COMP40600: Multimedia Security

Individual Assignment

James Dorrian (UCD: 13369451)

April 29, 2017

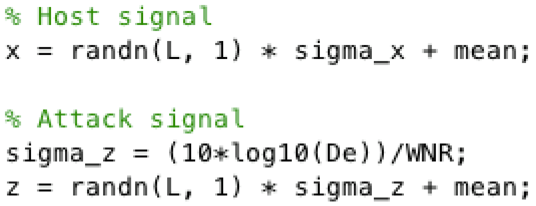
Table of Contents

1 Third Assignment: Non-side-informed Methods

In class, we studied non-side-informed data hiding methods which represent the method that did not exploit a priori knowledge about of the host signal pdf.

1.1 DSSS with known spreading sequence

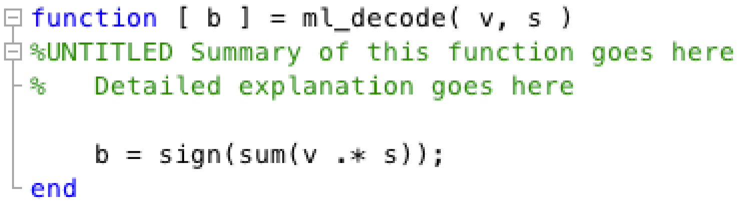
The first step was to solve the equation for HWR given by $\text{HWR}(\text{dB}) = 10\log_{10}\sigma_X^2/D_E$,. I decided to do this using a value of 10 for sigma of X, due to the fact that it solved as an integer value (which equates to 1). After using this result to calculate gamma the next step was to generate a host signal using the values calculated above and attack signal given by $\text{WNR}(\text{dB}) = 10\log_{10} D_E/\sigma_Z^2$.



```
% Host signal
x = randn(L, 1) * sigma_x + mean;

% Attack signal
sigma_z = (10*log10(De))/WNR;
z = randn(L, 1) * sigma_z + mean;
```

After generating the uniform binary symbol b and pseudorandom vector s, I obtained the watermarked vector by adding the vector generated by the equation $w[i] = b \cdot s[i] \cdot \gamma$ for all $i = 1, \cdots, L$ to the host signal. The attacked watermark vector was then obtained by adding the attack signal to the previously obtained watermarked vector. Finally, I created a function to apply the ML decoder in order to retreive $\hat{b}$ from attacked watermark vector.

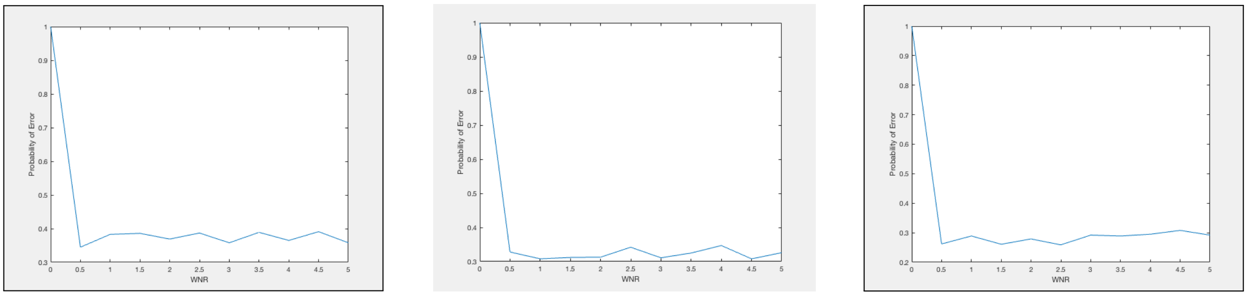


```
function [ b ] = ml_decode( v, s )
%UNTITLED Summary of this function goes here
%   Detailed explanation goes here

    b = sign(sum(v .* s));
end
```

Once $\hat{b}$ was obtained from the attacked watermark vector it is compared to the binary symbol b and if they are NOT equal the decoding error count c was incremented. An empirical probability of decoding error was then calculated by dividing the count by N.

