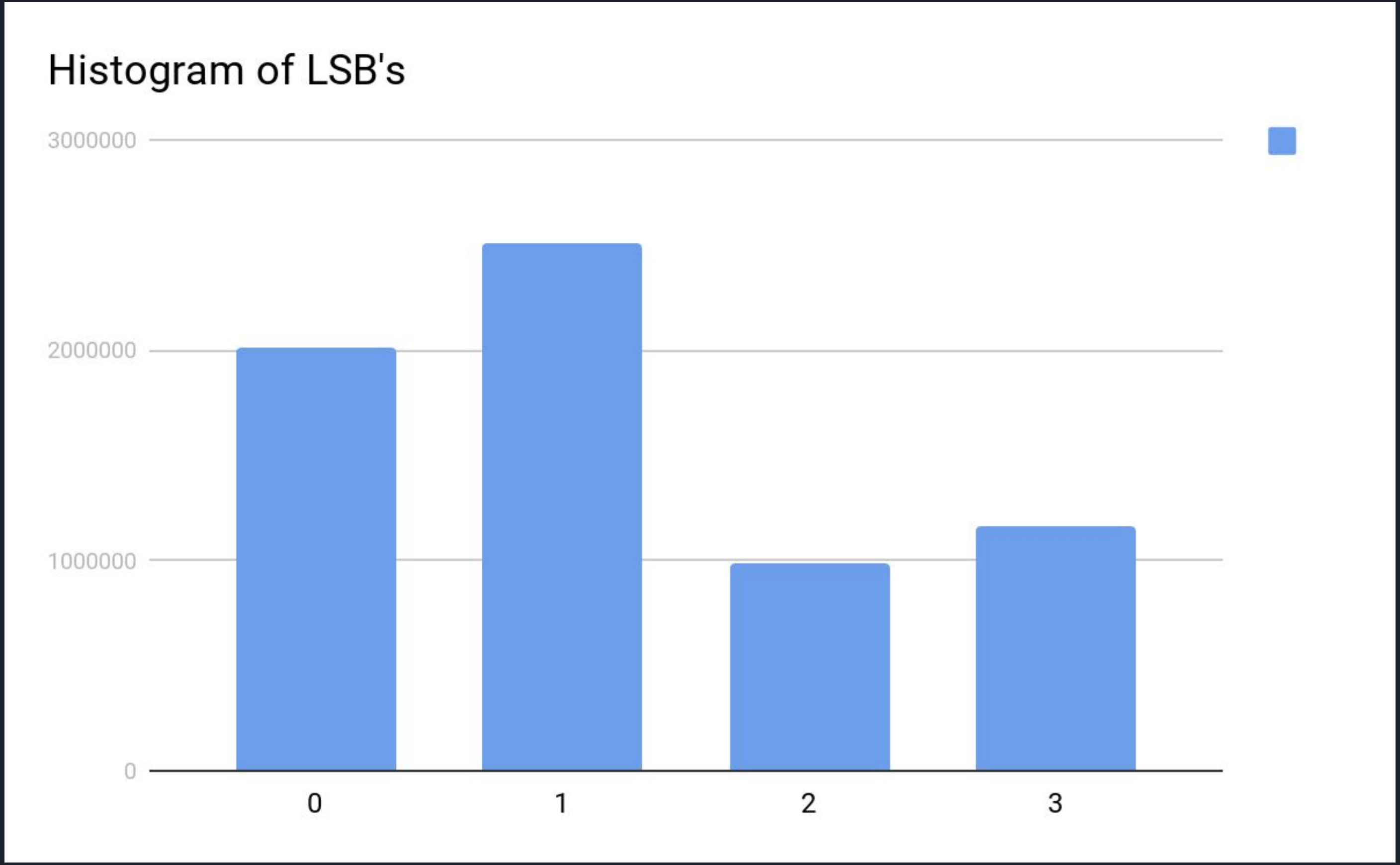


Detection & Attacks

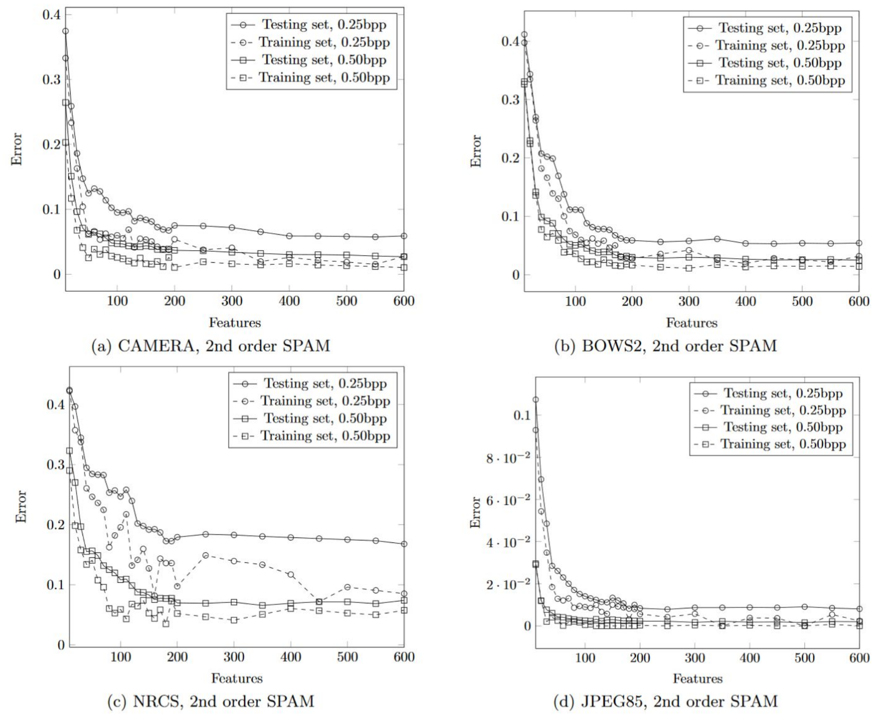
Detection



Detection



Detection



(a) CAMERA, 2nd order SPAM

(b) BOWS2, 2nd order SPAM

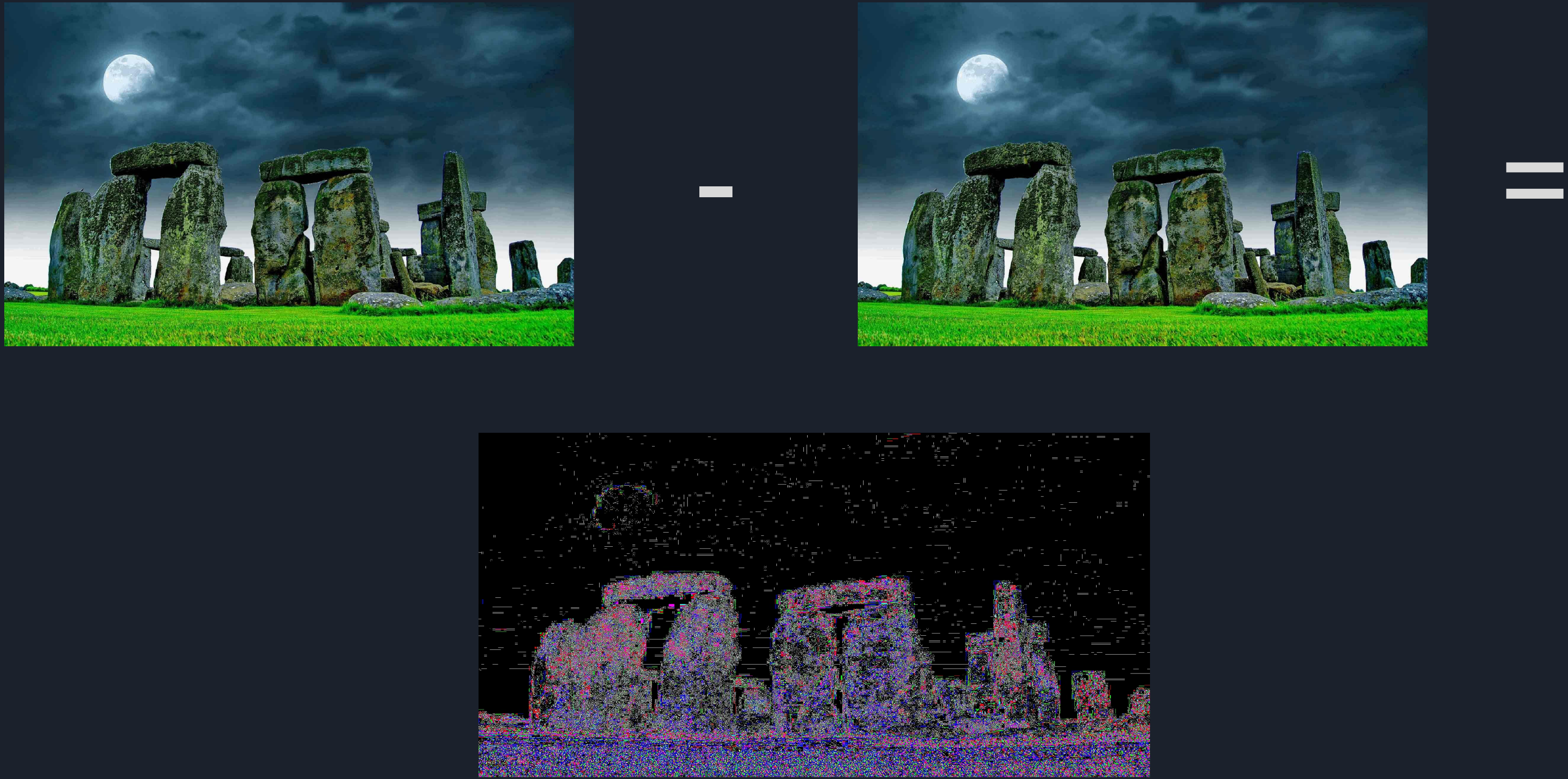
