EQ1220 - Project Assignment 2

Serkan Arda Yilal, Daniel Morales

I. Introduction

In this project, we are asked to decode an image that will reveal the identity of James Bond's target for his current mission. We need to equalize the received key, which has been distorted by the unknown channel impulse response, and successfully recover the original message. To do so, we will use the known training sequence transmitted in the preamble and define a linear MMSE estimator using a FIR filter. We will measure the error of filters of different lengths with the MSE. We also study the impact that random bit errors in the key have in the decoding of the image.

II. Communication System Model

We have a digital communication system with a channel of unknown impulse response. The binary key $s(k)$ is mapped to the constellation $\{-1, 1\}$ to form $x(k)$, which is transmitted using PAM. After going through the channel, $y(k)$ is received on the other end. The first 32 bits of the key are a training sequence known by the receiver, which will allow us to derive a filter $h(k)$ and equalize the received signal into $z(k)$. The equalized signal then goes into the detector to get an estimate of the original signal $\hat{x}(k)$ and key $\hat{s}(k)$.

On the other hand we have the encoded image, which has not been distorted but is encrypted. If the equalization is good enough to recover the key, we will be able to decode the image and reveal our suspect.

III. Design of FIR Filter

A. Linear MMSE estimation

We will design an equalizing filter of order L which will be a linear MMSE (Minimum Mean Square Error) estimator. This type of filter is also known as FIR Wiener filter. The MSE function that will be minimized is defined as

$$\overline{\text{MSE}}(\hat{X}) = \mathbb{E}\big\{(X - \mathbf{Y}^T\mathbf{h})^2\big\}, \tag{1}$$

where X is the process we want to estimate, $\mathbf{Y}$ is the vector of observations and $\mathbf{h}$ is the filter of order L.

If we differentiate (1) with respect to $\mathbf{h}$ and set it equal to 0 to find a minimum, we reach the following expression:

$$\mathbb{E}\big\{\mathbf{Y}(X - \mathbf{Y}^T\mathbf{h})\big\} = 0, \tag{2}$$

The interpretation of that equality is that the observations and the error must be orthogonal. The optimal filter $\mathbf{h}_{opt}$ that satisfies this condition is given by the Wiener-Hopf equation:

$$\mathbf{h}_{opt} = \mathbf{R}_Y^{-1}\mathbf{r}_{XY}. \tag{3}$$

Therefore, we can obtain the optimal filter from the auto-correlation matrix of the observations Y, provided that it is invertible, and the cross-correlation between the sought quantity X and observations Y.

B. Estimation of parameters

In order to calculate the optimal filter, we first need to obtain $\mathbf{R}_Y$ and $\mathbf{r}_{XY}$. We rely on the known training sequence of 32 symbols to estimate these parameters.

Starting with the cross-correlation vector, the expression is

$$\mathbf{r}_{XY} = \mathbb{E}\left\{X(n)\begin{pmatrix} Y(n) \\ Y(n-1) \\ \vdots \\ Y(n-L) \end{pmatrix}\right\} = \begin{pmatrix} r_{XY}(0) \\ r_{XY}(1) \\ \vdots \\ r_{XY}(L) \end{pmatrix}. \tag{4}$$

We will compute an estimate for each component of the cross-correlation using the 32 samples of the training sequence and the received symbols. For larger indexes, the estimate will be less accurate since we have less combinations of samples to average. The unbiased estimator we used is given by

$$\hat{r}_{XY,U}(k) = \frac{1}{N-k}\sum_{n=0}^{N-k-1} x(n+k)y(n) \tag{5}$$

for $k = 0, \ldots, L < N = 32$

We checked that the estimated acf was valid, it was positive at the origin and had an absolute maximum value at the origin. We also compared to the performance of the biased estimator. Since the unbiased is more accurate, it provided a better quality in the recovered image.

