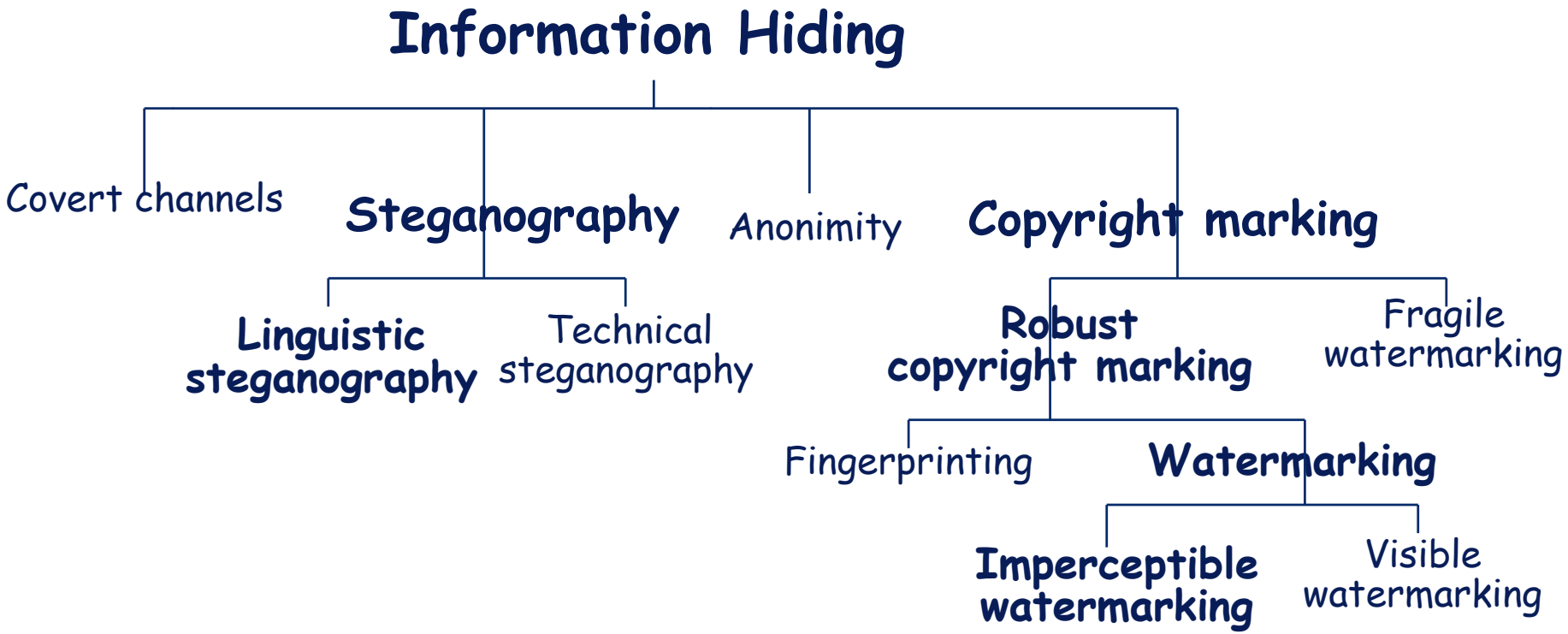
Information Hiding: Steganography & Steganalysis

Dr. Zoran Duric

Department of Computer Science
George Mason University
Office: Nguyen Engineering Building 4443
Email: zduric@cs.gmu.edu
URL: http://www.cs.gmu.edu/∼zduric/
URL: http://www.cs.gmu.edu/∼vislab/

Some slides from N. Johnson, Y. Kim, and & N. Memon



Source: F.L. Bauer, *Decrypted Secrets—Methods and Maxims of Cryptology.* Berlin, Heilderberg, Germany: Springer-Verlag, 1997.

Steganography

Covered writing

- From Herodotus to Thatcher (wax tablets, letter spacing)
- Messages should be undetectable (e.g. invisible ink)
- Messages concealed in media files (redundant bits, i.e. perceptually insignificant data)
- Perceptually insignificant data is common in (uncompressed) media files.

