LEAST SIGNIFICANT BIT EMBEDDINGS: IMPLEMENTATION AND DETECTION

Aaron Miller
Advisor: Mike Eckmann

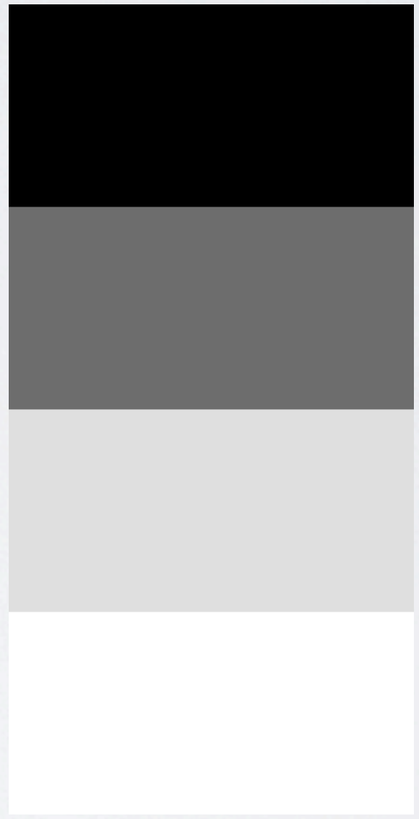
STEGANOGRAPHY

- Technique that hides a message into a digital object (cover) by making small changes so that the message's existence is difficult to detect

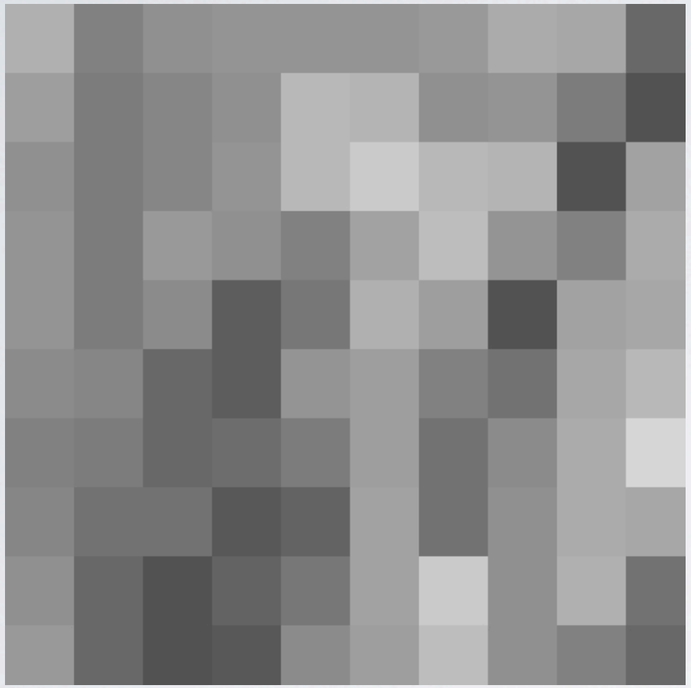
- Images, audio, text, video

GRAYSCALE VALUES

- $0_{10} \longrightarrow 00000000_2 \longrightarrow$ Black$\longrightarrow$
- $93_{10} \longrightarrow 01011101_2 \longrightarrow$ Dark Gray$\longrightarrow$
- $217_{10} \longrightarrow 11011001_2 \longrightarrow$ Light Gray$\longrightarrow$
- $255_{10} \longrightarrow 11111111_2 \longrightarrow$ White$\longrightarrow$