To derive the auto-correlation matrix, we will first estimate the auto-correlation vector. Using the fact that the auto-correlation is symmetric and $\mathbf{R}_Y$ is a Toeplitz matrix, the matrix can be expressed as

$$\mathbf{R}_Y = \begin{pmatrix} r_Y(0) & r_Y(1) & \dots & r_Y(L) \\ r_Y(1) & r_Y(0) & \dots & r_Y(L-1) \\ \vdots & \vdots & \ddots & \vdots \\ r_Y(L) & r_Y(L-1) & \dots & r_Y(0) \end{pmatrix} \tag{6}$$

To obtain the auto-correlation of Y we will use again an unbiased estimator, written as

$$\hat{r}_{Y,U}(k) = \frac{1}{N-k} \sum_{n=0}^{N-k-1} y(n+k)y(n) \tag{7}$$

for $k = 0, \dots, L < N = 32$

At this point, we can obtain the L coefficients of the FIR filter $\mathbf{h}_{opt}$ by using the estimated parameters in equation (3).

IV. Evaluation of Equalizer

A. Equalizer

We have designed an equalizing filter from the knowledge of the channel distortion on the training sequence. The equalizing block will apply the filter to the received signal and output a recovered signal that should resemble the original transmission.

$$z(k) = \sum_{l=0}^{L} h_{opt}(l)y(k-l) \tag{8}$$

B. Evaluation

Since we use a linear estimation method, which is limited by the finite number of filter taps, the recovered signal $z(k)$ will never be a perfect copy of the original signal $b(k)$. Provided that we are using an optimal filter, we will minimize the error in the mean square sense, but some error will always exist.

A good measurement of the equalizer's performance is the MSE. Since we do not know ground truth about the whole key, we can only compute the MSE in relation to the training sequence values. Furthermore, we can only measure error of samples from $L+1, \dots, 32$, as we don't know the channel before $k = 0$ and the filter uses the last $L+1$ sampled observations.

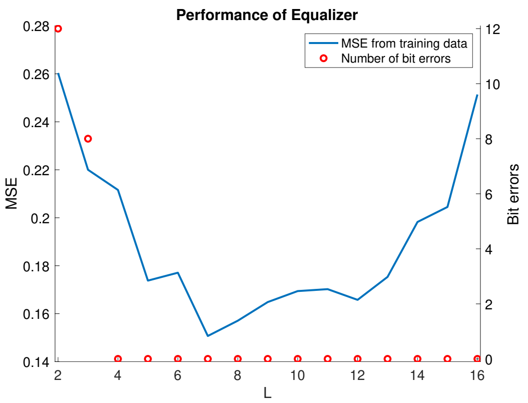

Fig. 1: MSE and number of bit errors of equalized signal with respect to the training sequence for different L values

Following from (1), the empirical MSE is

$$\overline{\text{MSE}}(Z) = \frac{1}{N-L-1} \sum_{k=L+1}^{N} (x(k) - z(k))^2 \tag{9}$$

The choice of L is a sensitive parameter of the equalizer. A longer FIR filter can potentially be more precise as it has more coefficients, but the estimation accuracy of correlation in (4) and (7) will resent as the limited number of samples for large indexes increases the variance.

In Figure 1 we plot the MSE from (9) as well as the number of bit errors after decoding. The MSE is the better error measurement as it provides more granularity. The lowest MSE is for $L = 7$ at 0.15. However, since we have a very limited training sequence, MSE is subject to a non-negligible variance. Therefore, we can only conclude that the best equalizer has a length L probably somewhere between 7 and 12, the lowest values in the plot. Later we will cross check that with a visual inspection.

V. Decoder and Image Recovery

After equalizing the received signal, the next step is to decode the symbols. We have a simple constellation of two symbols $\{-1, 1\}$, and the decoder can be realized by maximum likelihood with a sign function.

