SESSION 1: 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
  - $x \in \mathcal{X}$ = watermarked signal;
  - $s \in \mathcal{S}$ = host signal;
  - $m \in \mathcal{M}$ = message;
  - $k \in \mathcal{K}$ = cryptographic key.
- In the following examples, $\mathcal{M}$ is a binary sequence.
- For 1-bit watermarking, $\mathcal{M} = \{0, 1\}$.
- For data hiding, cardinality $|\mathcal{M}|$ is large, typically exponential in length of sequence s
  $\Rightarrow R$ bits of hidden information per sample of host signal

Decoder

A decoder is a function $\hat{m} = g(y, k)$ where

- y is the received (attacked) signal;
- k is the cryptographic key shared with the encoder.
- $\hat{m} \in \mathcal{M}$ is the decoded message

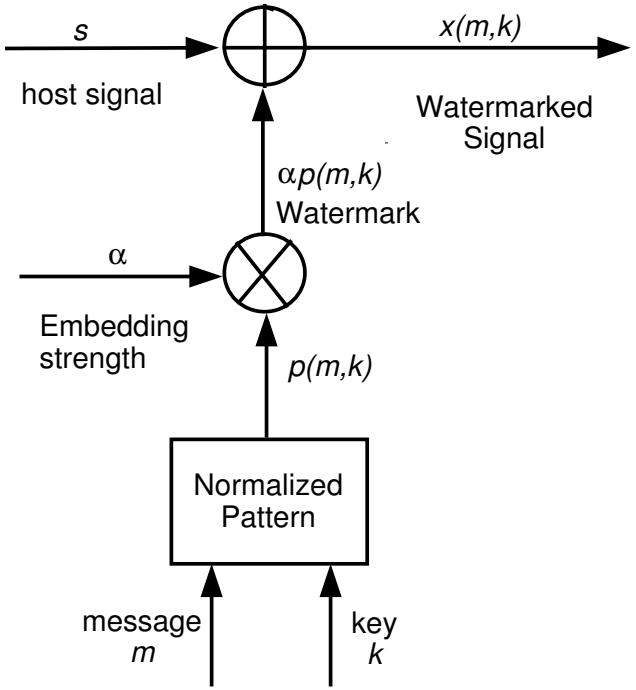
Least Significant Bit (LSB) Methods

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

$$77 = (01001101)$$

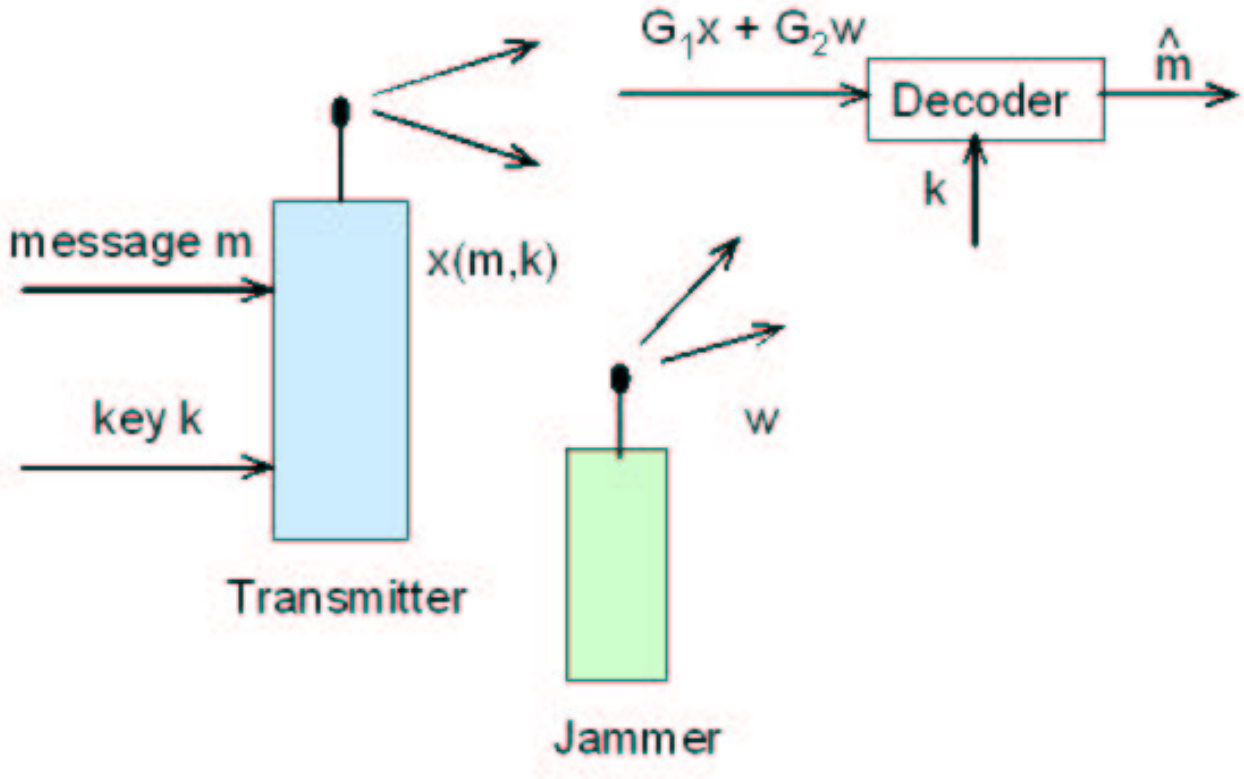
- Replace all n LSB's by hidden binary message
  $\Rightarrow R = 1$ bit/sample
- Popular steganographic method
- Highly vulnerable to noise!