DIGITAL IMAGES

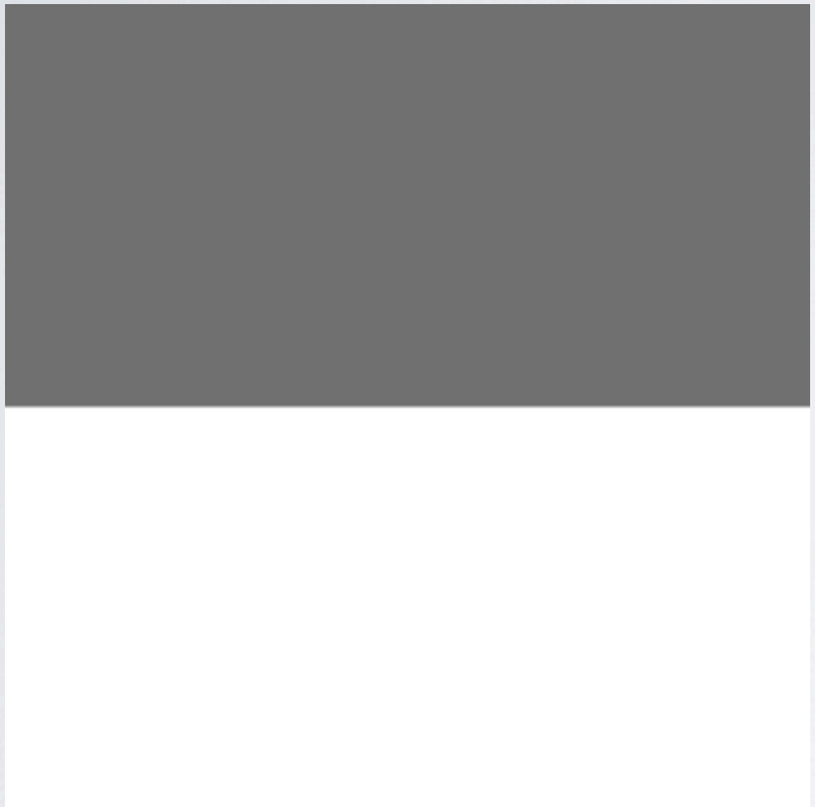


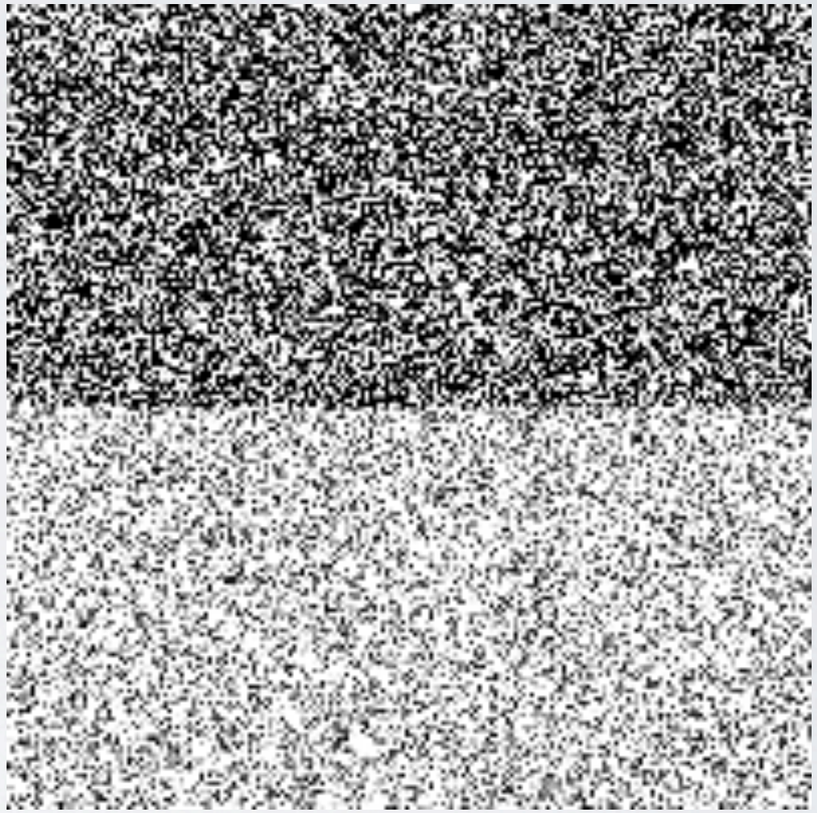
165	116	124	135	137	125	136	166	159	88
140	112	114	127	167	170	125	138	118	61
126	113	116	128	177	205	171	163	82	127
134	112	134	134	116	148	194	144	100	165
133	115	124	82	85	163	158	61	134	159
123	125	88	68	132	153	125	80	151	164
117	120	83	88	111	157	102	109	158	208
120	106	96	77	74	148	97	114	158	178
134	95	68	81	88	150	185	133	159	110
142	92	62	71	118	143	182	145	115	86

GRAYSCALE IMAGES

- Intensity
- 1 8-bit binary value for each pixel
- [00000000, 11111111]