(c) NRCS, 2nd order SPAM

(d) JPEG85, 2nd order SPAM

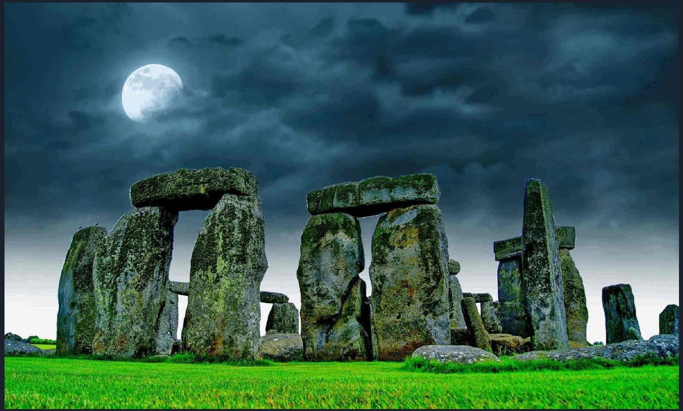
Figure 4: Discrepancy between errors on training and testing set plot with respect to number of features. Dashed line: errors on training set, solid line: errors on the testing set.

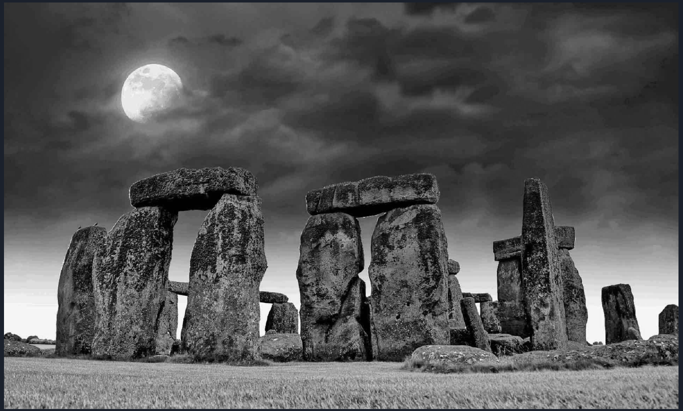
T. Pevny and P. Bas and J. Fridrich Steganalysis by subtractive pixel adjacency matrix. Steganalysis by subtractive pixel adjacency matrix, Princeton, NJ, September 7-8, 2009