Null Cipher

Kahn, Codebreakers, 1967 (Sent by a German spy during WWI):

Apparently neutral's protest is thouroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

Kipper, Investigators guide to steganography, 2004:

News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Null Cipher

Sent by a German spy during WWI:

Apparently neutral's protest is thouroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

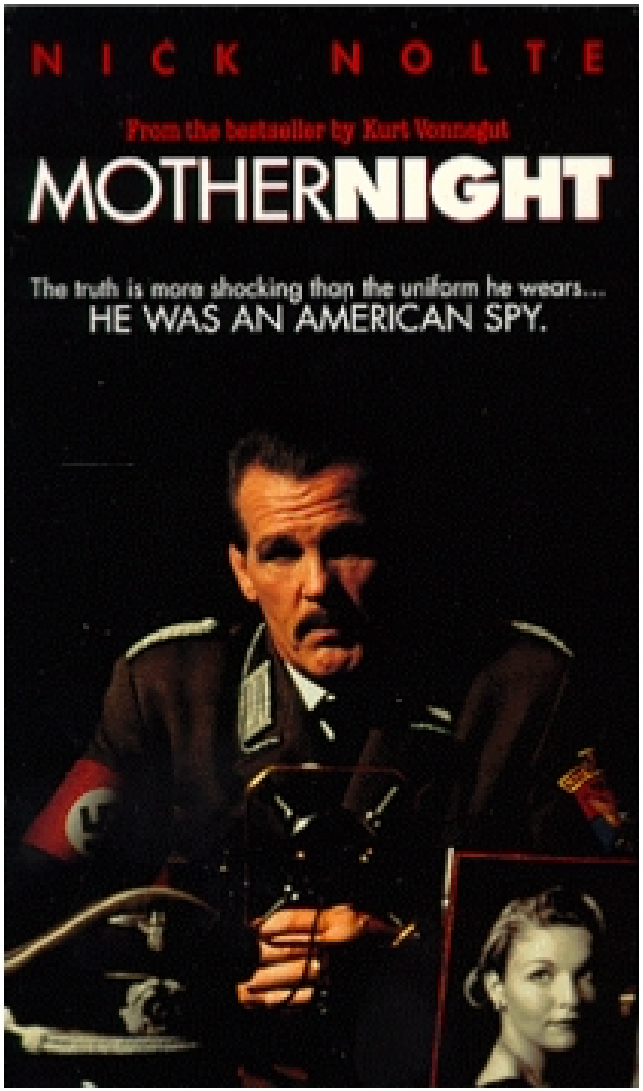
Pershing sails from NY June 1!

Investigators guide to steganography:

News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Newt is upset because he thinks he is President.

Mother Night



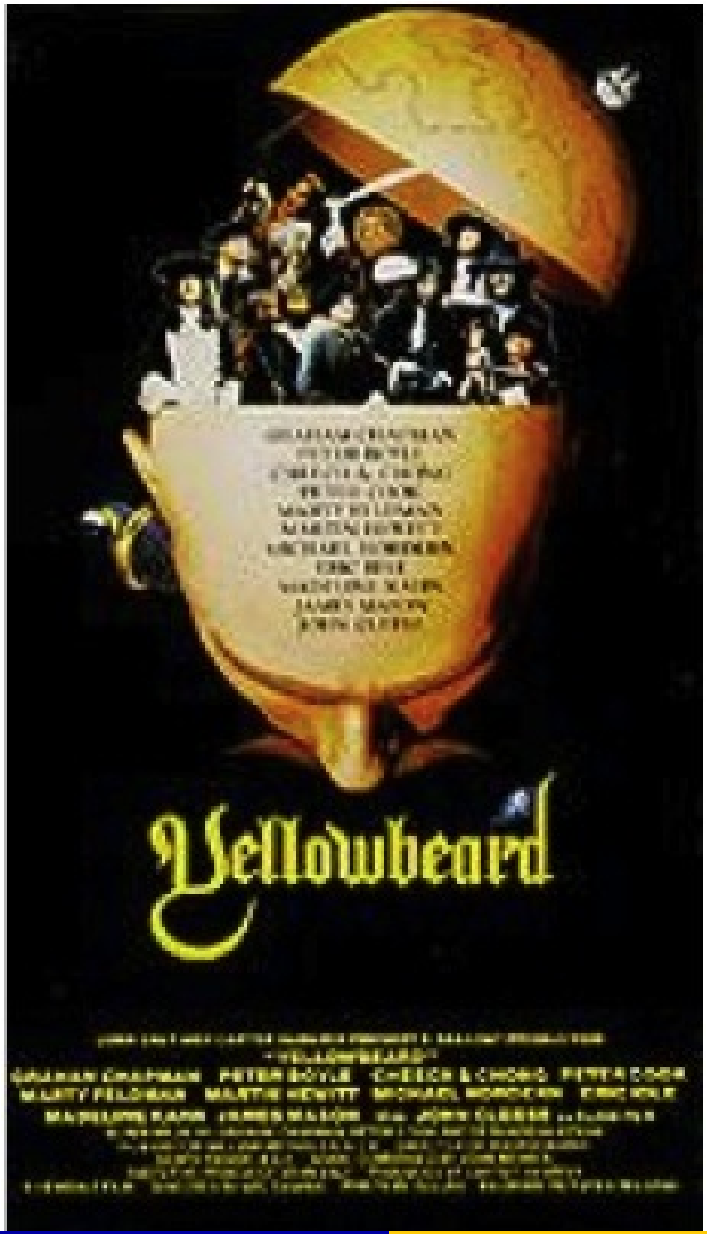
U.S. spy in Nazi Germany during WWII passes Secret messages in radio broadcasts.

