Project 2

Chenting Zhang, Shaotian Wu

I. Introduction

In this project, we need to decode an image that James Bond received. We only have encrypted image and spy data at hand, so we need to design an equalizer to equalize the received signal and then decode the encrypted image using the reconstructed key. To do so, we need to define a linear MMSE estimator using a FIR filter and select the best filter order from the known training sequence. Lastly, we will add random bit errors to test the limited bit errors through which the decoder could not decode the image anymore.

II. Problem Formulation and Solution

A. Design the equalizer and detector

We shall use the model of causal FIR Wiener filter to solve this problem. We denote X(n) as the process we want to estimate, Y as the vector of observations and h as the filter of order L. Then An estimator with a finite unit impulse response(FIR) is given by the structure as follows:

$$\hat{X}(n) = \sum_{l=0}^{N-1} h(l)Y(n-l) = \mathbf{h}^T\mathbf{Y}(n), \qquad (1)$$

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

$$\mathbf{Y}(n) = \begin{pmatrix} Y(n) \\ \vdots \\ Y(n-N+1) \end{pmatrix} \quad \mathbf{h} = \begin{pmatrix} h(0) \\ \vdots \\ h(N-1) \end{pmatrix}.$$

The optimal parameter vector to minimize the MSE is given by the solution to the normal equations[1]

$$\mathbf{h}_{FIR} = \mathbf{R}_\mathbf{Y}^{-1}\mathbf{r}_{X\mathbf{Y}}. \qquad (2)$$

In this specific problem, we need to estimate the cross correlation function of X and Y ($\mathbf{r}_{X\mathbf{Y}}$) and auto correlation function of Y ($\mathbf{R}_\mathbf{Y}$) respectively.

For $\mathbf{R}_\mathbf{Y}$, the expression is written as follows

$$\begin{aligned}\mathbf{R}_\mathbf{Y} &= E\left[\begin{pmatrix} Y(n) \\ \vdots \\ Y(n-N+1) \end{pmatrix}\begin{pmatrix} Y(n) & \cdots & Y(n-N+1) \end{pmatrix}\right] \\ &= \begin{pmatrix} r_Y(0) & \cdots & r_Y(N-1) \\ & \ddots & \\ r_Y(N-1) & \cdots & r_Y(0) \end{pmatrix}.\end{aligned} \qquad (3)$$

For $k = 0, 1, 2, \cdots, L$ The estimator of $r_Y(k)$ could be written as

$$\hat{r}_Y(k) = \frac{1}{N-k}\sum_{n=1}^{N-k} Y(n+k)Y(n). \qquad (4)$$

It is an unbiased estimator since it is positive and has an absolute maximum value at the origin. Likewise, For $\mathbf{r}_{X\mathbf{Y}}$, the expression is written as follows

$$\mathbf{r}_{X\mathbf{Y}} = E\left\{X(n)\begin{pmatrix} Y(n) \\ \vdots \\ Y(n-N+1) \end{pmatrix}\right\} = \begin{pmatrix} r_{XY}(0) \\ \vdots \\ r_{XY}(N-1) \end{pmatrix}. \qquad (5)$$

For $k = 0, 1, 2, \cdots, L$ The unbiased estimator of $r_{XY}(k)$ could be written as

$$\hat{r}_{XY}(k) = \frac{1}{N-k}\sum_{n=1}^{N-k} Y(n+k)X(n). \qquad (6)$$

By plugging in the estimators of $r_Y(k)$ and $r_{XY}(k)$ in equation (3) and equation(5), we could obtain $\mathbf{h}_{FIR}$, which is the optimal coefficients $\mathbf{h}_{opt}$ of equalizer of different order L.

Now by applying this equalizer to the received signal, we could get the equalized signal and the reconstructed key. We denote the equalized signal as $\hat{r}(k)$, reconstructed key as $\hat{b}(k)$, they could be written as follows:

$$\hat{r}(k) = \sum_{l=0}^{L} h_{opt}(l)y(k-l), \qquad (7)$$

$$\hat{b}(k) = sign\left\{\hat{r}(k)\right\} = \begin{cases} -1, & \hat{r}(k) \le 0 \\ 1, & \hat{r}(k) > 0 \end{cases}, \qquad (8)$$

where L is the order of the equalizer. Then we use the MSE(mean square error) to measure the performance of each equalizer. Given the training sequence, we could calculate the MSE of each equalizer. Besides, we could only use the training sequence from L+1 to 32 due to the fact that we do not know the received signal $y(k-L)$ when $k-L<0$.