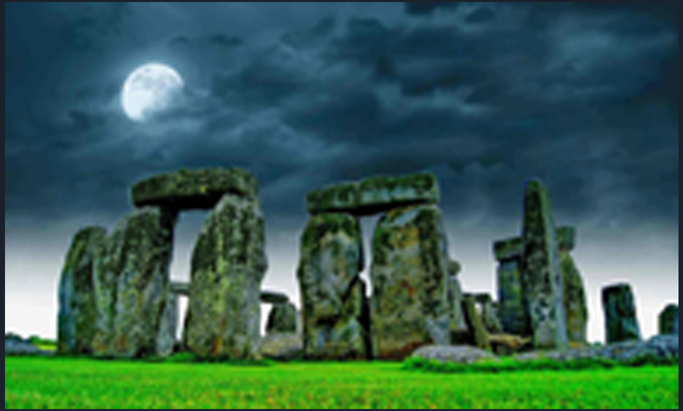
Detection

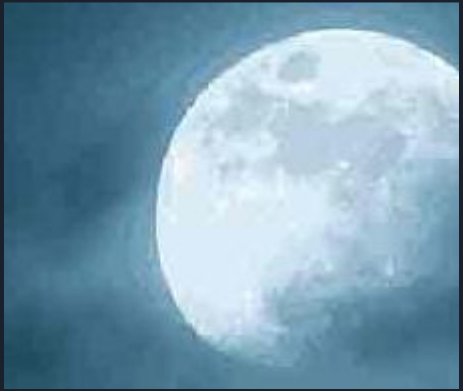


Defeating Steganography

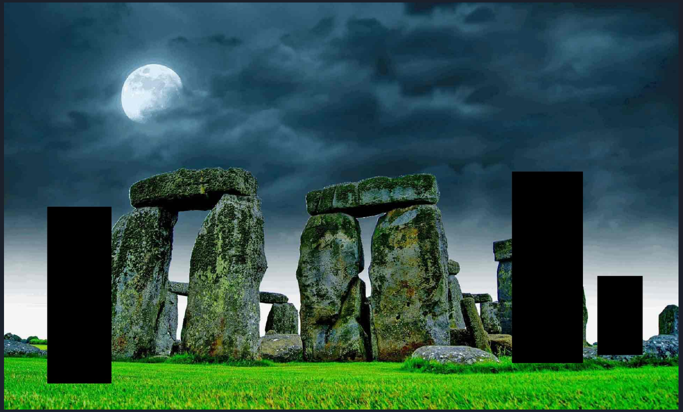


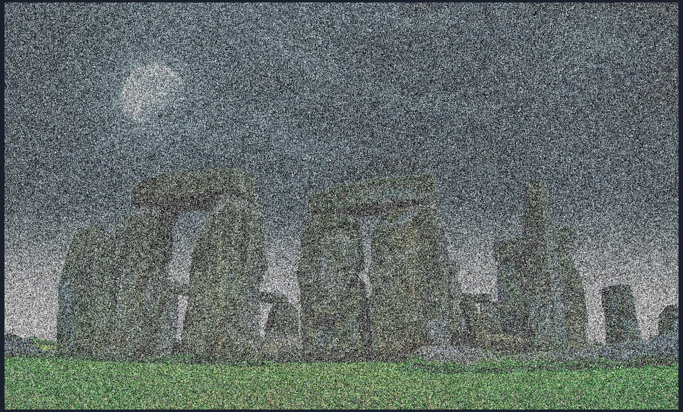


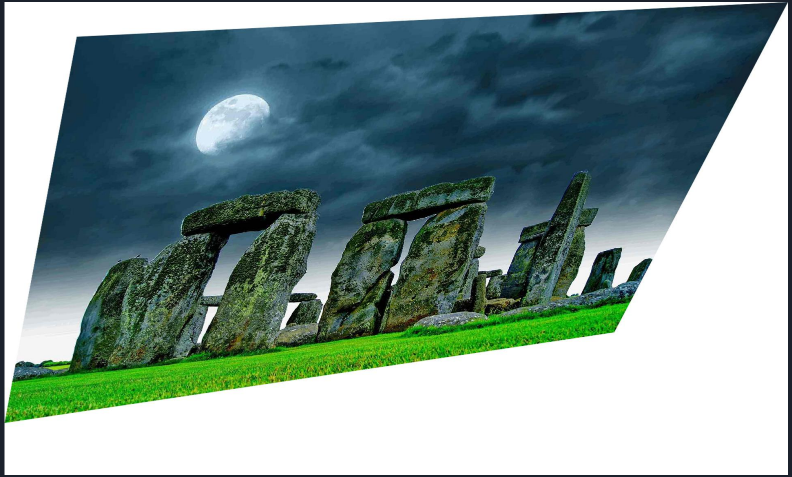




Defeating Steganography







Use Cases

https://commons.wikimedia.org/wiki/File:Confectionary_and_candy_at_display_in_Kiwi_Allehelgensgate_grocery_store-supermarket_in_Bergen,_Norway_2017-10-18_b.jpg

