

## 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
  - $x \in \mathcal{X}$  = 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

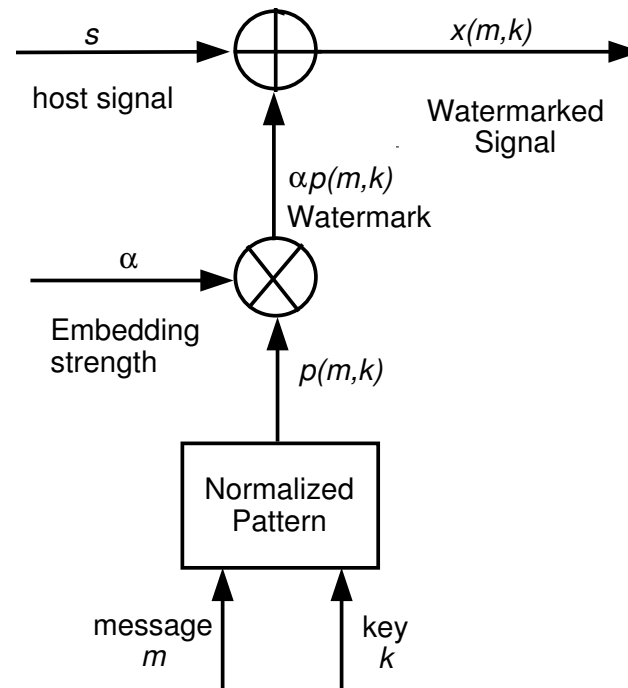
## Least Significant Bit (LSB) Methods

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

$$77 = (0100110\mathbf{1})$$

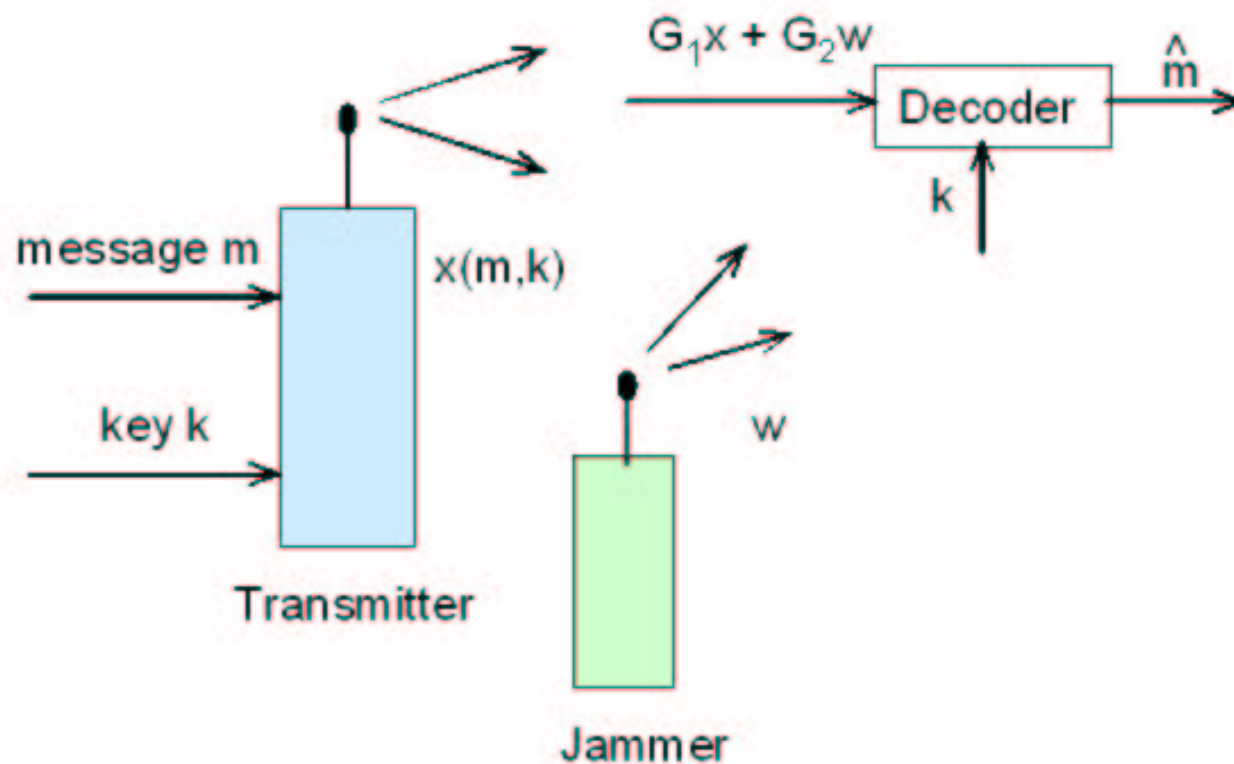
- Replace all  $n$  LSB's by hidden binary message  
 $\Rightarrow R = 1$  bit/sample
- Popular steganographic method
- Highly vulnerable to noise!