The empirical MSE is

$$MSE = \frac{1}{32-L}\sum_{k=L+1}^{32}(\hat{b}(k)-x(k))^2, \qquad (9)$$

when L increments from 1 to 32, we could calculate the values of MSE corresponding to the given L, the scatter diagram in figure(1) shows that the optimal L should lie in small value intervals. Theoretically, we could observe from figure(2) that the MSE has the least value 0.1956 when $L=7$.

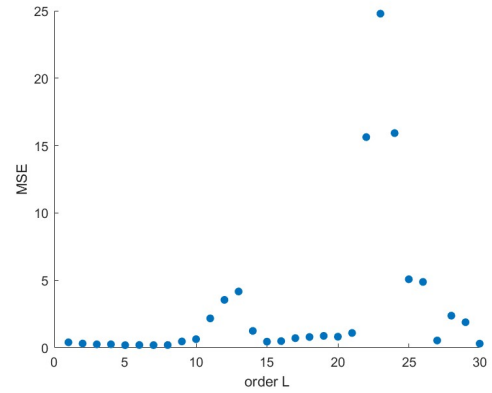


Fig. 1: MSE(L from 1 to 32)

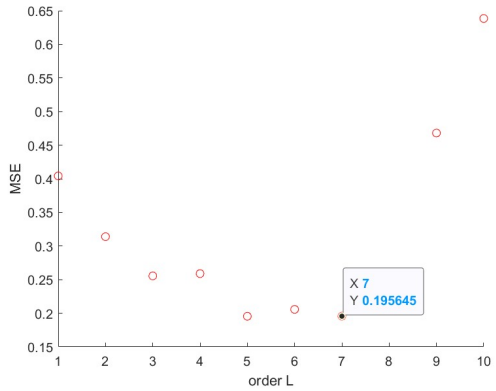
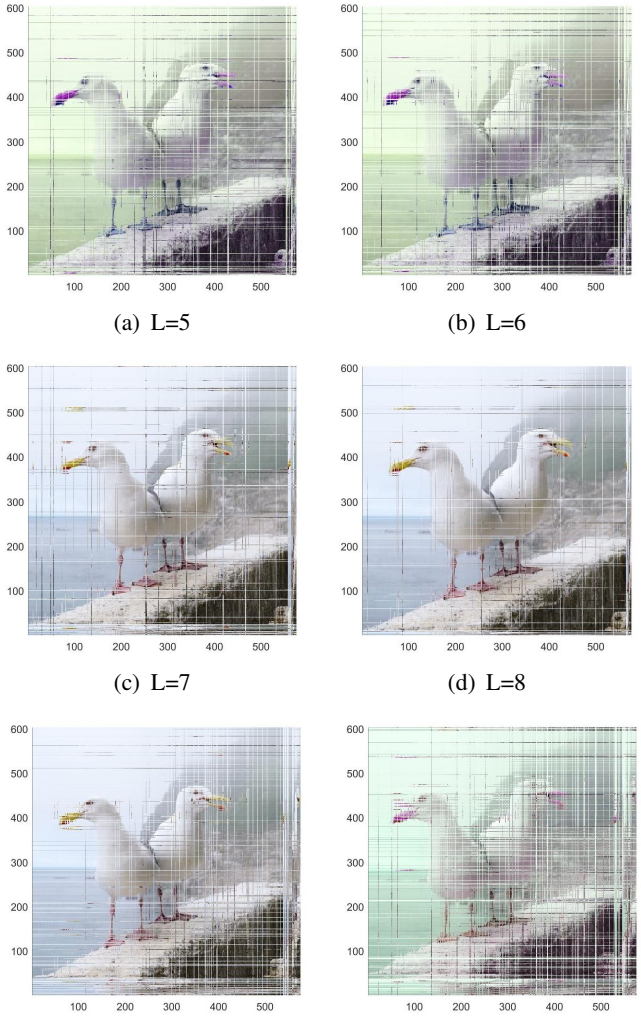


Fig. 2: MSE(L from 1 to 10)

B. Decode the encrypted image

Now we try to use the reconstructed key to decode the encrypted image. Observing from the six sub images in figure(3) below, we could conclude that L=8 is the optimal order of the equalizer filter while the theoretical value L=7 is the sub-optimal choice.



