EQ1220 Signal Theory – Project Assignment 2

Yuqi Zheng, Ernan Wang

I. INTRODUCTION

In this project, we are going to simulate the encryption system and the digital communication model. We aim to design an FIR equalizer and find a good filter order to reconstruct the distorted input key which is used to decode an encrypted image. In addition, we will investigate the number of bit errors that the key can contain. To fulfil our goals, we will combine mathematical derivations with the implementations of MATLAB.

II. PROBLEM FORMULATION AND SOLUTION

A. Assignment 1 and Assignment 2

In this section, we are supposed to design an FIR equalizer h to remove the effect of the channel and reconstruct the key, $X(k)$, from the received signal $Y(k)$. Besides, we need to find a relatively good filter order L.

We choose the casual FIR Wiener filter to equalize the received sequence. First, we assume the order of this filter is L. Then, we can obtain an estimator with a finite unit sample response of received signal as follows[1],

$$\hat{X}(n) = \sum_{l=0}^{L} h(l)Y(n-l) = \boldsymbol{h}^T\boldsymbol{Y}(n), \quad (1)$$

where the vectors $\boldsymbol{Y}(n)$ and $\boldsymbol{h}$ are given by

$$\boldsymbol{Y}(n) = \begin{pmatrix} Y(n) \\ \vdots \\ Y(n-L) \end{pmatrix}, \boldsymbol{h} = \begin{pmatrix} h(0) \\ \vdots \\ h(L) \end{pmatrix}. \quad (2)$$

The optimal (the one that is minimizing the MSE) parameter vector is shown as below,

$$\boldsymbol{h}_{FIR} = \boldsymbol{R}_{\boldsymbol{Y}}^{-1}\boldsymbol{r}_{XY}, \quad (3)$$

where

$$\boldsymbol{R}_{\boldsymbol{Y}} = \begin{pmatrix} r_Y(0) & \cdots & r_Y(L) \\ \vdots & \ddots & \vdots \\ r_Y(L) & \cdots & r_Y(0) \end{pmatrix}, \quad (4)$$

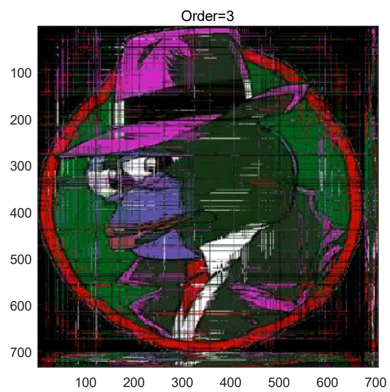
$$\boldsymbol{r}_{XY} = \begin{pmatrix} r_{XY}(0) \\ \vdots \\ r_{XY}(L) \end{pmatrix}. \quad (5)$$

In MATLAB, we utilize the function xcorr() to calculate the autocorrelation function and the cross correlation function of the sequences. In particular, for a better performance, we set the normalization option to "biased" in this case. The formulas we use are as follows.

$$\hat{r}_{Y,biased}(m) = \frac{1}{N}\hat{r}_Y(m) = \frac{1}{N}\sum_{n=0}^{N-m-1} y_{n+m}y_n^* = \frac{N-m}{N}r_Y(m), \quad (6)$$

$$\hat{r}_{XY,biased}(m) = \frac{1}{N}\hat{r}_{XY}(m) = \frac{1}{N}\sum_{n=0}^{N-m-1} x_{n+m}y_n^* = \frac{N-m}{N}r_{XY}(m). \quad (7)$$

Based on the above principles, we realize a casual FIR Wiener filter whose order is L in MATLAB, with which we filter the received sequence. After filtering the received sequence, we decide the estimated sequence into 1 and -1 using sign function. Once the decision has been made, we obtain the reconstructed key, with which we decode encoded picture. Figure 1 shows the decoded pictures with the filters whose order is 3, 8, 11 and 14.