Use Cases

https://www.flickr.com/photos/k40s/2572079339

Use Cases

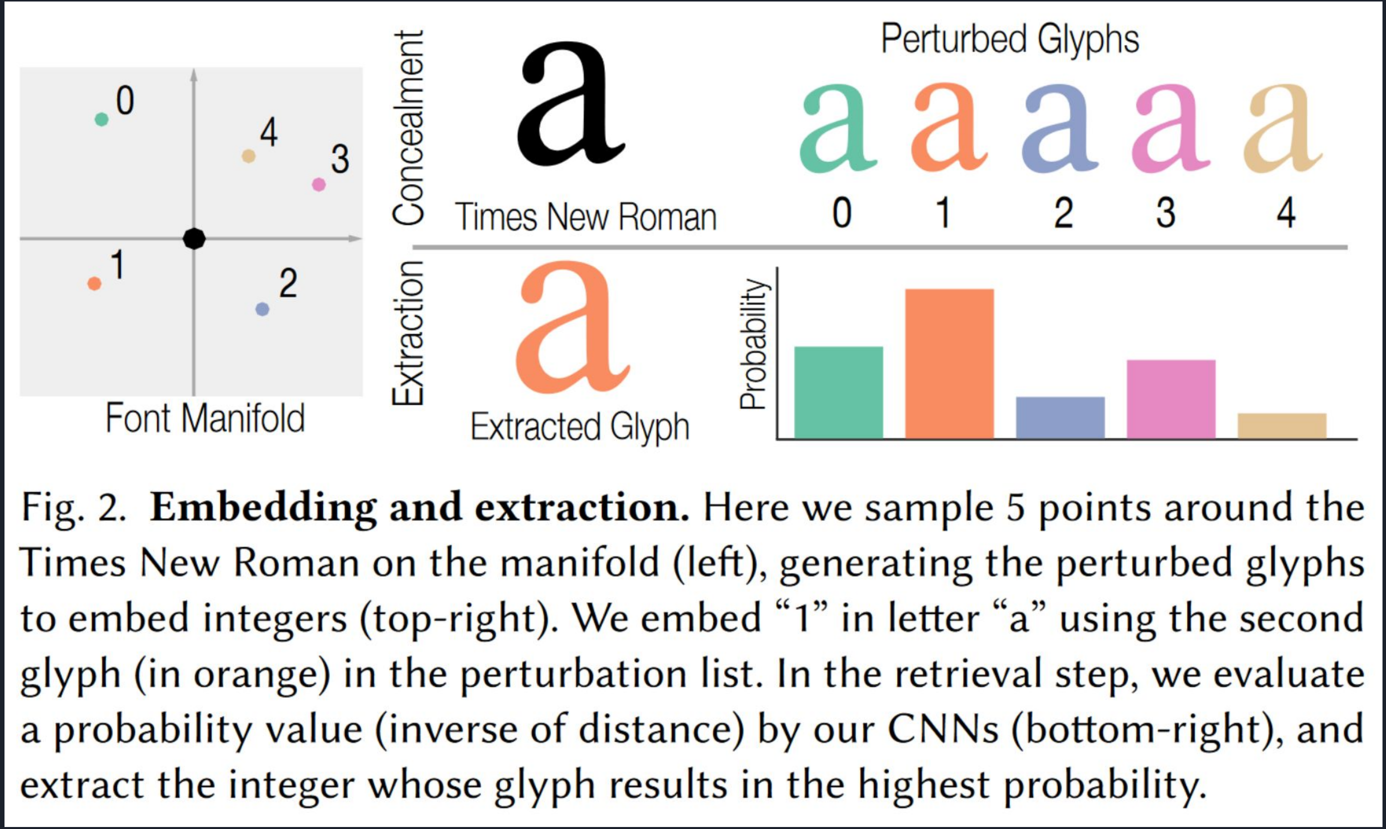
