Steganography

Alex Toumazis

History

- Herodotus - wax tablets, slave heads
- WWI - microdots, invisible ink
- Vietnam - morse code blinks

Users

- Military - e.g. spread spectrum/frequency hopping
- Criminals - and therefore law enforcement
- Internet users in repressive countries (or who are just paranoid)

Steganography vs Watermarking

- Undetectable
- Cover work irrelevant
- Robust
- data-carrying

- Robust
- Cover work important
- Undetectability can be useful
- zero-bit or data-carrying

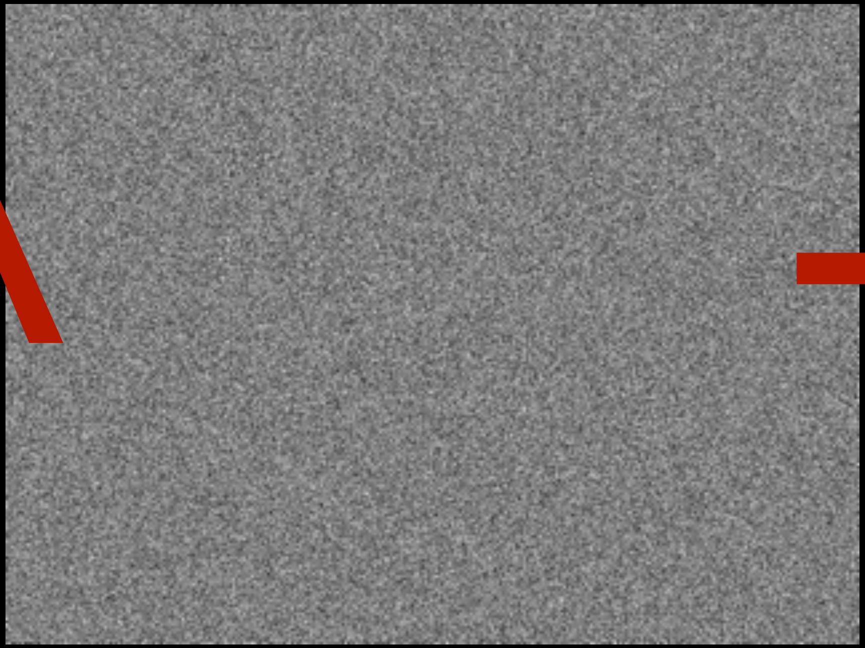
Demo

Embedding Hidden Data in Images

LSB

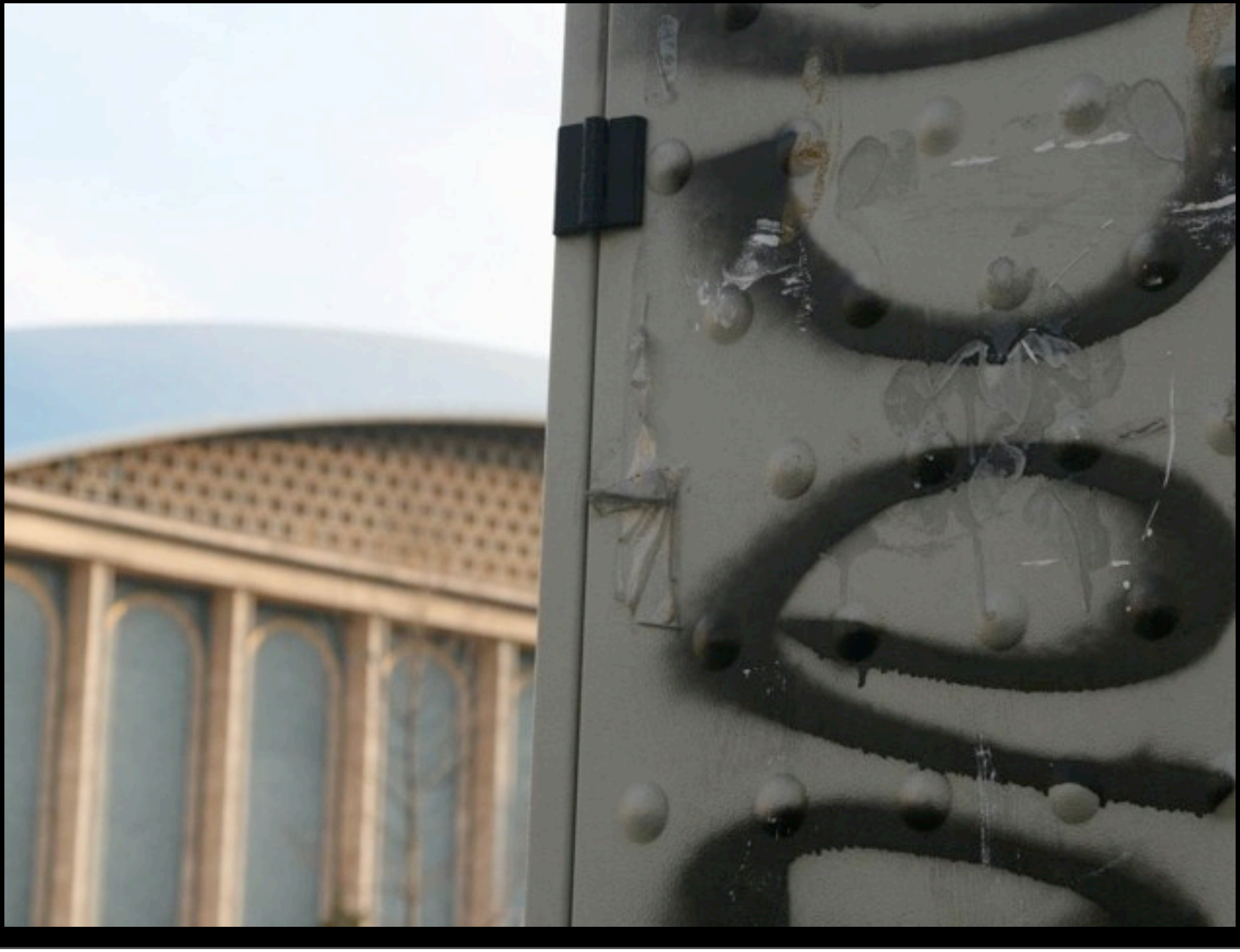
- Simply overwrite each pixel’s least significant bit with message
- In this demo, I encoded a 1-bit image into the green channel of a color photograph
- To attempt to hide the message, it’s been encrypted with a one-time pad

