SESSION 2: BASIC TECHNIQUES

- Encoders and Decoders
- Least Significant Bit (LSB) Methods
- Spread-Spectrum Modulation (SSM)
Encoders & Decoders

- An encoder is a function \( x = f(s, m, k) \) where
  - \( x \in X^N = \text{watermarked signal} \);
  - \( s \in S^N = \text{host signal} \);
  - \( m \in M = \text{message} \);
  - \( k \in K^N = \text{cryptographic key} \).

- For 1-bit watermarking, \( M = \{0, 1\} \).

- For data hiding, cardinality \( |M| \) is large, typically exponential in \( N \), the length of sequence \( s \)
  \[ R = \frac{1}{N} \log_2 |M| \] bits of hidden information per sample
A decoder is a function $\hat{m} = g(y, k)$ where

- $y \in Y^N$ is the received (attacked) signal;
- $k \in K^N$ is the cryptographic key shared with the encoder;
- $\hat{m} \in M$ is the decoded message.
Least Significant Bit (LSB) Methods

- Host sequence $s = \{s_1, s_2, \cdots, s_n\}$
- Each $s_i \in \{0, 1, \cdots, 2^b - 1\}$ ($b$ bits/sample)

$$77 = (01001101)$$

- Replace all $n$ LSB’s by hidden binary message
  $\Rightarrow R = 1$ bit/sample
- Popular steganographic method
- Highly vulnerable to noise!
Spread-Spectrum Modulation

- Attacker does not known secret pattern \( p \)
- Typically \( p = \) pseudo-random noise (PRN) sequence
- \( k = \) seed to PRN generator
Attacker’s signal is usually additive and independent of $x$. 
Decoder

• Define test statistics

\[ t(y, m, k), \quad m \in \mathcal{M} \]

and find \( m \) that maximizes \( t(y, m, k) \).

• Example #1: likelihood ratio test statistics

\[ t(y, m, k) = \frac{p(y, k|m)}{p(y, k|0)} \]

can be implemented only if attack channel is known.
• Example #2: correlation statistics

\[ t(y, m, k) = y \cdot p(m, k), \quad m \in \mathcal{M} \]

(common choice for blind SSM systems)

• Example #3: centered correlation statistics:

\[ t(y, m, k) = (y - s) \cdot p(m, k), \quad m \in \mathcal{M} \]

(common choice for nonblind SSM systems)

• Ideal in \( P_e \) sense if noise at decoder is white and Gaussian
Refinements

• Make watermark strength parameter $\alpha$ dependent on local characteristics of $s$

• Use test statistic better adapted to statistics of degradation process

• Still, detection performance is dominated by host-signal interference for blind SSM systems