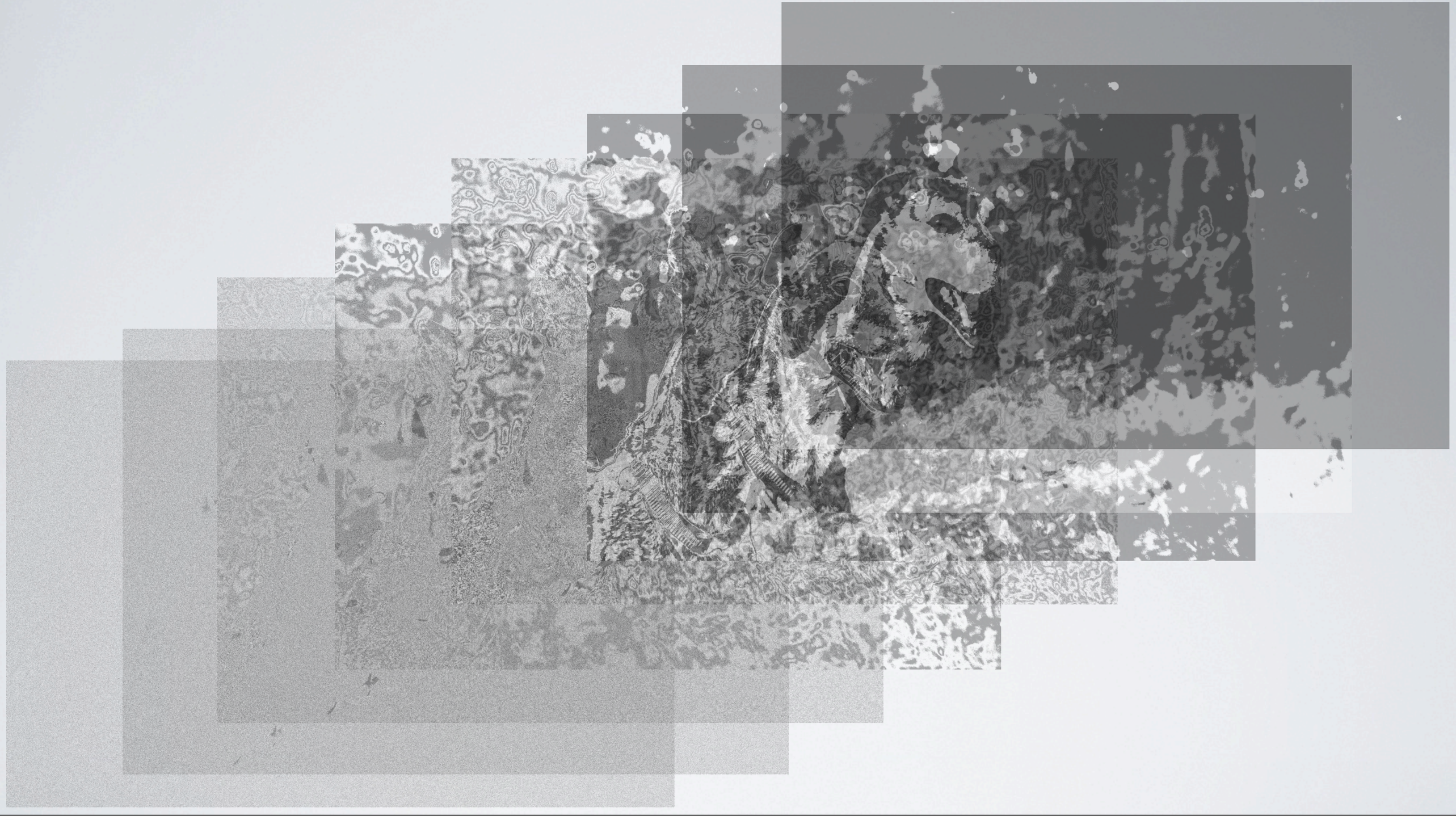
NOISE





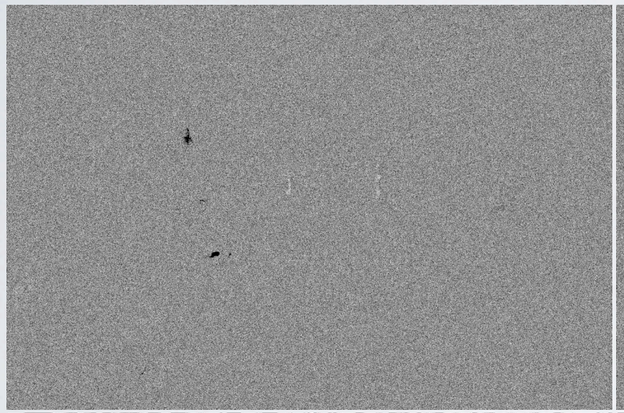
BIT PLANES

BIT PLANES

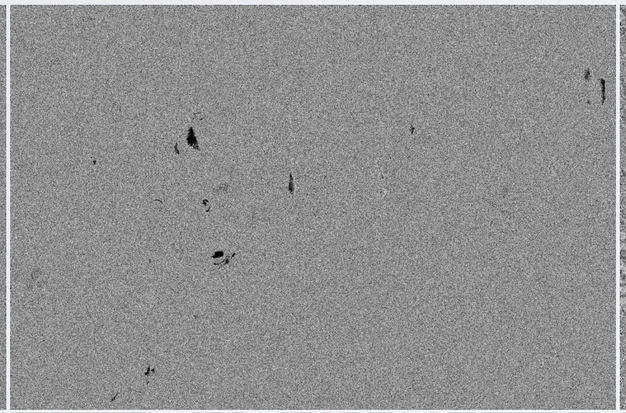


BIT PLANES

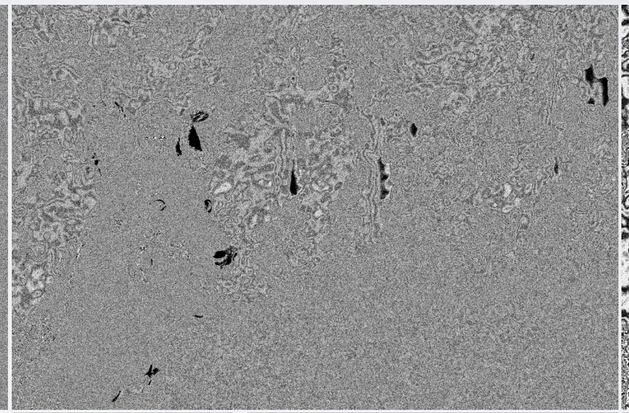
1



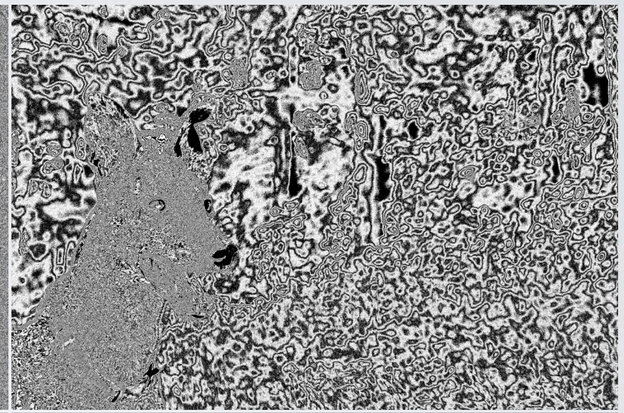
2



