Syllabus EECE 562

Data hiding history
- from ancient Greece to bits
- relationship between watermarking and steganography

Steganography
- basic concepts, definition, attributes, examples, stego tools available on the Internet

Steganographic security – theory
- basics of information theory
- Cachin's definition of steganographic security

Data hiding in raw (BMP) images
- color representation (RGB, YUV, HSV, transformations)
- LSB (least significant bit) embedding
- attacking LSB embedding (Sample Pairs Analysis)
- imaging sensors, signal processing in digital cameras
- data hiding by mimicking device noise (Stochastic Modulation)

Data hiding in palette (GIF) images
- palette formats (GIF)
- hiding by decreasing color depth, GIFshuffle, EzStego-like algorithms
- optimal palette parity assignment
- attack on EzStego-like algorithms (Pairs Analysis)

Data hiding in JPEG images
- the JPEG format
- the simplest JPEG data hiding algorithm – the J-Steg, attacking J-Steg
- improving J-Steg (OutGuess), attacking OutGuess
- F5 algorithm, matrix embedding, attacking F5
- modeling JPEG coefficients, parameter estimation
- model based steganography

Basics of block codes
- code length, minimal distance, covering radius
- sphere-covering bound, Singleton bound, Maximal Distance Separable codes (MDS)
- linear codes, generator matrix, parity-check matrix
- Reed Solomon codes
- codes for computer memory with defective cells

Wet paper codes
- random linear codes
- LT codes
- perturbed quantization

Matrix embedding
- Matrix embedding theorem
- binary Hamming codes, q-ary case
- random linear codes for large payloads

Universal blind steganalysis based on machine learning
- principles, approaches, ROC curves
- feature selection for the JPEG domain, calibration by recompression
- blind steganalyzer for JPEG format
- attacks using histogram characteristic function
- blind spatial domain steganalysis using higher order statistics
- blind steganalysis using resampling calibration

Textbook in preparation (will be available as a hard copy): J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications," Cambridge University Press, 400 pages, to appear later in 2008.

I. Cox, M. Miller, J. Bloome, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," revised 2nd edition, Morgan Kaufmann, to appear in 2006. Contains two chapters on steganography and steganalysis.

Other books on data hiding
Michael Arnold, et al., "Techniques and Applications of Digital Watermarking and Content Protection," 2003. Does not contain steganography.

Mauro Barni, Franco Bartolini, "Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications (Signal Processing and Communications, 21)," 2004 (expensive, $169, does not contain steganography).

Peter Wayner, "Disappearing Cryptography, Second Edition – Information Hiding: Steganography and Watermarking," The Morgan Kaufmann Series in Software Engineering and Programming, 2002. Does not have most of the material in this course.

Juergen Seitz, "Digital Watermarking for Digital Media," 2005. Edited book, does not contain steganography/steganalysis.

Chun-Shien Lu, "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property," 2004.

Joachim Eggers, Bernd Girod, "Informed Watermarking (The International Series in Engineering and Computer Science)," 2002. Focus on theoretical aspects of robust watermarking.

Fernando Perez-Gonzalez (Editor), Sviatoslav Voloshynovskiy, "Fundamentals of Digital Image Watermarking," Dec 2005 (does not contain steganography)

Eric Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication," 2003, narrative, non-technical.

Karen Bailey & Kevin Curran, "Steganography," June 2005. I do not know this book, but judging from its cost of $13.99 (paperback), it will probably have little technical material.

N. Johnson, Z. Duric, S. Jajodia, "Information Hiding, Steganography and Watermarking – Attacks and Countermeasures," Kluwer Academic Publishers, 2001. Collection of a few outdated papers, contains only a small fraction of what we will be talking about. Expensive.

A. Hanjalic, G.C. Langelaar, P.M.B. van Roosmalen, J. Biemond, R.L. Lagendijk, "Image and Video Databases: Restoration, Watermarking and Retrieval (Advances in Image Communication)," Elsevier Science, 2000. Does not contain steganography, steganalysis.

Wenjun Zeng, Heather Yu, and Ching-Yung Lin (editors), "Multimedia Security Technologies for Digital Rights management," to appear soon. Contains a chapter on Steganography and steganalysis written by me.

Image processing
R.C. Gonzales and R.E. Woods, "Digital Image Processing," Prentice Hall, 2002. This is a very readable text on image processing on a graduate level. This book was also used here in the Watson School for a CS course on image processing

Basics of linear codes
Dominic Welsh, "Codes and Cryptography," Clarendon Press, Oxford, 1988. Excellent undergraduate level book requiring only basics of calculus and probability.

Steganography and steganalysis
Stefan Katzenbeisser and Fabien Petitcolas, "Information Hiding, Techniques for Steganography and Digital Watermarking," Artech House, 2000. Edited book, wider span than the previous book, outdated. It only contains a small portion of what we will be talking about.

Statistics
E.R. Dougherty, "Random Processes for Image and Signal Processing," SPIE PRESS Monograph Vol. PM44, 1998.

Policies:

Academic Honesty All students must adhere to the Student Academic Honesty Code of the University and the Watson School. The Department of Electrical and Computer Engineering has adopted a standard policy to enforce these codes for violations involving course work. Category I violations result in a grade of 0 for the graded work plus a one letter course grade reduction. A *Report of Category I Academic Dishonesty* form is filed with the Provost's Office; if a prior report is already on file, the offense is automatically elevated to Category II. Category II violations result in at least a failing grade for the course plus any additional penalties determined by the Watson Academic Integrity Committee.

University Academic Honesty Code:
http://bulletin.binghamton.edu/program.asp?program_id=826
Watson School Academic Honesty Code:
http://www.binghamton.edu/watson/Watson_Academic_Honesty_Policy.pdf
ECE Department Academic Honesty Code Enforcement Policy
http://www.ece.binghamton.edu/documents/Academic_Honesty_Policy.pdf

This course is also offered under the articulation agreement between Binghamton University and SUNYIT. It is available to qualified students at Binghamton University via the distance learning system Enginet.