Saint

Receives and sends encoded messages by email.

Example of the *Open Code* form of steganography.

Yellowbeard

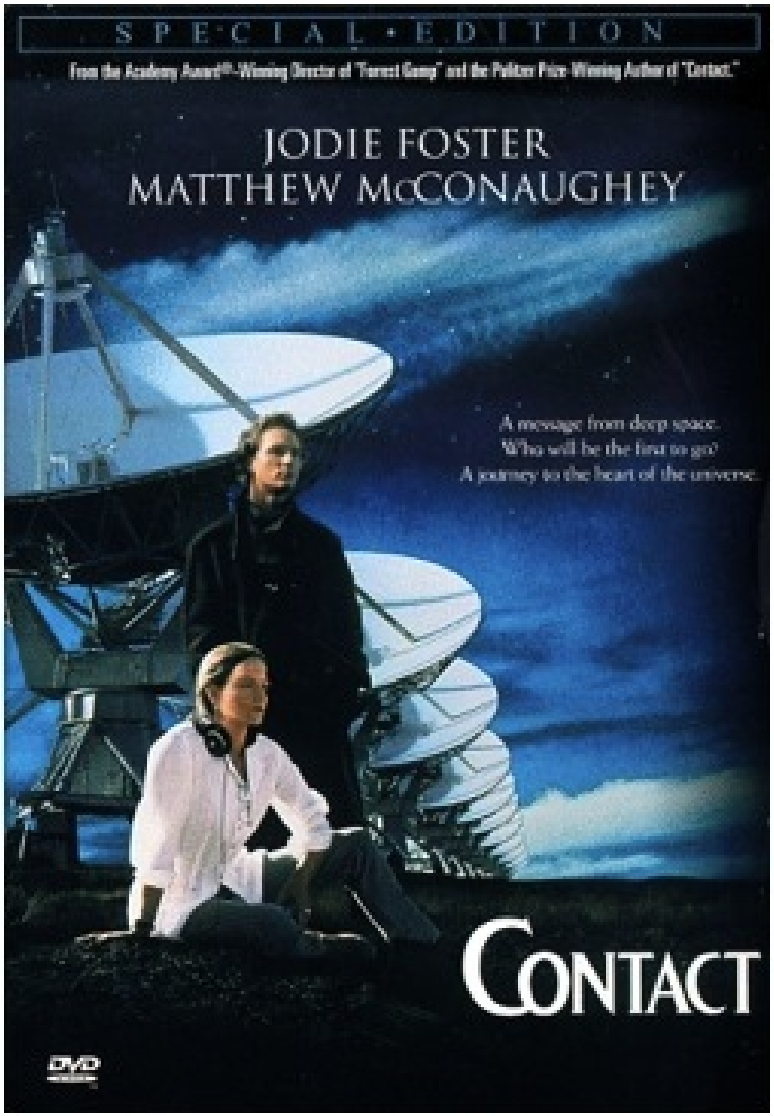


Yellowbeard's treasure map is tattooed on his son's head.

Independence Day

Aliens "hijack" satellite signals to embed a countdown sequence between spacecraft.
Example of Covert Channel.