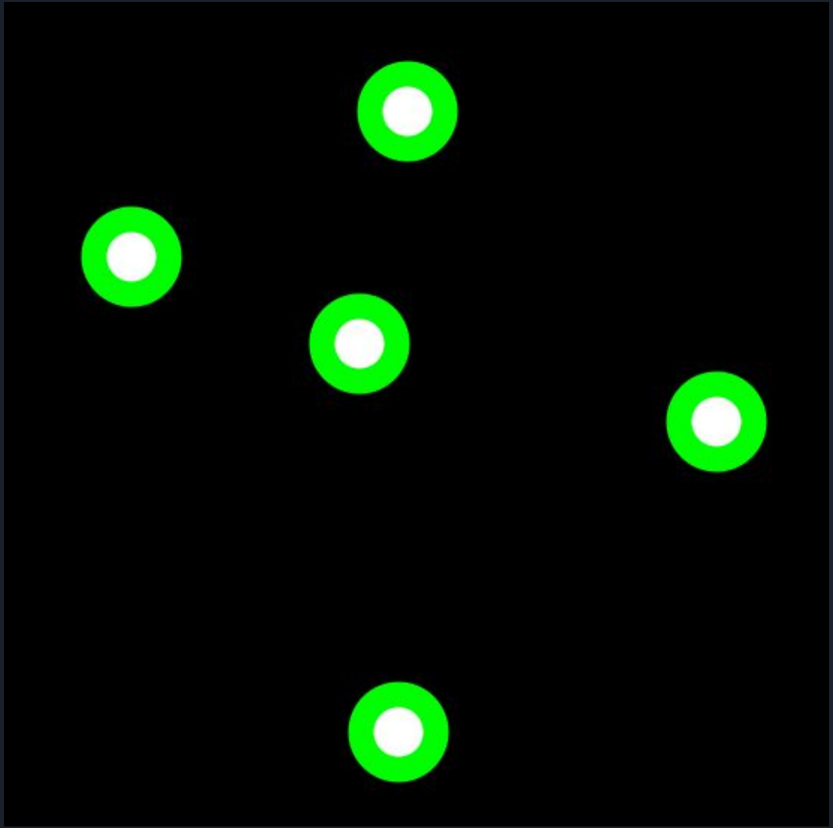
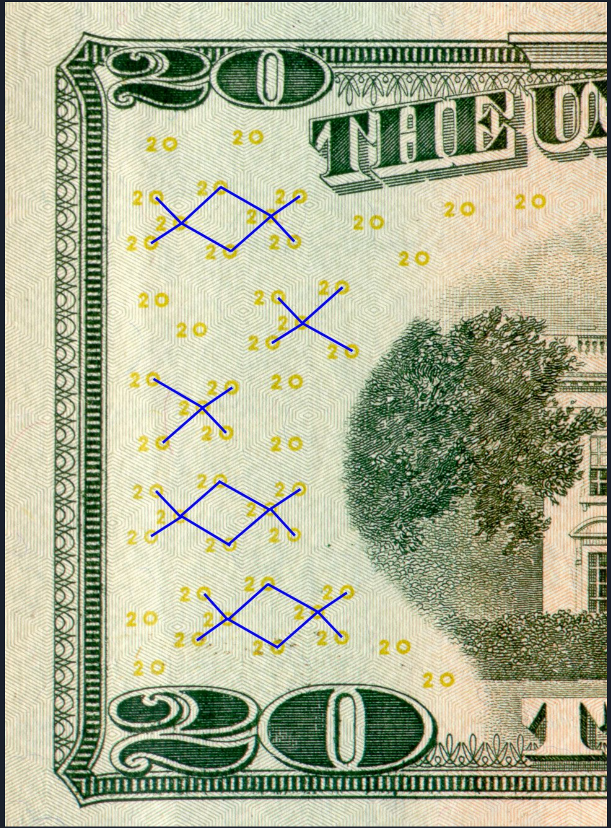