# Spread-Spectrum Modulation



- Attacker does not know 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  $x$

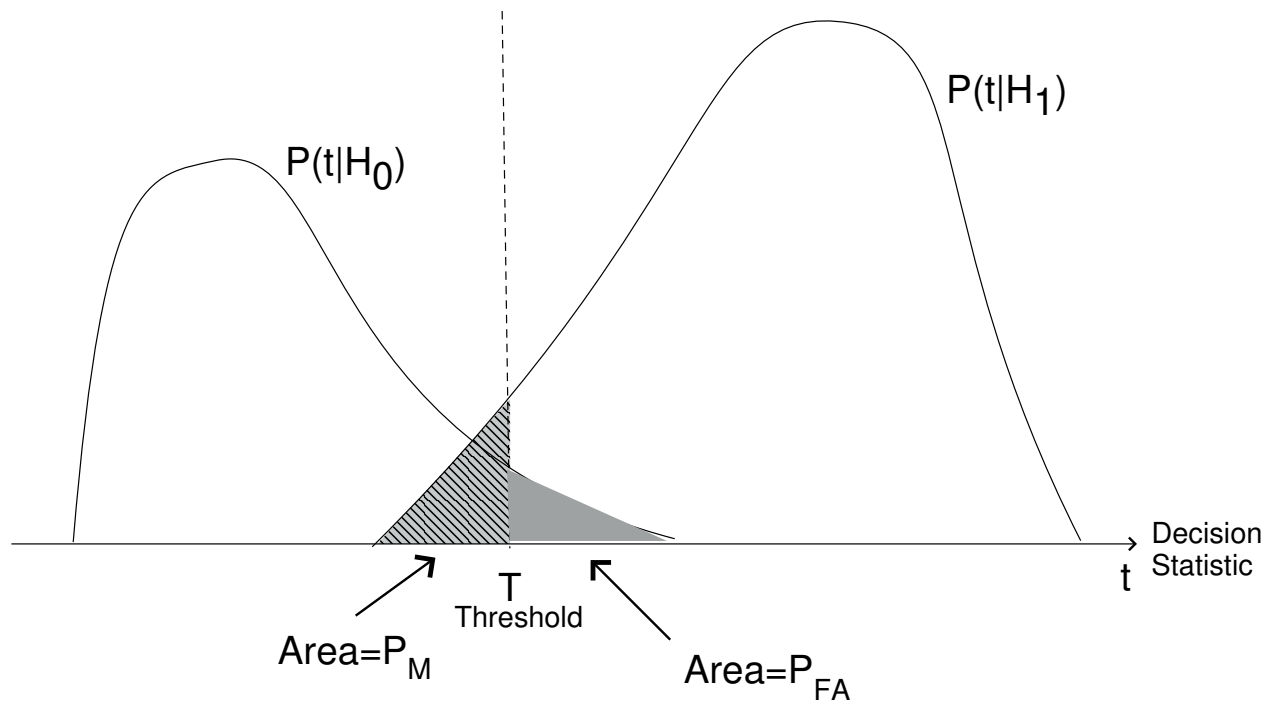
## Decoder

- 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  $t \begin{matrix} > \\ < \end{matrix} T$ , where

$t = t(y, k) = \text{test statistic}$ , and  $T = \text{threshold}$  of the test.



$$\begin{array}{c}
 H_1 \\
 \text{Test: } t > T \\
 < \\
 H_0
 \end{array}$$

- Common choice for blind SSM systems:

$$t(y, k) = \langle y, p(1, k) \rangle = \text{correlation statistic}$$

- Use  $t(y, k) = \langle y - s, p(1, k) \rangle$  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

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

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

## 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