Mother Night

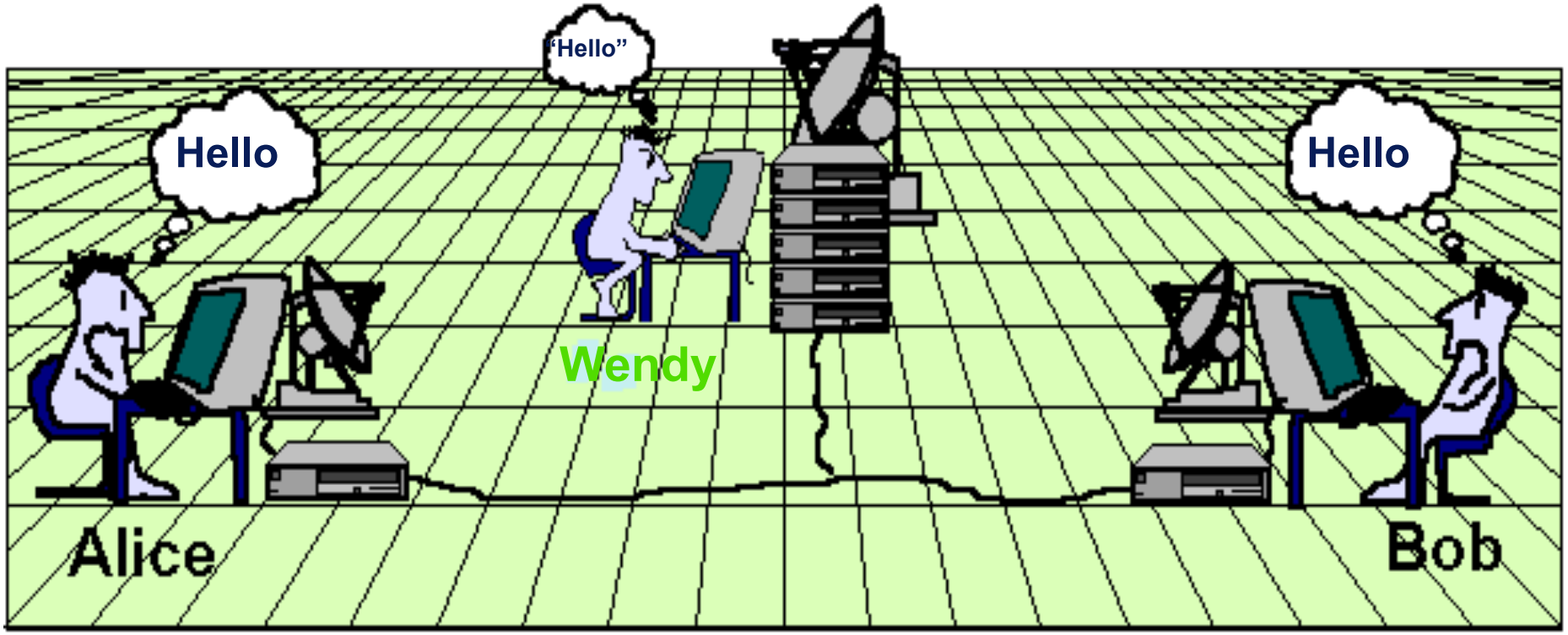


Television broadcast found embedded in a space signal sent to Earth.

Alien code found embedded within the frames of the television broadcast.

The primer to decode the alien message is embedded within the message. "Cracking" the code reveals blueprints to a machine.