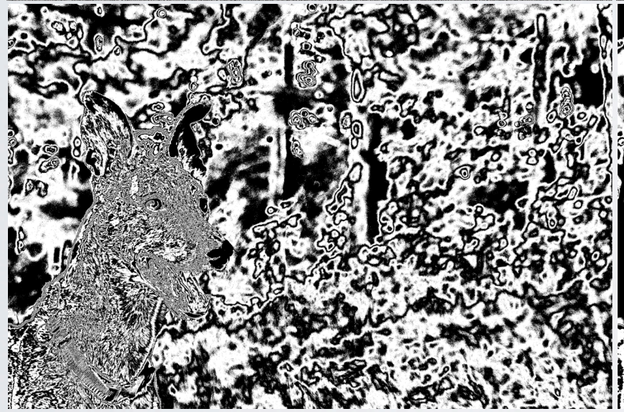
3



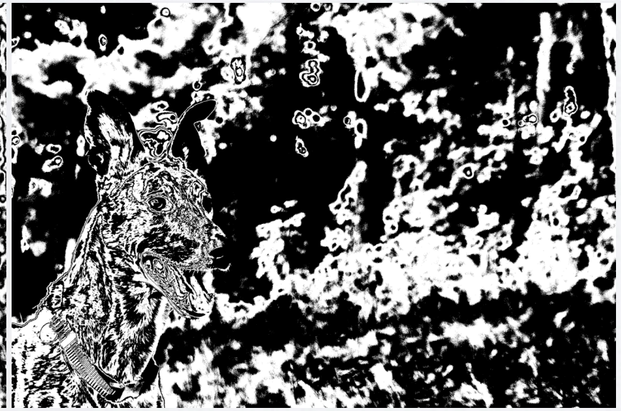
4



5



6



7

8

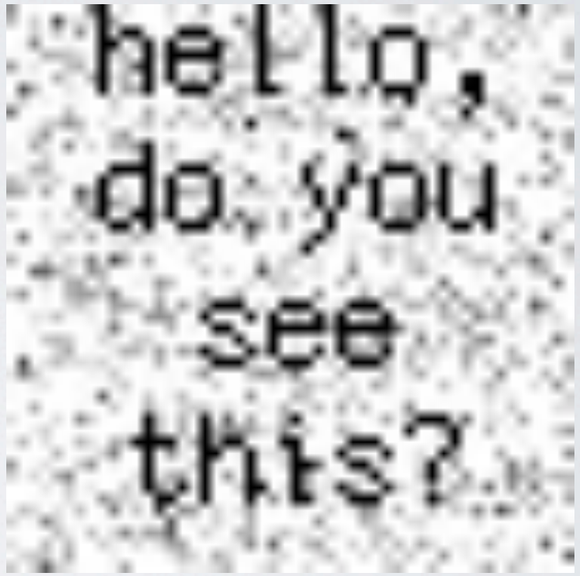
LSB EMBEDDING

- Overwrites the value of the least significant bit (LSB) of a pixel in a cover image
- Modification changes a pixel's intensity by 0 or 1