^

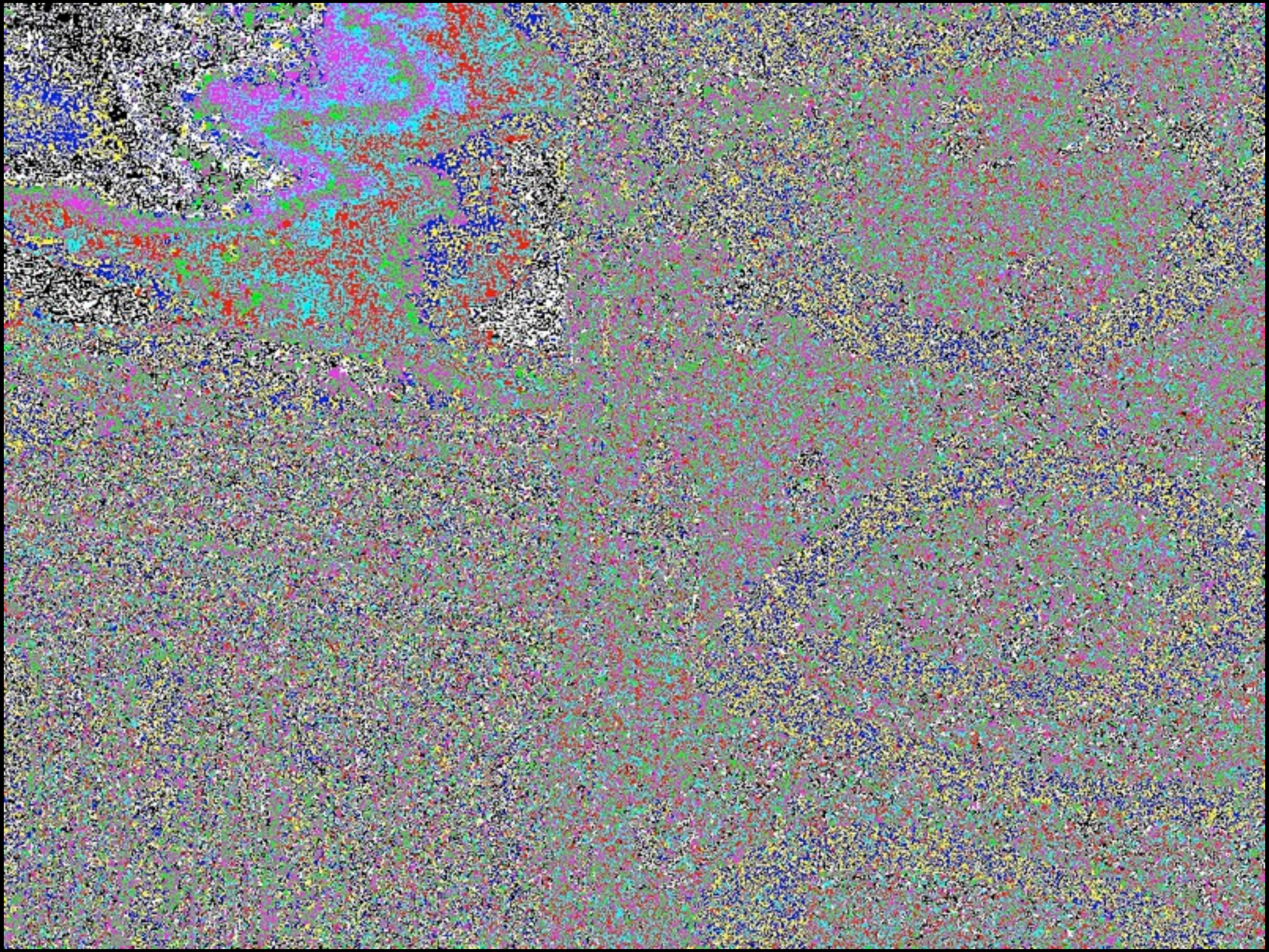


+

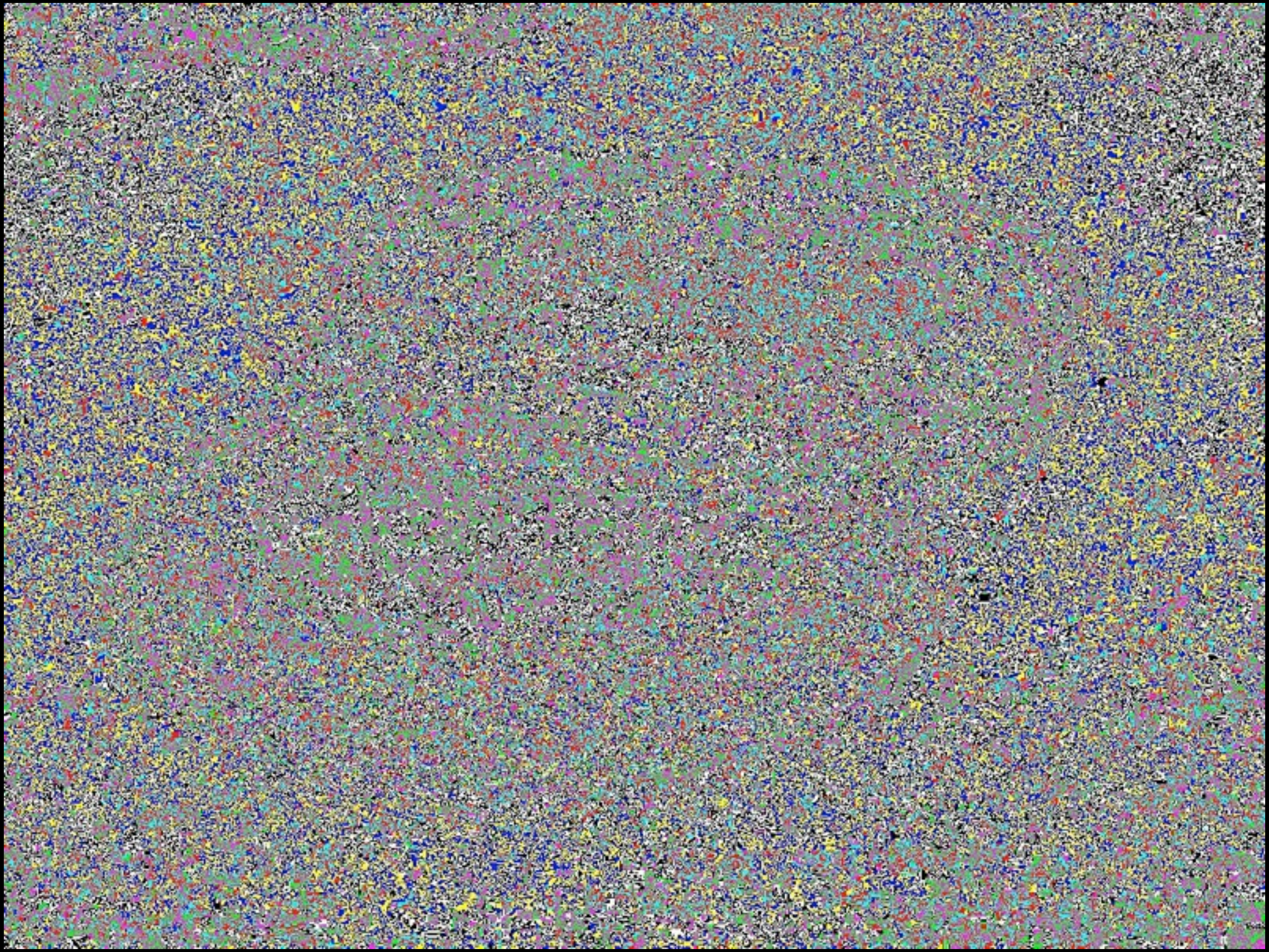
=



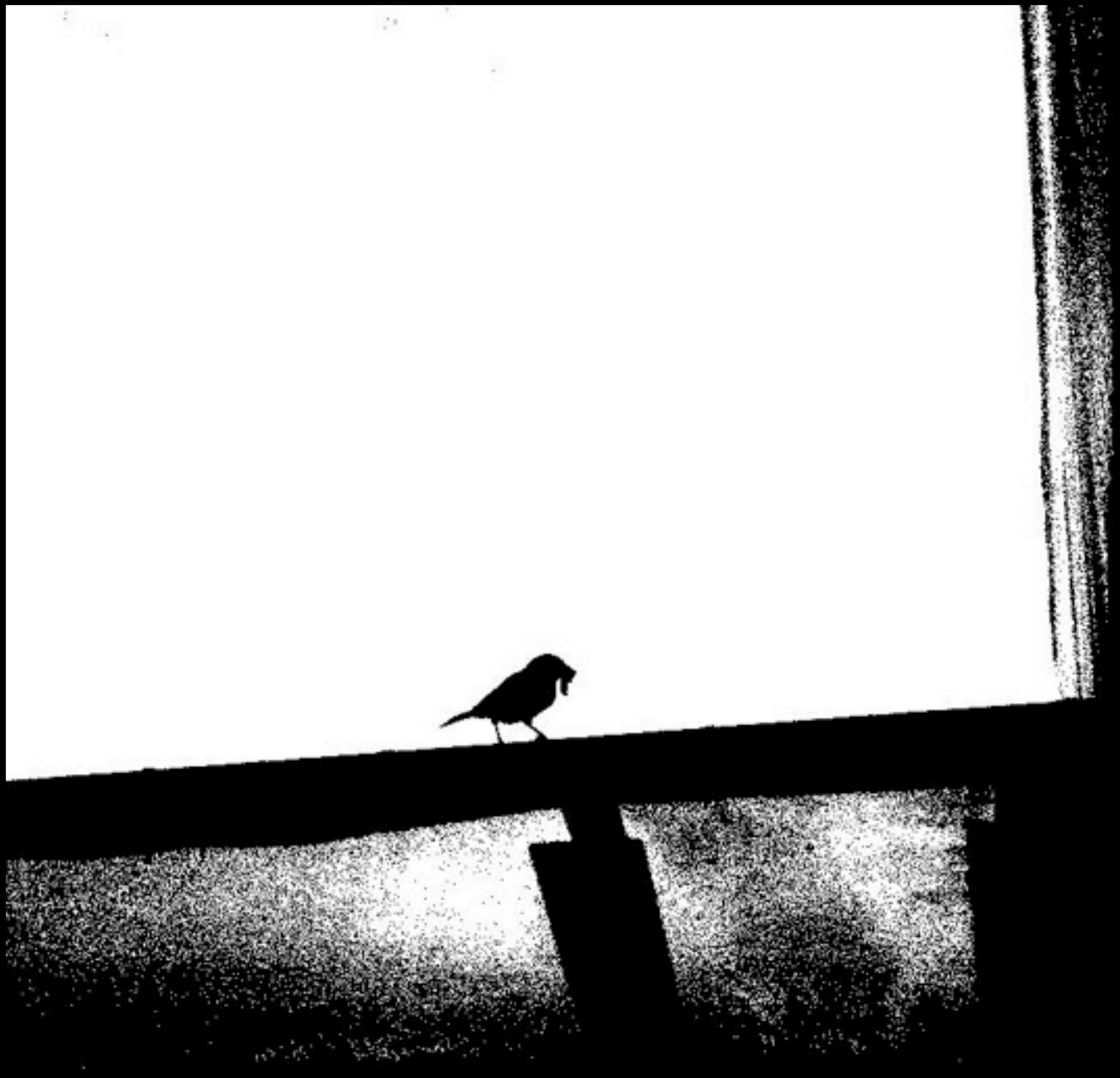
LSB: Original



LSB: Modified



Decrypted G LSBs

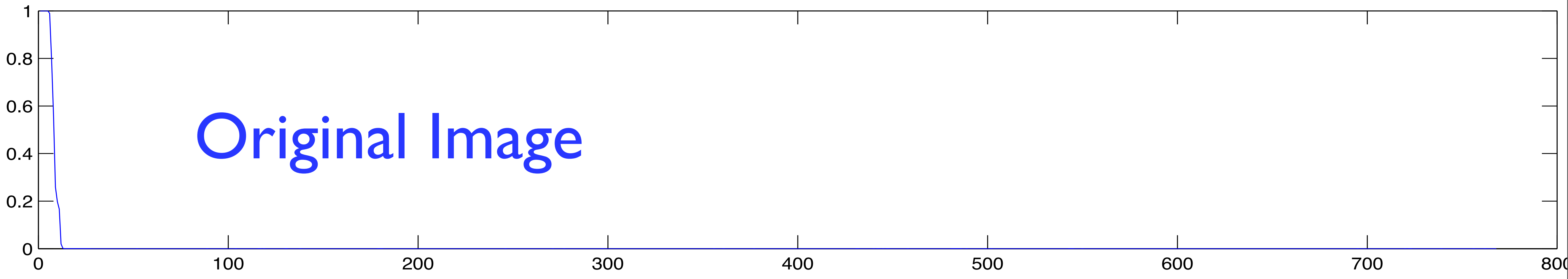


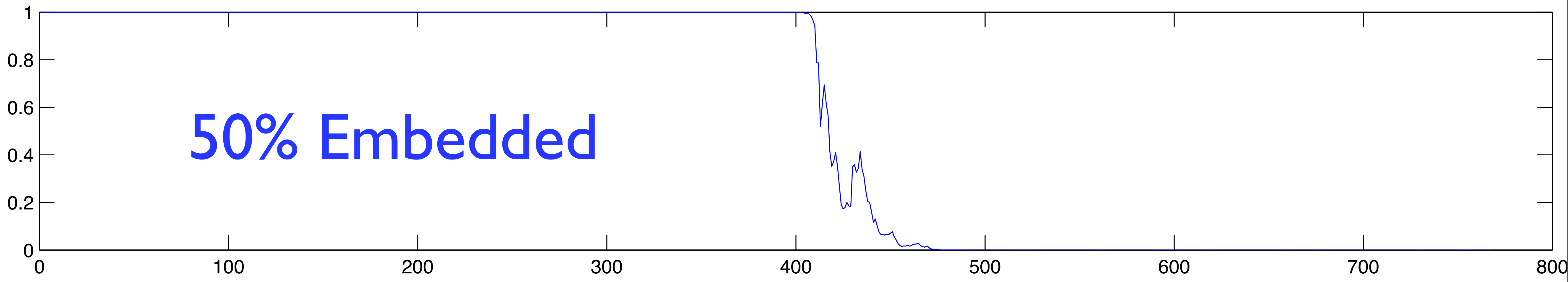
Statistical Attack

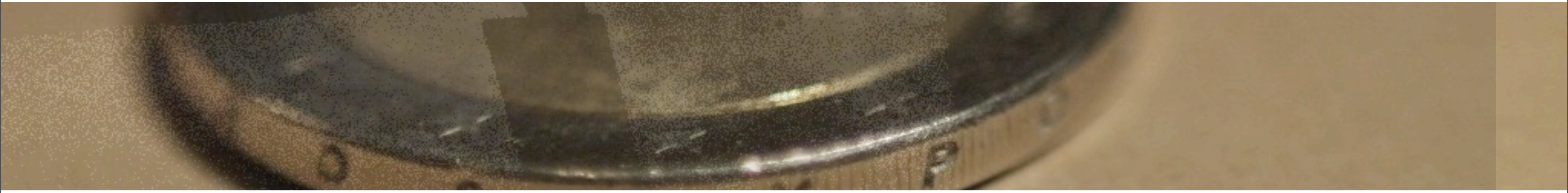
- Real LSBs are not (pseudo)random!
- χ^2 test:
  - Separate pixel values into k buckets
  - If LSB are random, buckets 2i and 2i+1 will have similar number of pixels
  - χ^2 test quantifies this and allows extraction of the probability of the data being consistent with Gaussian (random) distribution.