The graphs I obtained for repitiion values of 10,20 and 30 are shown below.



(a) (b) (c)

Figure 1: Graphs of P(Detection of Error) vs. WNR where N = 1000

It is clear from these graphs that the probability of the detection of error decreases as the repetition factor increases. The reason for the initial probability of one is that there is no watermark present. (sidenote: although it i hard to see in the document but the minimum value for graph A is 0.35, for graph B is 0.32 and for graph C is 0.25)

1.2 DSSS with unknown spreading sequence

Instead of using the pseudorandom vector s mentioned in part 1 we use a new pseudorandom vector in the decoder which implements an unknown spreading sequence.

Here N $=$ 1000 as outlined in the assignment brief and I used 10 for a value of N. This is the same value of N as used in $fig.1(a)$. As the below figure clearly illustrates the decoding error is distributed around 0.5 this is the approximate value given to random chance. This is because the decoding is done using a pseudorandom vector which does NOT use the secret key which was used in part 1.

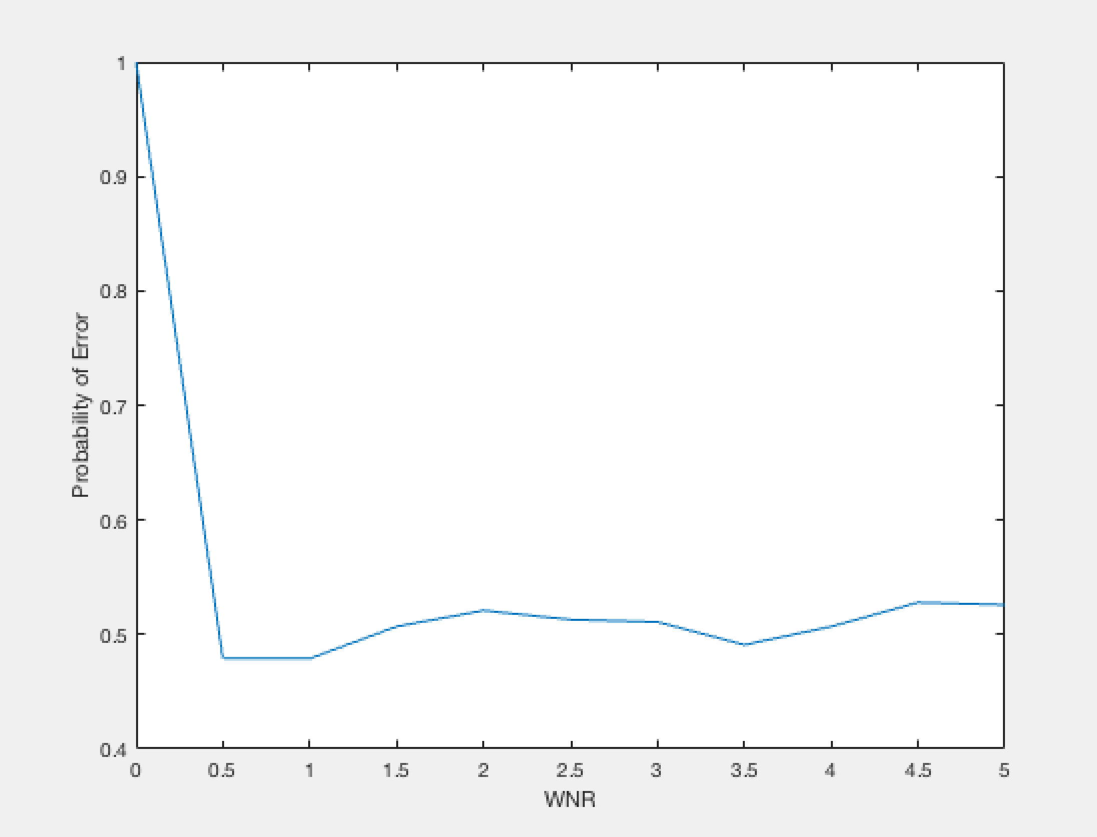


Figure 2: Decoding without secret key with values of L=10 and N=1000