STEGANOGRAPHY: PARTS

- The Cover
  - Noise
  - Variation
  - Size

- The Message
  - Size
  - Representation
  - Lossless vs. Lossy

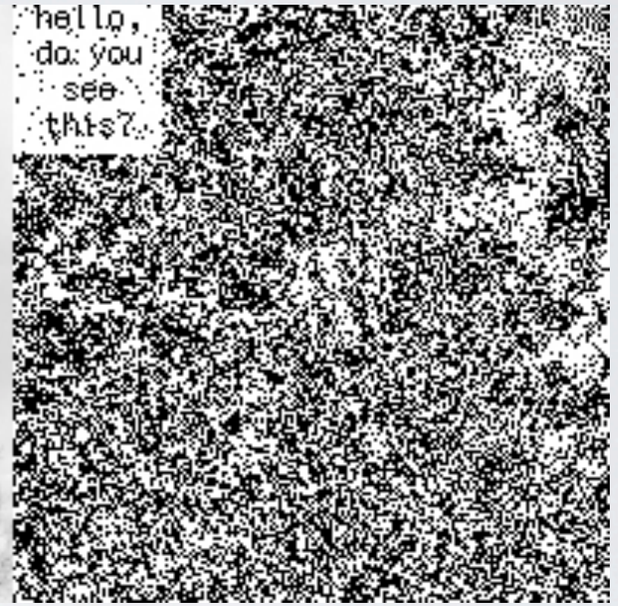


LSB EMBEDDING

- Hides message in the LSB of a cover
- Creates a stego object
- Resistant to detection
- Security Concern

HOW LSB STEGANOGRAPHY WORKS

- Cover: 10111011 (187)
- Message: 01110100 (116)
- Stego Object: 10111010 (186)

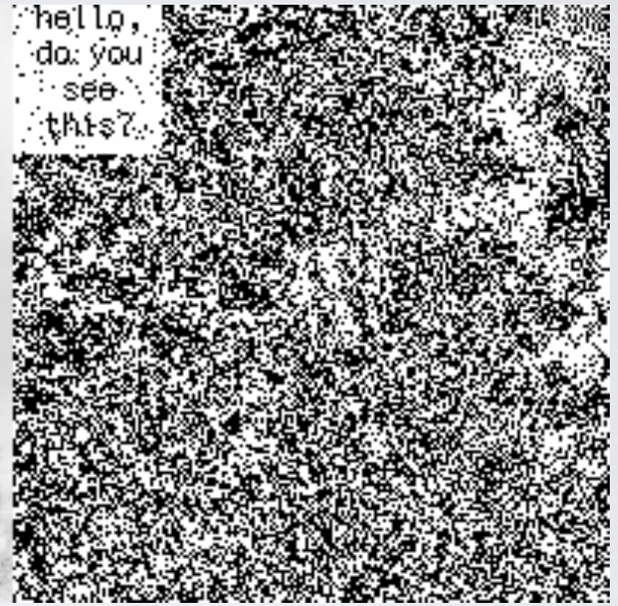


DETECTING LSB EMBEDDINGS

- Visual Attacks
- Statistical Attacks

VISUAL ATTACKS

- Simple
- Sequential Embeddings
- Observer



STATISTICAL ATTACKS

- Complex
- Targeted
- Exploit Image Characteristics

RS STEGANALYSIS

- Measures the noisiness of the LSBs before and after some flipping
- Uses the measurements to form a model
- Model predicts an embedded message length
- <0.5%

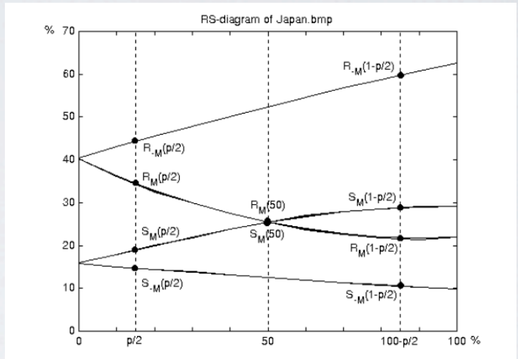


Figure 1. RS-diagram of a typical image. The *x*-axis is the relative number of pixels with flipped LSBs, the *y*-axis is the relative number of regular and singular groups with masks *M* and *–M*, *M*=[0 1 1 0]