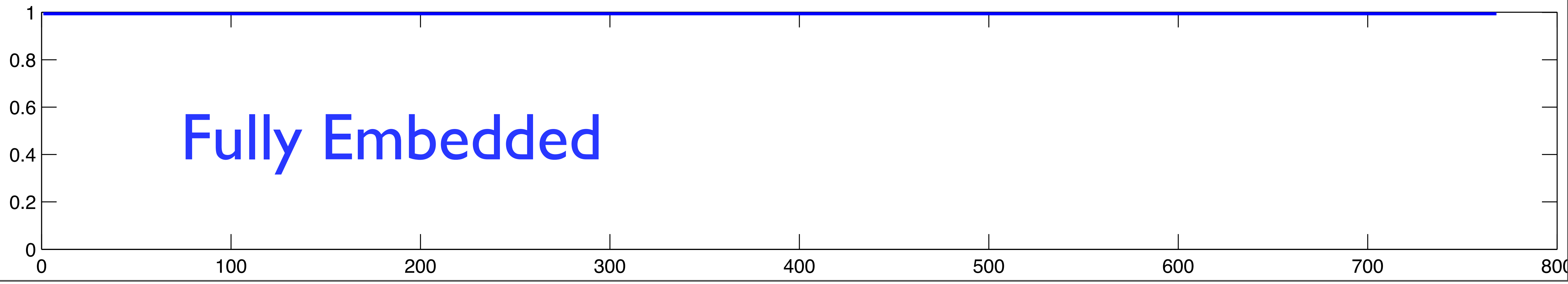
Plotting p(random)

- Plots show cumulative probability of embedded random data in the LSB against image row.


Original Image


50% Embedded




Fully Embedded

JSTEG

- Similar concept: alter LSB of DCT coefficients
- As each coefficient affects many pixels, this shouldn't be visible

For a long time I used to go to bed early. Sometimes, when I had put out my candle, my eyes would close so quickly that I had not even time to say "I'm going to sleep." And half an hour later the thought that it was time to go to sleep would awaken me; I would try to put away the book which, I imagined, was still in my hands, and to blow out the light; I had been thinking all the time, while I was asleep, of what I had just been reading, but my thoughts had run into a channel of their own, until I myself seemed actually to have become the subject of my book: a church, a quartet, the rivalry between Francois I and Charles V. This impression would persist for some moments after I was awake; it did not disturb my mind, but it lay like scales upon my eyes and prevented them from registering the fact that the candle was no longer burning. Then it would begin to seem unintelligible, as the thoughts of a former existence must be to a reincarnate spirit; the subject of my book would separate itself from me, leaving me free to choose whether I would form part of it or no; and at the same time my sight would return and I would be astonished to find myself in a state of darkness, pleasant and restful enough for the eyes, and even more, perhaps, for my mind, to which it appeared incomprehensible, without a cause, a matter dark indeed.