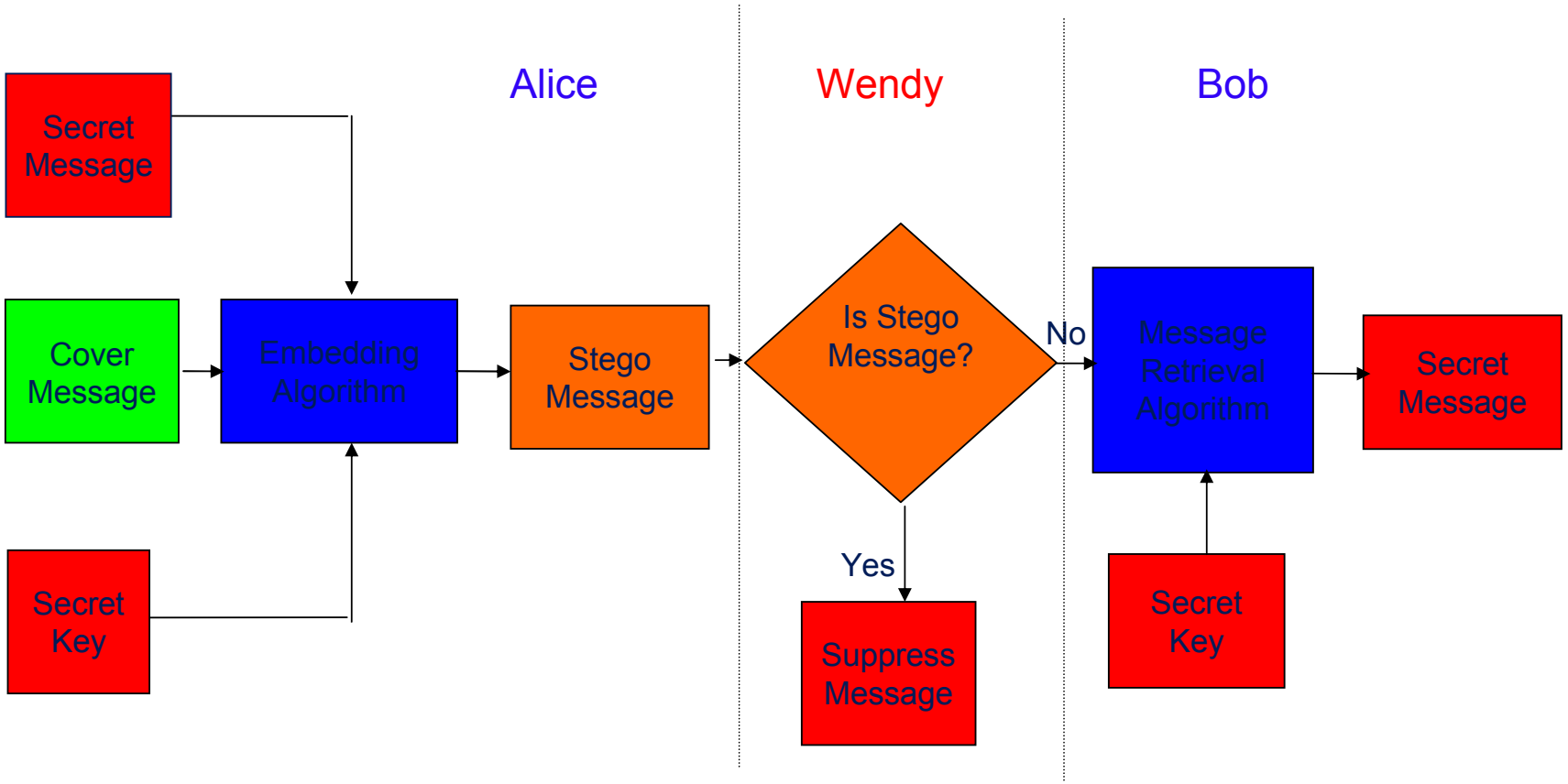
Modern Steganography



Simmons 1983

Done in the context of USA – USSR nuclear non-proliferation treaty compliance checking.

Modern Terminology and Simplified Framework



Secret Key Based Steganography

- If system depends on secrecy of algorithm and there is no key involved — *pure steganography*

  Note desirable. Kerkhoff's principle

- Secret Key based steganography
- Public/Private key based steganography

Active and Passive Warden Steganography

Wendy can be passive

- Examines all messages between Alice and Bob.
- Does not change any message.
- For Alice and Bob to communicate, Stego-object should be indistinguishable from cover-object.

Wendy can be active

- Deliberately modifies messages by a little to thwart any hidden communication.
- Steganography against active warden is difficult.
- Robust media watermarks provide a potential way for steganography in presence of active warden.

Lossy vs. Lossless Steganography

Lossless steganography: modify lossless compression methods.

- An example would be modifying run length encoding process to embed messages.
- During the encoding process the method checks all run lengths longer than one pixel.
- Suppose that a run length of ten pixels is considered and that one bit needs to be embedded.
- To embed a bit one the run length is split into two parts whose lengths add to ten, say nine and one; to embed a bit zero the run length is left unmodified.

Lossless Steganography: Decoding

- The receivers check all run lengths. Two run lengths of the same color are decoded as a one.
- A run length longer than one pixel, preceded and followed by run lengths of different colors, are decoded as a zero.
- Clearly, this technique relies on obscurity since detecting a file with information embedded by this technique is not hard.