(a) L=5 (b) L=6

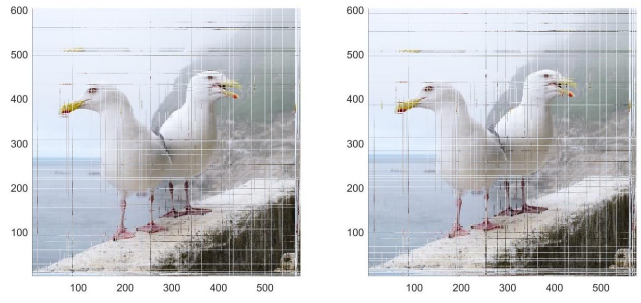
(c) L=7 (d) L=8

(e) L=9 (f) L=10

Fig. 3: Decoded images given different values of L

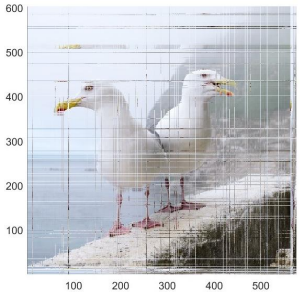
C. Add random bit errors

Based on the analysis above, we choose the equalized filter order L=8. Thus, we will obtain a corresponding reconstructed key which has 11842 bit long. In this part, we would add random number of bit errors to the reconstructed key and test the limited bit errors through which the decoder could not decode the image anymore. The number of ran-

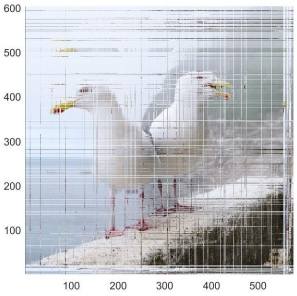


(a) error bits=0

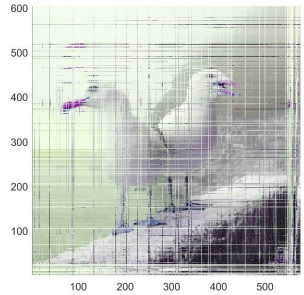
(b) error bits=50



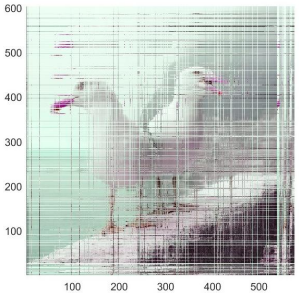
(c) error bits=100



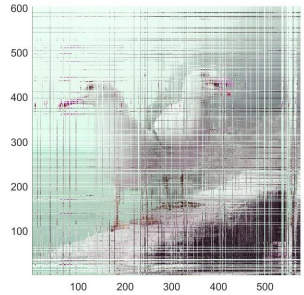
(d) error bits=200



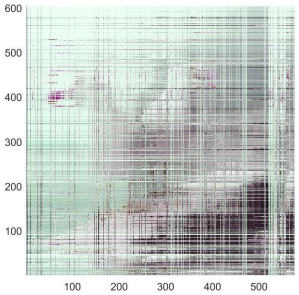
(e) error bits=300



(f) error bits=400



(g) error bits=500



(h) error bits=1000

Fig. 4: Decoded images given random error bits

dom bit errors would be selected from the sequence $\{0, 50, 100, 200, 300, 400, 500, 1000\}$.

We could observe from figure(4) below that the decoded images start to become distorted with increasing random error bits. When error bits increases to 300, the decoded image changes its true color. Additionally, as is illustrated in the sub figure(h), when the number of error bits increases to 1000, it is hard to recognize the ”suspect” in the decoded image.

III. Conclusions

In this project, we have designed an filter to help James Bond decode an encrypted image he received. Firstly, we used the FIR Wiener filter model to solve this problem. In detail, We obtained the filter coefficients by calculating the auto-correlation function and cross correlation function from the training sequence and generated the reconstructed key. Then we used MSE to estimate the performance of the reconstructed key and obtain the theoretically optimal order of filter L. After that, we put it into practice and decoded the image given different values of L. Lastly we added random bit errors to test the threshold of the stability of the reconstructed key.

References

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