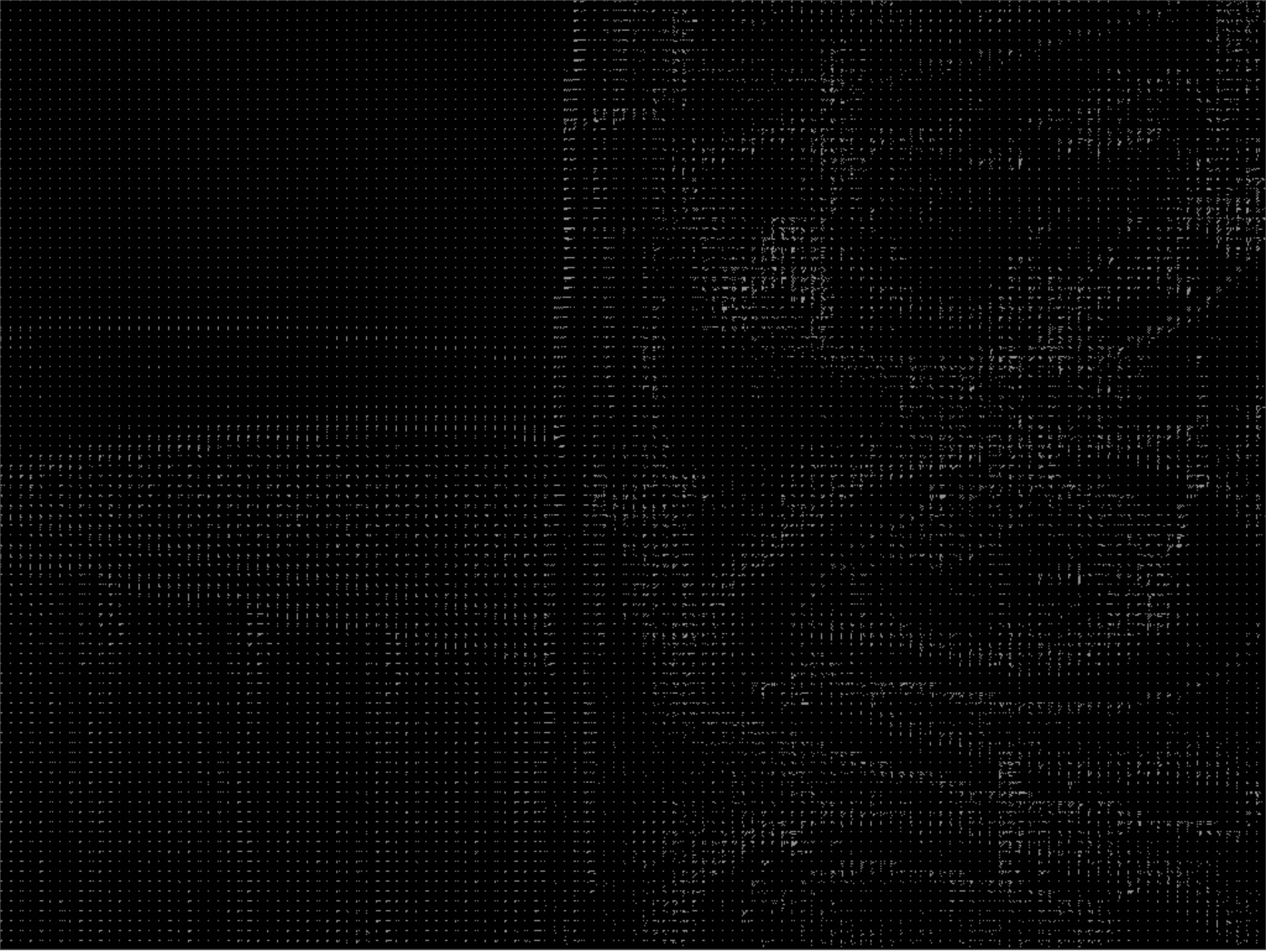
Key

Encrypted text

+

Original Image

Apply DCT



Apply Inverse DCT

Visual attack?