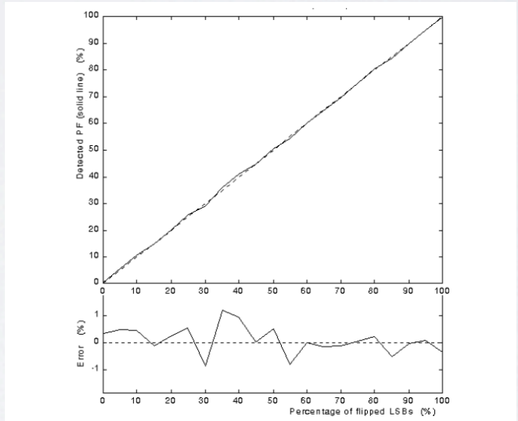


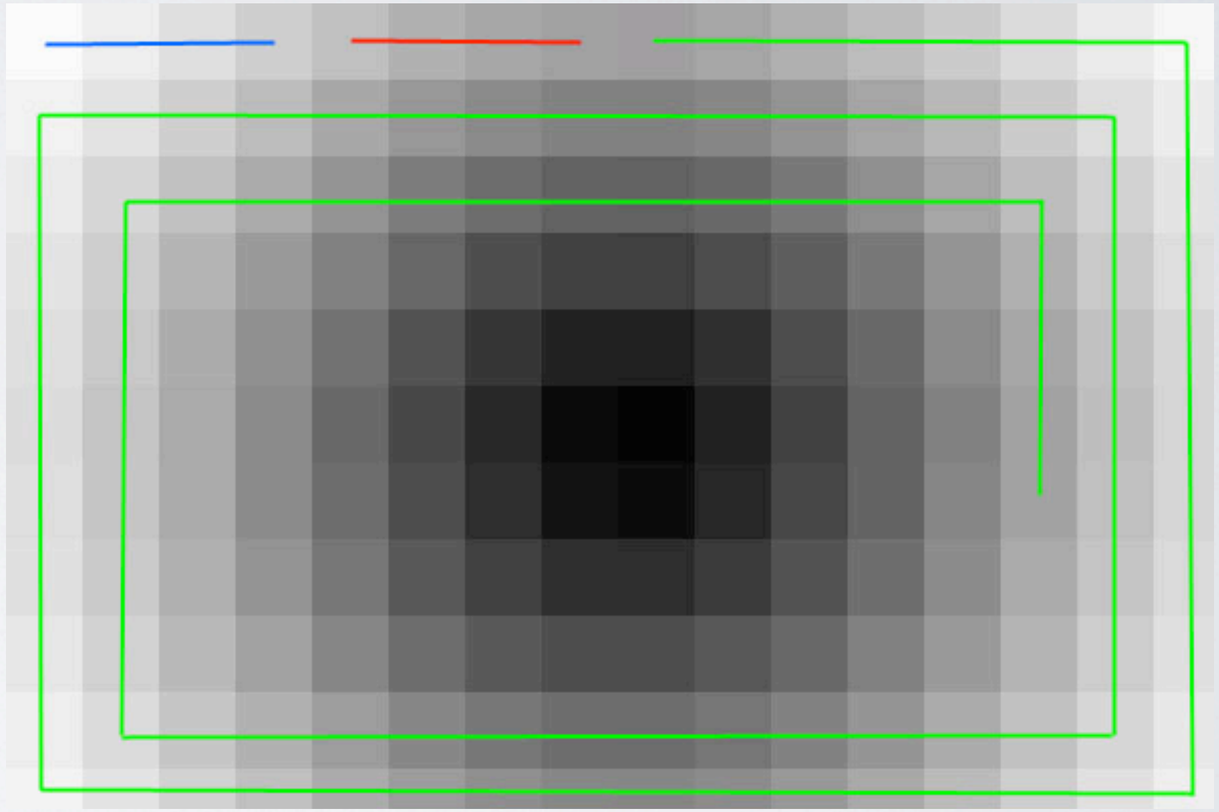
Figure 2. Estimated percentage of flipped pixels using the RS Steganalysis (solid line) vs. the actual number of flipped pixels for 'kyoto.bmp'. The bottom part of the figure shows the magnified detection error