Spread-Spectrum Modulation



- Attacker does not known secret pattern p
- Typically p = pseudo-random noise (PRN) sequence
- k = seed to PRN generator

Motivation: Jamming Problem

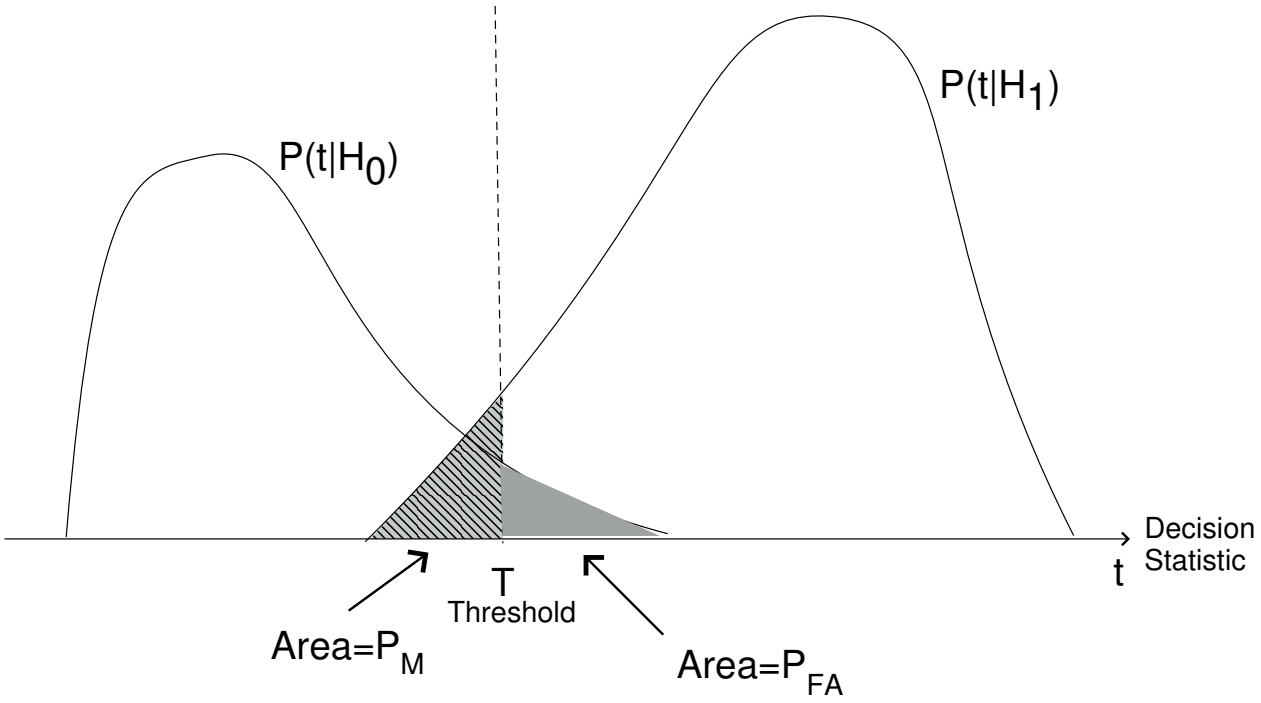


Attacker's signal w is usually additive and independent of x

Decoder

- First consider $m \in \{0, 1\}$, with $p(0, k) = 0$
- Define two hypotheses $\begin{cases} H_0 & : \ m = 0 \\ H_1 & : \ m = 1 \end{cases}$
- Decoder often takes the form $t \underset{H_0}{\overset{H_1}{\gtrless}} T$, where

  $t = t(y, k) =$ *test statistic*, and $T =$ *threshold* of the test.



$$\text{Test: } t \underset{<}{\overset{>}{}} T \quad \begin{matrix} H_1 \\ \\ H_0 \end{matrix}$$

- Common choice for blind SSM systems:

$$t(y,k) = < y,\, p(1,k) > \quad = \text{ correlation statistic}$$

- Use $t(y,k) = < y - s,\, p(1,k) >$ for private SSM systems
- Ideal in P_e sense if noise at decoder is white and Gaussian
- If $|\mathcal{M}| > 2$, then define $|\mathcal{M}|$ correlation statistics

$$t(y,m,k) = < y, p(m,k) >, \quad m \in \mathcal{M}$$

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

Refinements

- Make watermark strength parameter α 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