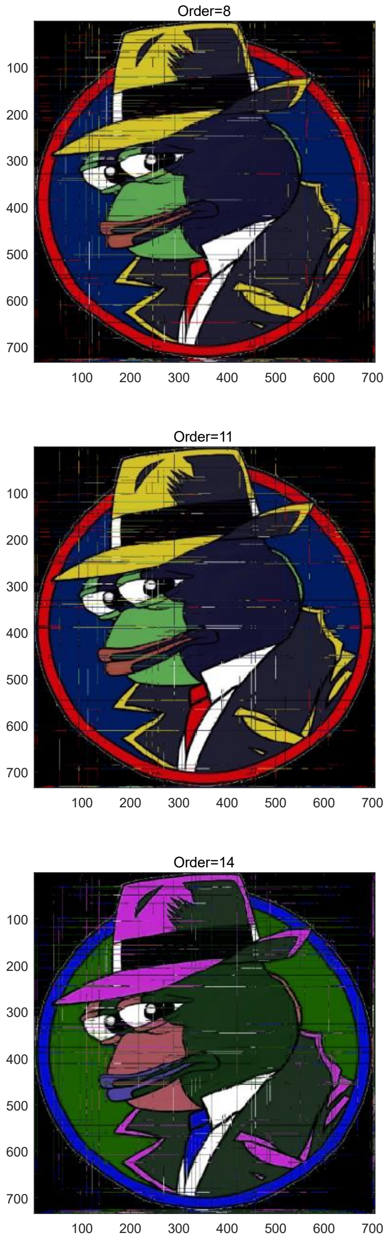


Figure 1:Decoded picture with differnt orders.

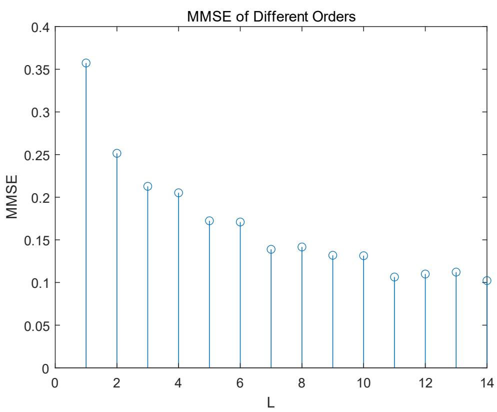


Figure 2: MSE when filter's order varies.

From the decoded pictures, we observe that when the order of filter is 11, the decoded picture is the clearest one.

Besides, to measure the performance of the equalizer, we calculate the MSE of the sequence reconstructed from different order and the result is shown in Figure 2. The formula we use is given as follows.

$$MSE[\hat{X}(\boldsymbol{Y})] = E\left[\left(\hat{X}(\boldsymbol{Y}) - X\right)^2\right]. \qquad (8)$$

From Figure 2, we can see when the order of the filter is 11, the MSE is relatively small.

According to the numerical and visual results listed above, we conclude 11 to be the best choice of the order and the type of the filter is the casual FIR Wiener filter.

B. Assignment 3

In this section, we introduce random bit errors in the reconstructed signal. Besides, we plan to investigate the maximum number of bit errors that the image can tolerate under recognizable conditions.

In this case, we set the filter order L to be 11 since it maximizes the performance of the equalizer as shown in Assignment 2.

To introduce the bit errors randomly, we plan to change the values of random positions of the signal passing through the detector. The number of the positions to be changed is the number of bit errors we plan to introduce.

In MATLAB, we utilize the randperm() function to realize this. The function randomly selects the positions of the detected signal and we multiply its values by -1. Hence, we complete the introduction of random bit errors. Then, we decode the encrypted picture with this changed signal.

We find that as more bit errors are introduced, the decoded picture starts to get blurred and the color even changes. When the number reaches 2800, the decoded picture becomes completely unrecognizable as shown in Figure 3.

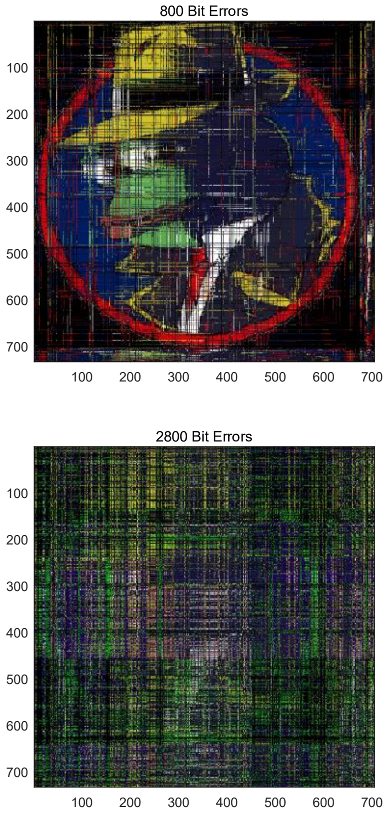


Figure 3:Decoded picture with bit errors.

III. CONCLUSIONS

In this project, we look into the processing and reconstruction of the signal. Especially, we study the FIR Wiener filtering. We determine the equalizing filter coefficients and the best filter order based on visual results and MMSE. In this way, we get the key to decode the picture. Also, we find the maximum number of bit errors can be introduced.

Actually, the signal reconstructed is not perfect because the equalizer is linear rather than optimal. The optimal filter will have a better performance which can be further studied.

REFERENCES

[1] P. Handel, R. Ottoson, H. Hjalmarsson, Signal Theory, KTH, 2012