$$\hat{x}(k) = \text{sign}\big(z(k)\big). \tag{10}$$

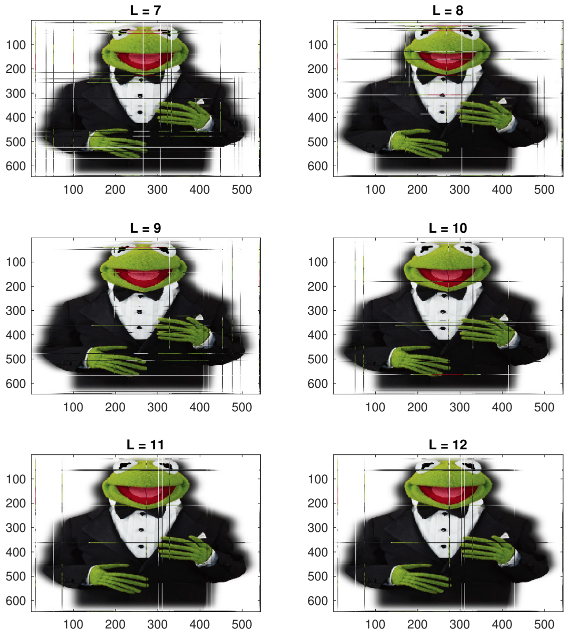

Fig. 2: Decoded images using the key recovered from different equalizer filters of order L

The recovered key $\hat{s}(k)$ is obtained by mapping $\hat{x}(k)$ to $\{0, 1\}$ and allows us to decode the encrypted image. In Figure 2 we compare the decoded images using different keys corresponding to equalization with different values of L. From visual inspection, we conclude that the best results seem to come from using a FIR filter of order $L = 9$. It is not 7, as we had anticipated with MSE, but it is within the range of low MSE values.

VI. Random bit errors

After we reconstruct our key with the most optimal filter order, $L = 9$, we will introduce random bit errors in that reconstructed key. By doing that, we will try to detect a threshold number of random bit errors such that the encoded image cannot be decoded anymore.

We introduce randomly distributed bit errors by changing the bit values of randomly chosen indexes of the key. First, we will start to have small amounts of random bit errors at the beginning. Then we will slightly increase the amount of the error so that we can detect the aforementioned threshold faster. For this purpose, our bit error amounts will be $\{0, 25, 100, 175, 250, 325, 400, 500, 600, 700, 875, 1050\}$ consecutively.

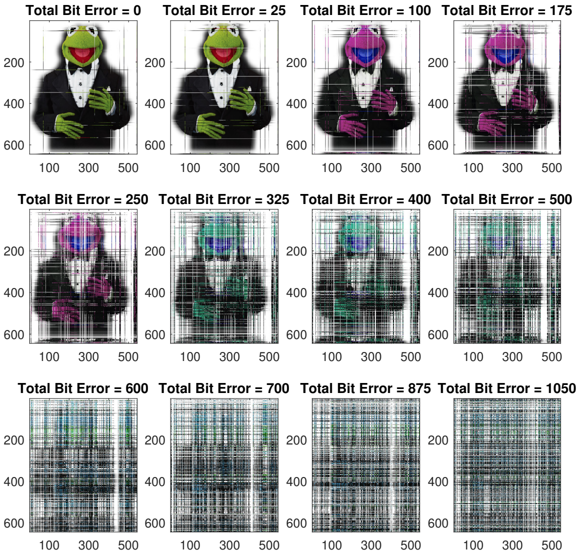

Fig. 3: Impact of Random Bit Errors

As we observe the decoded images with different amounts of bit errors in Fig. 3, we see that the image starts to become distorted and even lose its true colors starting from 100 errors, out of a 11932 bit long key. If we increase the amount of random bit errors in our reconstructed key, we will not be able to decode the image and recognize anything after around 700 bit errors.

VII. Summary and Conclusions

Throughout this project, we have designed our FIR filter by estimating auto-correlation and cross-correlation functions from training data, so we could obtain our filter coefficients from the Wiener-Hopf equation. We had to find optimal filter length considering the trade-off between potential filter accuracy and amount of training data, and measured that with a MSE function. We learned that the best performance measurement did not quite match with the best result on a visual inspection, due to the limited length of training sequence used to compute MSE. After equalizing the received signal, we applied a maximum likelihood detector based on sign function and successfully decoded the encrypted image with the estimated key. Lastly, we have introduced random bit errors in our estimated key to test its durability against bit errors such that the encoded image will not be decoded within the estimated key anymore.