Exam questions

2020

Multimedia Security and Privacy

Digital watermarking

1. Explain the difference in the usage of and requirements to digital robust watermarking, steganography and tamper proofing.
2. Explain the difference between the watermarking and data hiding. Explain when each technology can be used.
3. Explain the watermark detection problem. Explain the difference between the Neyman-Pearson and Bayesian hypothesis testing. Explain the errors.
4. Explain which parameters of image and watermark influence the distributions of sufficient statistics under different hypothesis and error probabilities.
5. Explain the main classes of attacks against robust watermarking.

Content fingerprinting

1. Explain the main differences between content fingerprinting (robust perceptual hashing) and cryptographic hashing.
2. Explain the usage of content fingerprinting in various applications. What are the main advantages?
3. Explain the construction of content fingerprinting function based on random projections and binarization.
4. Explain the statistics of coefficients under random projections used in content fingerprinting. Properties.
5. Explain which distribution of bits in content fingerprinting is of preference for practice. Why? How to achieve it?
6. Explain the difference between the sufficient statistics in digital watermarking (linear cross-correlation) and Hamming distance? What are the consequence of these differences?
7. Explain the usage of content fingerprinting for fast indexing and identification. Explain the direct search and searches based on knowledge of bit errors in fingerprints.

Privacy protection

1. Explain authentication and identification from the signal processing point of view. What are the main concerns behind this approach?
2. Explain privacy protection based on fuzzy commitment scheme. Advantages and drawbacks.
3. Explain privacy protection based on helper data scheme. Advantages and drawbacks.