Hiding in Images

Idea: hide by modifying least significant bits (LSBs) of pixels (raw uncompressed images)

$$10001111 \; 10001100 \; 10001011 \; 10010110 \ldots$$

- There are a lot of pixels in raw images
- Take an original image: rgb 410×614, 755k
- Convert to JPEG: 80% quality, 84k
- Insert the JPEG image into the original by replacing the LSBs by the bits of the JPEG file
- No noticable difference

Original/Uncompressed Image

80% JPEG Compression

JPEG Inserted into the Original Image

LSB Methods: The given "cover" is an image.

Image represented by pixel values

- Raw images: each pixel is a byte (gray value)
- Raw images: each pixel is a byte (color index in a palette)
- Raw images: each pixel is three bytes (r,g,b values)
- Image represented by a sequence of JPEG coefficients.
- LSBs of pixel values or JPEG coefficients can be altered freely.
- There are *many* LSBs in an image.
- Q: How many JPEG coefficients in an image
- A: As many as image pixels, but most are zeros and should not be changed; Only non-zero coefficients can be changed.

Embedding by Modifying Carrier Bits

- First approach identifies the carrier bits—i.e. the bits that will encode a message—and modifies them to encode the message.
- These carrier bits could be one or more LSBs of selected bytes of raster data—the selection process itself can use a key to select these bytes in pseudo-random order.
- Also, the raster data can be either raw image bytes (brightnesses and colors), or JPEG coefficients.
- Embedding is done by modifying the carrier bits suitably to encode the message.
- The message can be decoded from the carrier bits only—i.e., the receiver identifies the carrier bits and extracts the message using the key and the algorithm.

Comparing Steganography Steganography

These techniques can be compared using the following criteria (Westfeld, F5)

- The *embedding rate* – the number of embedded bits per a carrier bit.
- The *embedding efficiency* – the expected number of embedded message bits per modified carrier bit.
- The *change rate* – the average percentage of modified carrier bits.

Message Embedding

- Compare the carrier bits and the message bits and change the carrier bits to match the message:
- Changing the carrier bits to match the message bits.
- Using bit parity of bit blocks to encode message bits. Embed 1 bit per n carrier bits.
- Matrix encoding of message bits into carrier bits. Embed k bits using $n = 2^k - 1$ cover bits.

Changing the Carrier Bits to Match the Message Bits

- Bit flipping: $0 \longrightarrow 1$ or $1 \longrightarrow 0$.
- Subtracting 1 from the byte value.
- For example, let the raster data bytes be

$$01000111 \;\; 00111010 \;\; 10011000 \;\; 10101001,$$

- Using flipping to embed the message bits **0010** produces

$$01000110 \;\; 00111010 \;\; 10011001 \;\; 10101000,$$

- Using subtraction to embed the message bits **0010** produces

$$01000110 \;\; 00111010 \;\; 10010111 \;\; 10101000,$$

Matrix Encoding

- Embeds k message bits using n cover bits, where $n = 2^k - 1$.
  $k = 2,\ n = 3;\ k = 3,\ n = 7;\ k = 7,\ n = 127;\ \ldots$
- Embed a k-bit code word $\mathbf{x}$ into an n-bit cover block $\mathbf{a}$.
- Let the bits of $\mathbf{x}$ be $x_i,\ i = 1 \ldots k$ and let the bits of $\mathbf{a}$ be

  $a_j,\ j = 1 \ldots n$.
- Let f be *xor* of carrier bit indexes weighted by the bit values, i.e.

$$f(\mathbf{a}) = \bigoplus_{j=1}^{n} a_j \cdot j$$

and let

$$s = \mathbf{x} \oplus f(\mathbf{a}).$$

- A modified cover block $\mathbf{a}'$ is then computed as

$$\mathbf{a}' = \begin{cases} \mathbf{a}, & s = 0 \ (\Leftrightarrow \mathbf{x} = f(\mathbf{a})) \\ a_1 a_2 \ldots \neg a_s \ldots a_n, & s \neq 0 \end{cases}.$$

- On the *decoder side* a k-bit message block $\mathbf{x}$ is obtained from an n-bit carrier block $\mathbf{a}'$ by computing

$$\mathbf{x} = f(\mathbf{a}').$$

- As an example let $\mathbf{x} = 101$ and let $\mathbf{a} = 1001101$. Therefore,

$$\begin{aligned} f(1001101) &= 001 \oplus 100 \oplus 101 \oplus 111 = 111 \quad \rightarrow \\ s &= 101 \oplus 111 = 010 \quad \rightarrow \quad a' = 1101101, \end{aligned}$$

i.e., the second bit was flipped to obtain $f(\mathbf{a}') = f(1101101) = 101$.