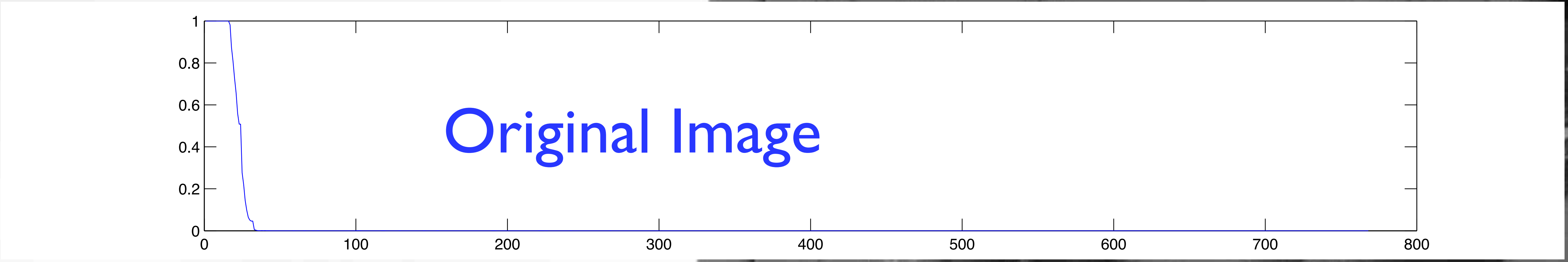
Embedded Message

No Message

Statistical Attack

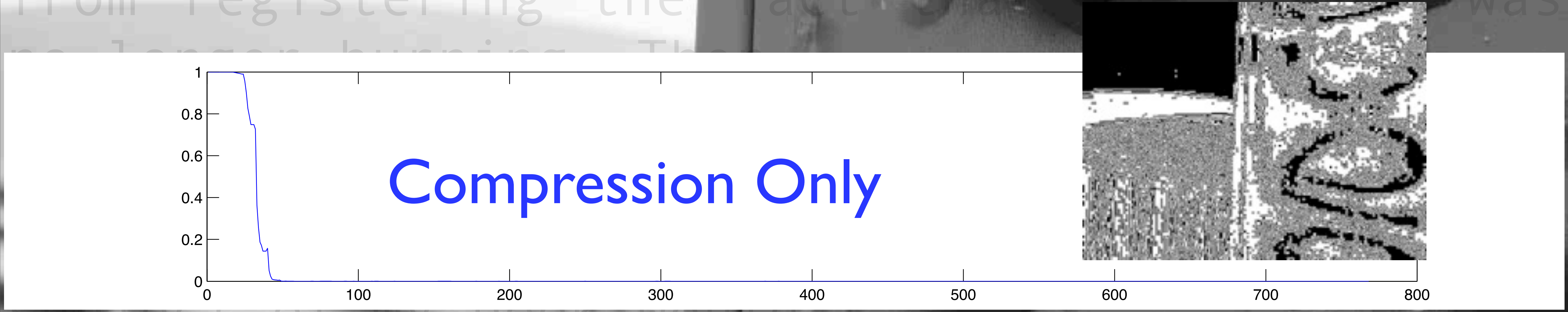
- Real LSB of DCT coefficients are not (pseudo) random!
- χ^2 test:
  - Separate coefficient values into k buckets
  - If LSB are random, buckets 2i and 2i+1 will have similar frequency
  - χ^2 test quantifies this and allows extraction of the probability of the data being consistent with Gaussian (random) distribution.

a church, a quartet; the rivalry between
Francois I and Charles V. This



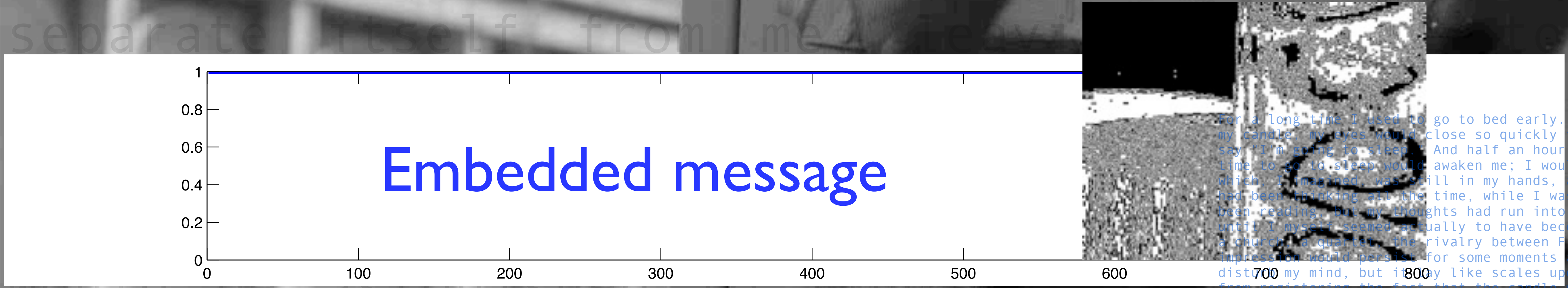
Original Image

from registering the fact that was
no longer burning. The



Compression Only

subject of my book would
separate itself from me



Embedded message

For a long time I used to go to bed early.
my candle, my eyes would close so quickly
say "I'm going to sleep." And half an hour
time to go to sleep would awaken me; I wou
which, I imagined, was still in my hands,
had been thinking all the time, while I wa
been reading, but my thoughts had run into
until I myself seemed actually to have bec
a church, a quartet, the rivalry between F
impression would persist for some moments
disturb my mind, but it lay like scales up
from registering the fact that the candle
it would begin to seem unintelligible, as
existence must be to a reincarnate spirit;
separate itself from me, leaving me free t
part of it or no; and at the same time my
would be astonished to find myself in a st
restful enough for the eyes, and even more
which it appeared incomprehensible, withou
indeed.