Fig. 2. **Embedding and extraction.** Here we sample 5 points around the Times New Roman on the manifold (left), generating the perturbed glyphs to embed integers (top-right). We embed “1” in letter “a” using the second glyph (in orange) in the perturbation list. In the retrieval step, we evaluate a probability value (inverse of distance) by our CNNs (bottom-right), and extract the integer whose glyph results in the highest probability.

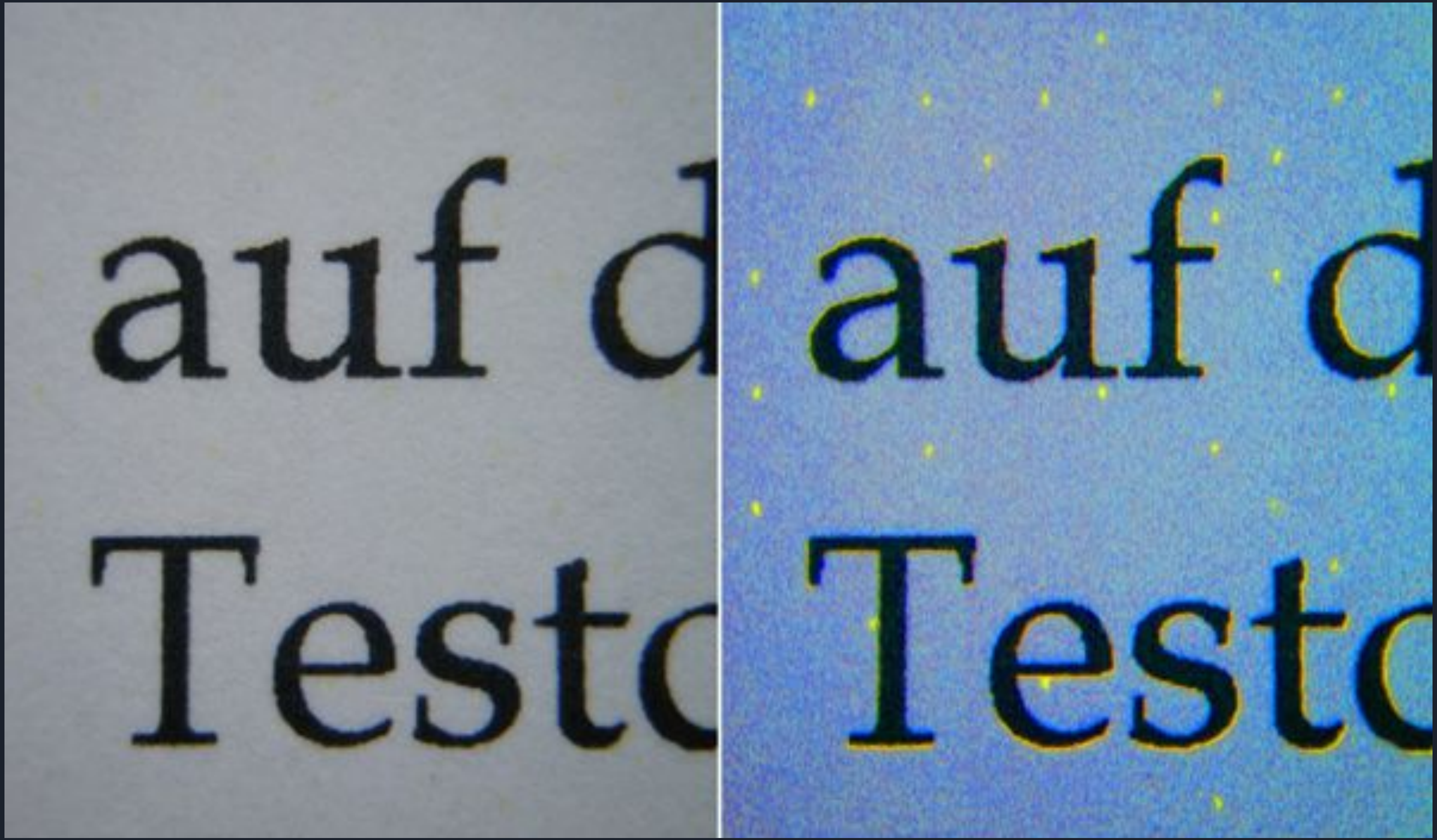
Chang Xiao, Cheng Zhang, and Changxi Zheng. 2018. FontCode: Embedding Information in Text Documents Using Glyph Perturbation. ACM Trans. Graph. 37, 2, Article 15 (February 2018), 16 pages. DOI: https://doi.org/10.1145/3152823