SPIRAL LSB STEGANOGRAPHY

- How can we create an algorithm which:
  - Is not overly complex
  - Resists visual attacks
  - Distributes embedded pixels

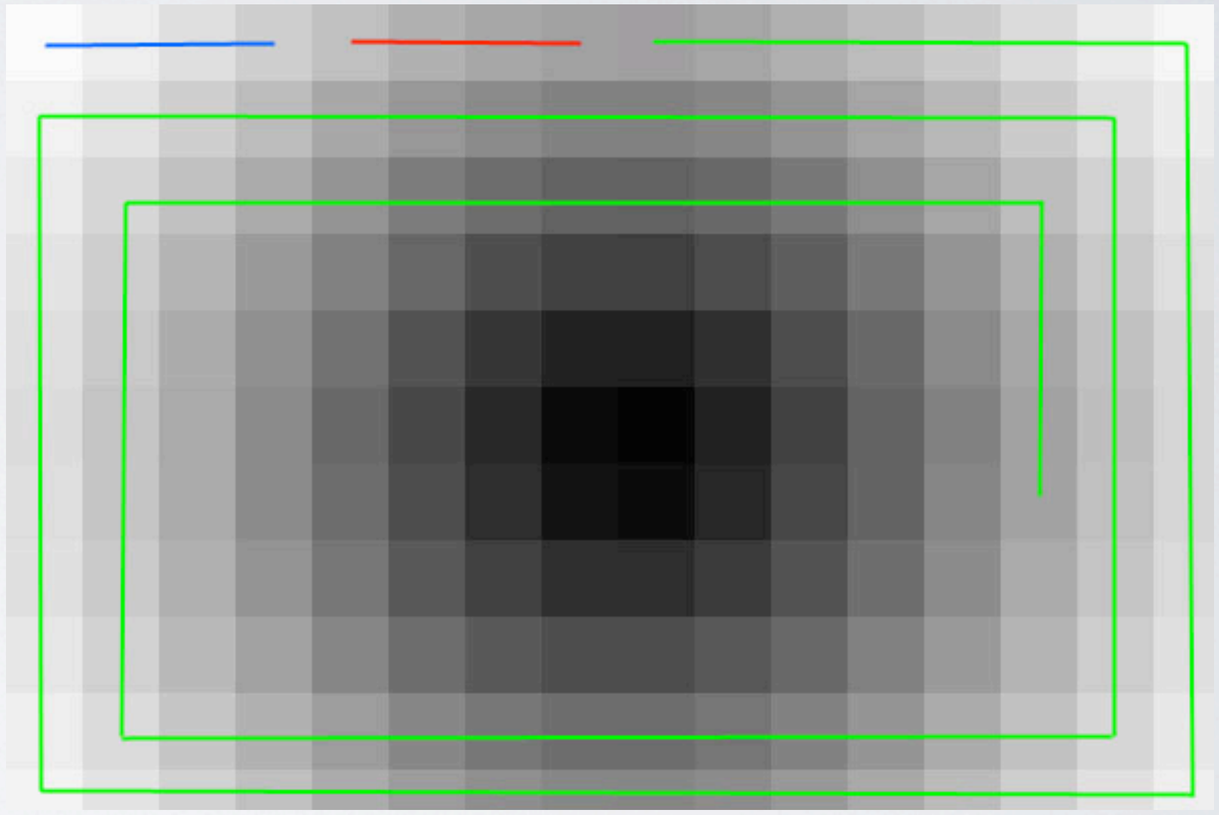
SPIRAL EMBEDDING

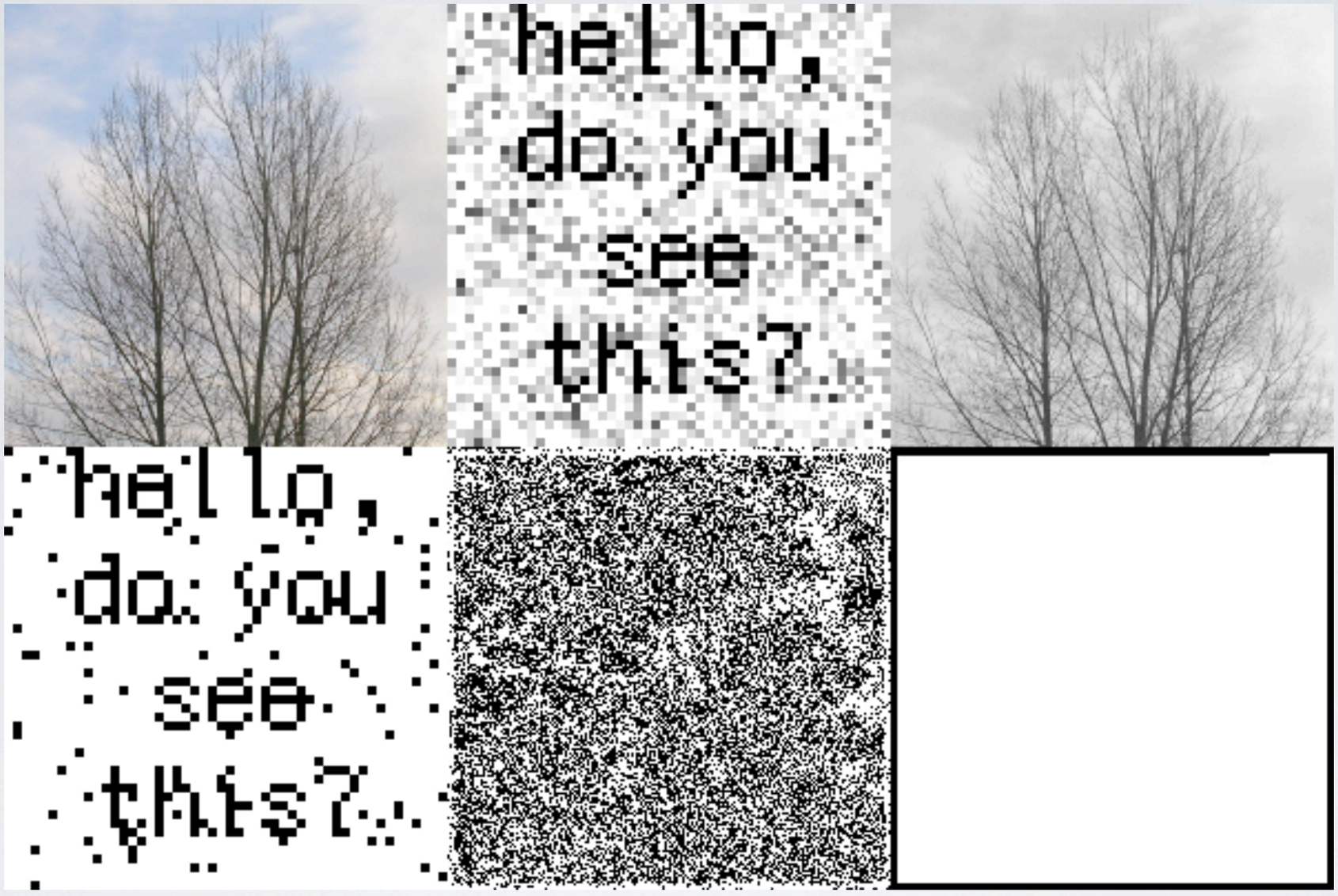
- Embed size of message in upper left corner
- Write serialized message values
- Spiral inward until entire message has been embedded



DECODING

- Reverse of embedding
- Unpack the dimensions of the message
- Continue until all message data has been read
- Construct the message





SPIRAL EMBEDDING RESULTS

DEMONSTRATION

CONCLUSION

- Steganography
- LSB Embeddings
- Visual & Statistical Attacks
- Spiral Embedding

REFERENCES

[1] Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color and grayscale images. Proceedings of the 2001 workshop on Multimedia and security new challenges - MM&Sec '01, 27. New York, New York, USA: ACM Press. doi:10.1145/1232454.1232466

[2] Lyu, S., & Farid, H. (2006). Steganalysis using higher-order image statistics. Forensics and Security, IEEE Transactions on, 1(1), 111-119.

[3] Gonzalez, Rafael C., and Paul A. Wintz. "Image Compression Standards." Digital Image Processing. 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002. 492-510. Print.

[4] Muñoz, A. (2007). XStegSecret beta v0.1. Retrieved from http://stegsecret.sourceforge.net/index.html

[5] Provos, N. (2001). Detecting steganographic content on the internet. Ann Arbor. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Detecting+Steganographic+Content+on+the+Internet#0

[6] Rocha, A., Scheirer, W., & Boult, T. (2011). Vision of the unseen: Current trends and challenges in digital image and video forensics. ACM Computing Surveys (. Retrieved from http://dl.acm.org/citation.cfm?id=1978805

[7] Węgrzyn, M. Virtual Steganographic Laboratory for Digital Images (VSL). Retrieved from http://vsl.sourceforge.net/

[8] Westfeld, A. (2001). F5 — A Steganographic Algorithm High Capacity Despite Better Steganalysis, 289-302.

[9] Westfeld, A., & Pfitzmann, A. (n.d.). Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos , and S-Tools — and Some Lessons Learned, 1-16.