would be astonished to
of darkness, pleasant and
restful enough for the and even

Other Techniques

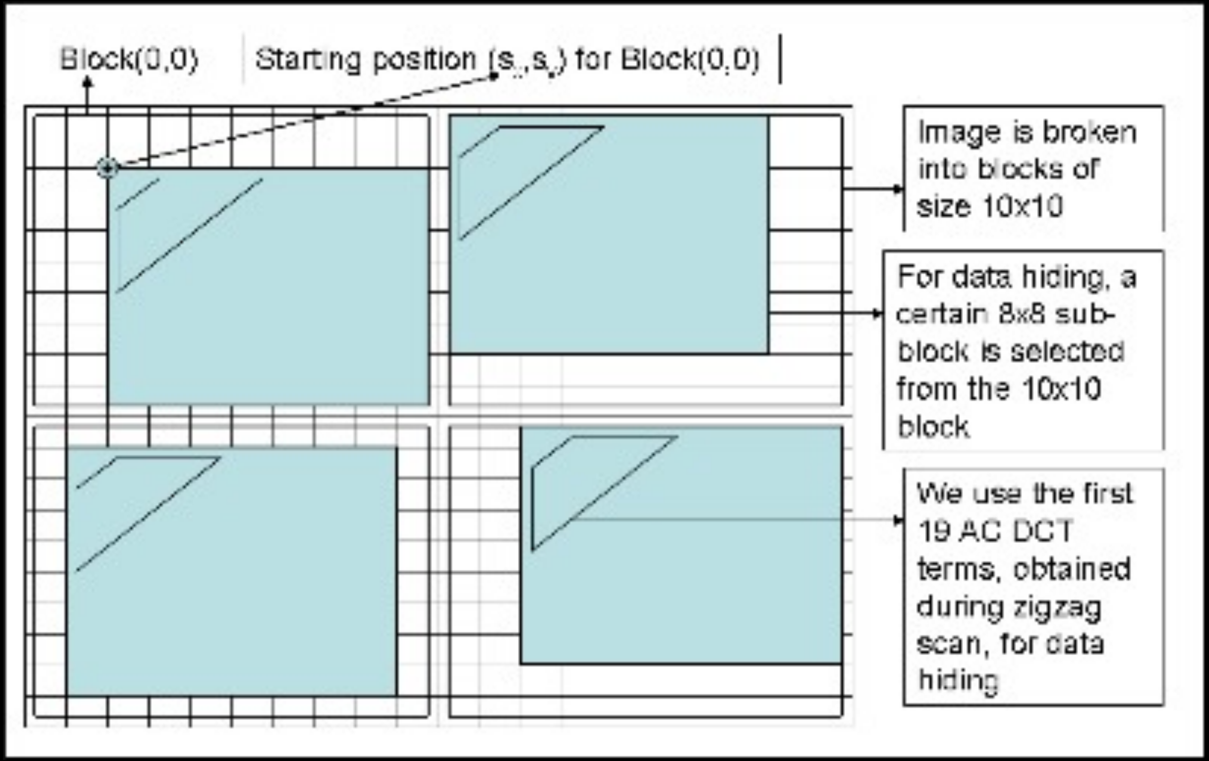
(Not implemented)

Spread-Spectrum

- Applicable to all media
- Attempts to spread signal evenly across entire cover work
- e.g. “Secure Spread Spectrum Watermarking for Multimedia”
    - This is a watermarking paper so I’ll stop here

YASS (2007)

- Similar to JSTEG
- Divide image into BxB blocks
- Pseudorandomly (based on key) select 8x8 block within each BxB block
- Compute DCT, hide data in low frequency AC components (Why?)



Block(0,0)

Starting position (s_x,s_y) for Block(0,0)

Image is broken into blocks of size 10x10

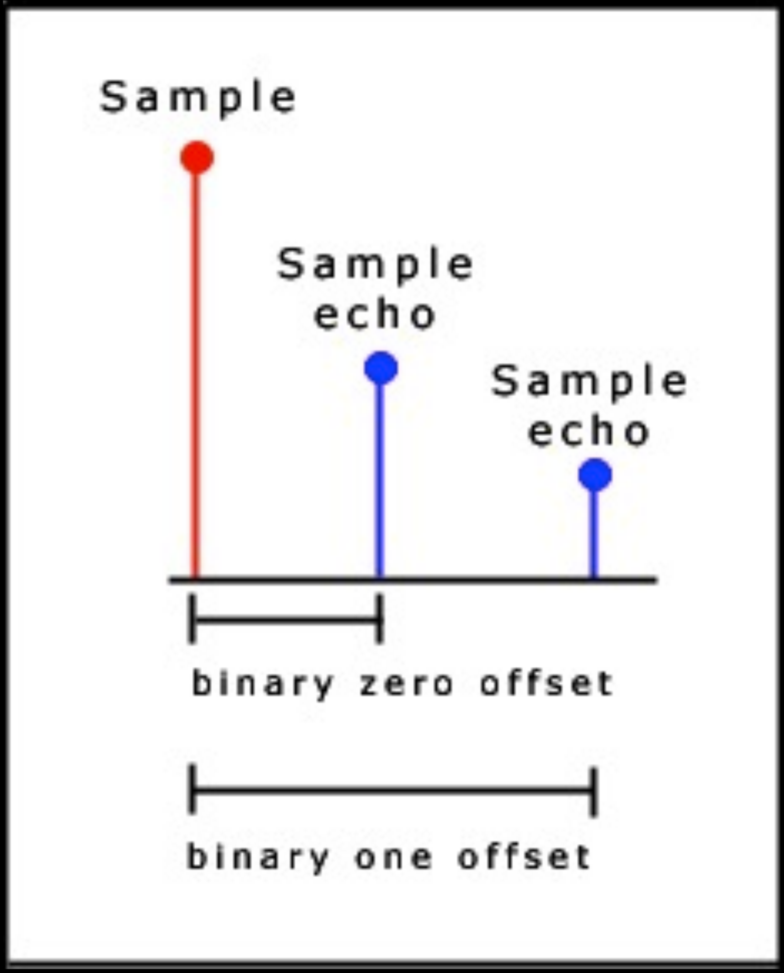
For data hiding, a certain 8x8 sub-block is selected from the 10x10 block

We use the first 19 AC DCT terms, obtained during zigzag scan, for data hiding

Echo Hiding (1996)

- Adds imperceptible echos to sound files

- Informations is encoded by varying parameters: offset, amplitude and decay



Audio Files for Audiophiles (2009)

- Uses ‘supraliminal’ channel
- Embeds data as audible beats or notes tailored to the cover work
- Different approach: attempts to achieve undetectability without imperceptibility
  - (so cover must be secret)
- Implementation is very fragile

?