Use Cases - Anti-Counterfeiting

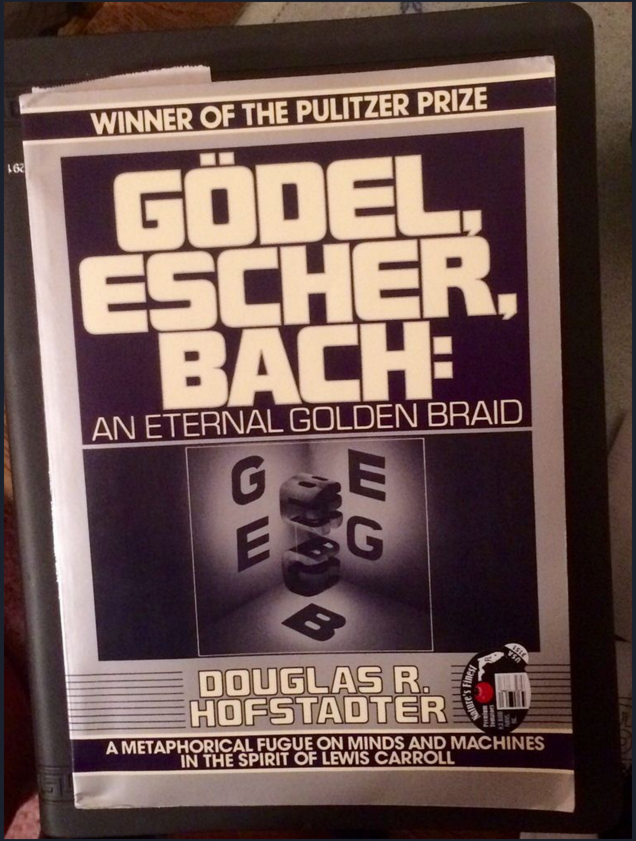




Use Cases



Learning More


WINNER OF THE PULITZER PRIZE
GÖDEL, ESCHER, BACH:
AN ETERNAL GOLDEN BRAID
DOUGLAS R. HOFSTADTER
A METAPHORICAL FUGUE ON MINDS AND MACHINES IN THE SPIRIT OF LEWIS CARROLL

https://www.flickr.com/photos/byzantiumbooks/22787526418

WHAT'S THIS?
DOUGLAS HOFSTADTER'S SIX-WORD AUTOBIOGRAPHY. AFTER ALL THOSE 700-PAGE TOMES, I GUESS HE WANTED TO TRY FOR BREVITY.
HUH. LET'S SEE...
I'M SO META, EVEN THIS ACRONYM
...WHOA.
I THINK HE NAILED IT.

https://xkcd.com/917/

Learning More

Kali - Steghide and Stegosuite

FontCode: http://www.cs.columbia.edu/cg/fontcode/

HUGO: Tomas Pevny, Tomas Filler, Patrick Bas. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography. Information Hiding, Jun 2010, Calgary, Canada. pp.2010, 2010. <hal-00541353>

SPAM: T. Pevny, P. Bas and J. Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 215-224, June 2010.
doi: 10.1109/TIFS.2010.2045842

SIGGRAPH & CVPR

HIDDEN IN PLAIN SIGHT

Ryan Fox

foxrow.com

Slides: https://foxrow.com/assets/stego.pdf

Twitter: @ryan_fox