

## SESSION 2: BASIC TECHNIQUES

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

## Encoders & Decoders

- An encoder is a function  $\mathbf{x} = f(\mathbf{s}, m, \mathbf{k})$  where
  - $\mathbf{x} \in \mathcal{X}^N =$  watermarked signal;
  - $\mathbf{s} \in \mathcal{S}^N =$  host signal;
  - $m \in \mathcal{M} =$  message;
  - $\mathbf{k} \in \mathcal{K}^N =$  cryptographic key.
- For 1-bit watermarking,  $\mathcal{M} = \{0, 1\}$ .
- For data hiding, cardinality  $|\mathcal{M}|$  is large, typically exponential in  $N$ , the length of sequence  $\mathbf{s}$   
 $\Rightarrow R = \frac{1}{N} \log_2 |\mathcal{M}|$  bits of hidden information per sample

## Decoder

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

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

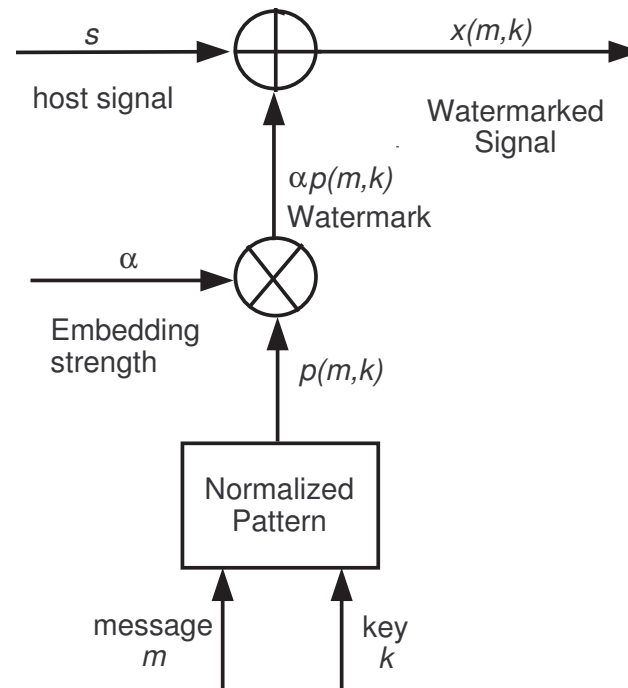
## Least Significant Bit (LSB) Methods

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

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

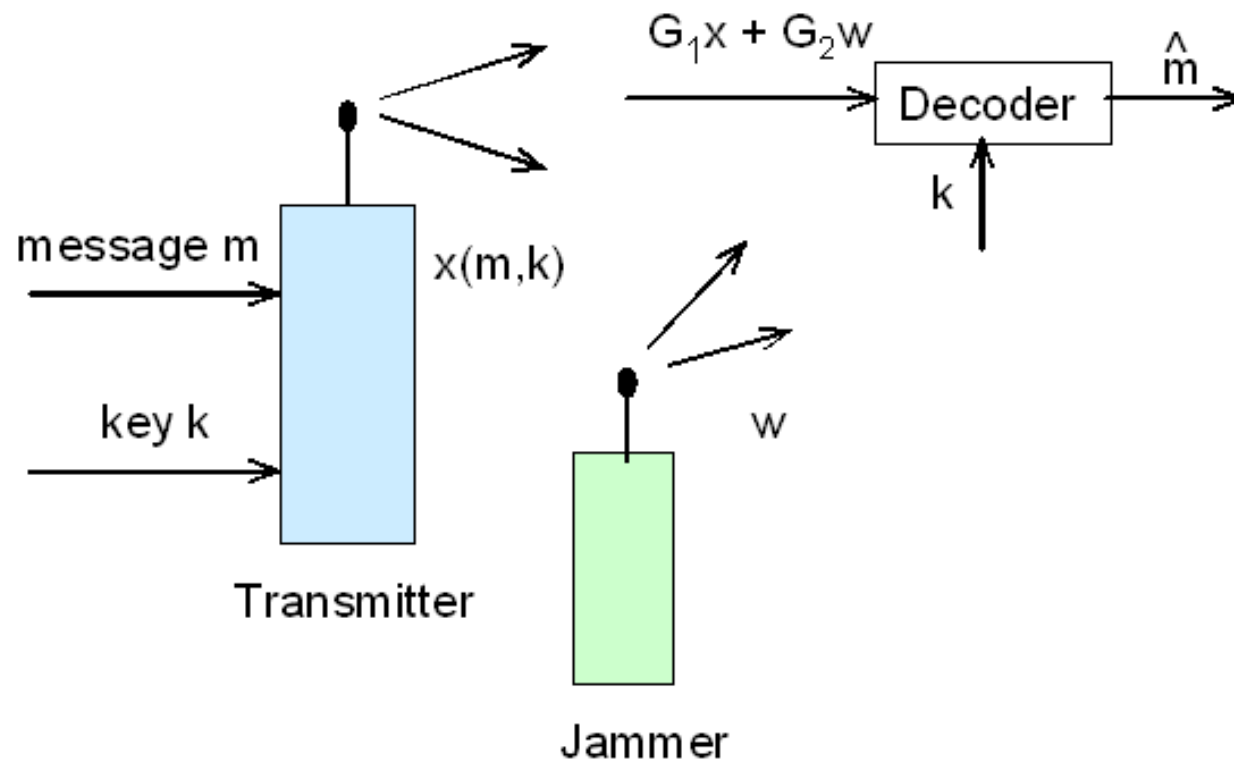
- Replace all  $n$  LSB's by hidden binary message  
 $\Rightarrow R = 1$  bit/sample
- Popular steganographic method
- Highly vulnerable to noise!

# Spread-Spectrum Modulation



- Attacker does not know secret pattern  $\mathbf{p}$
- Typically  $\mathbf{p}$  = pseudo-random noise (PRN) sequence
- $\mathbf{k}$  = seed to PRN generator

## Motivation: Jamming Problem



Attacker's signal is usually additive and independent of  $\mathbf{x}$

# Decoder

- Define test statistics

$$t(\mathbf{y}, m, \mathbf{k}), \quad m \in \mathcal{M}$$

and find  $m$  that maximizes  $t(\mathbf{y}, m, \mathbf{k})$ .

- Example #1: likelihood ratio test statistics

$$t(\mathbf{y}, m, \mathbf{k}) = \frac{p(\mathbf{y}, \mathbf{k}|m)}{p(\mathbf{y}, \mathbf{k}|0)}$$

can be implemented only if attack channel is known

- Example #2: correlation statistics

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

(common choice for blind SSM systems)

- Example #3: centered correlation statistics:

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

(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  $\mathbf{s}$
- Use test statistic better adapted to statistics of degradation process
- Still, **detection performance is dominated by host-signal interference** for blind SSM systems