Signal Theory Project 2

Hanqi Yang, Qian Zhou

I. INTRODUCTION

In this project, we investigate model of a simple digital communication system. We mainly focus on building an equalizer with an appropriate filter order L and a detector to reconstruct the received data, i.e. the key, which can be used to decode the encrypted image. We also discuss the impact of the number of bit errors on the quality of recovered image.

In the first part, we build the system model and derive the coefficient of filter. In the second part, we discuss the choice of filter order L and reconstruct the encrypted image, and then investigate the impact of number of bit errors.

II. MODEL BUILDING

The encrypted data bits, $s(k) \in \{0,1\}$, are initially mapped to

$$b(k) = \begin{cases} -1 & s(k) = 0, \\ 1 & s(k) = 1. \end{cases} \quad (1)$$

$b(k)$ will be transmitted through the channel with a distortion h and some additive noise $n(k)$. The output signal $r(k)$ will pass through the equalizer and the detector that can be used to reconstruct $b(k)$. The reconstructed data will be used to decode the encrypted picture.

Since the channel distortion is a time-invariant, time-discrete and unknown FTR filter h , the output of channel is

$$r(k) = \sum_{l=0}^{3} h(l)b(k-l) + n(k), \; k = 1,\dots,N, \quad (2)$$

The equalizer filter should be designed as

$$z(k) = \sum_{l=0}^{L} w(l)r(k-l) \approx b(k),$$

$$\text{for } k = L+1,\dots,32 \quad (3)$$

To obtain $w(l)$, channel distortion should be tested by a training sequence of 32 symbols which are added at the beginning of data. The sequence is known to the receiver. We can only measure the equalizer performance for $k = L+1,\dots,32$ because $k-l$ must be larger than 0 and length of the training data is 32. For $k \le L$, the equation cannot be used, so we use the training sequence instead.

Define a matrix $\mathbf{R}$, a vector $\mathbf{w}$, a vector $\mathbf{z}$ to rewrite equation (3) as matrix form

$$\mathbf{Rw} = \mathbf{z} \quad (4)$$

where

$$\mathbf{R} = \begin{bmatrix} r(L+1) & r(L) & \cdots & r(1) \\ r(L+2) & r(L+1) & \cdots & r(2) \\ \vdots & \vdots & \ddots & \vdots \\ r(32) & r(31) & \cdots & r(32-L) \end{bmatrix}$$

$$\mathbf{w} = \begin{bmatrix} w(0) \\ w(1) \\ \vdots \\ w(L) \end{bmatrix} \qquad \mathbf{z} = \begin{bmatrix} z(L+1) \\ z(L+2) \\ \vdots \\ z(32) \end{bmatrix}$$

The MSE can be expresses as

$$MSE(\mathbf{w}) = \frac{1}{32\text{-}L} \sum_{k=L+1}^{32} (b(k) - z(k))^2$$

$$= \frac{1}{32\text{-}L} (\mathbf{b} - \mathbf{Rw})^T (\mathbf{b} - \mathbf{Rw}). \quad (5)$$

The solution which minimizes the MSE is also the least-square solution for the coefficient $\mathbf{w}$. As mentioned in [2], let

$$\mathbf{J}(\mathbf{w}) = (\mathbf{b} - \mathbf{Rw})^T (\mathbf{b} - \mathbf{Rw})$$

$$= \mathbf{b}^T\mathbf{b} - 2\mathbf{b}^T\mathbf{Rw} + \mathbf{w}^T\mathbf{R}^T\mathbf{Rw} \quad (6)$$

the gradient is

$$\frac{\partial \mathbf{J}(\mathbf{w})}{\partial \mathbf{w}} = -2\mathbf{R}^T\mathbf{w} + 2\mathbf{R}^T\mathbf{Rw} \quad (7)$$

Setting the gradient equal to zero yields the least squares estimator

$$\mathbf{w} = (\mathbf{R}^T\mathbf{R})^{-1}\mathbf{R}^T\mathbf{b} \qquad (8)$$

LS is a linear estimator, so it only works when there is a linear relationship between the known quantity and the quantity to be estimated. Only if the $\mathbf{R}^T\mathbf{R}$ is irreversible, the equation (8) can be calculated.

If the input process is a weakly stationary stochastic process, the casual finite impulse response (FIR) Wiener filter can also minimize the MSE by estimating the ACF and cross correlation terms once. Even though the Wiener filter is optimal in most cases, it does not perform much better than LS for a finite training sequence of length 32 due to the noise n(k).

When the coefficient $\mathbf{w}$ of equalizer is calculated, we can remove noise and distortion from received data. Finally, we use the detector to reconstruct $b(k)$. The detector is modeled as

$$\hat{b}(k) = sign\{z(k)\} = \begin{cases} 1 & z(k) > 0 \\ -1 & z(k) < 0 \end{cases} \qquad (9)$$

III. RESULTS AND ANALYSIS

A. Choice of filter order

When choosing an appropriate equalizer filter order L, we need to consider both having a detailed model and having enough equations in (3).

We use an arbitrary transfer function with four taps (order 3),

$$h(k) = \begin{cases} 1, & \mathrm{k} = 0 \\ 0.7, & \mathrm{k} = 1,2,3 \\ 0, & \text{otherwise} \end{cases} \qquad (10)$$

and white noise $n(k) \overset{\text{i.i.d.}}{\sim} N(0, 0.2^2)$ to generate a new $r(k)$ according to equation (2). Based on the methods mentioned in Part II, we obtain $\mathbf{w}$ and substitute it into $MSE(\mathbf{w})$ in (5). Then we can plot MSE in function of filter order L, which is shown in Figure 1. Because the actual realization of Gaussian noise is different each time, this introduces a great deal of randomness into the calculation of the MSE, resulting in a change in the image of equation (5) each time it is performed. We have therefore iterated this process 10 times, with each line in the Figure 1 representing one iteration.

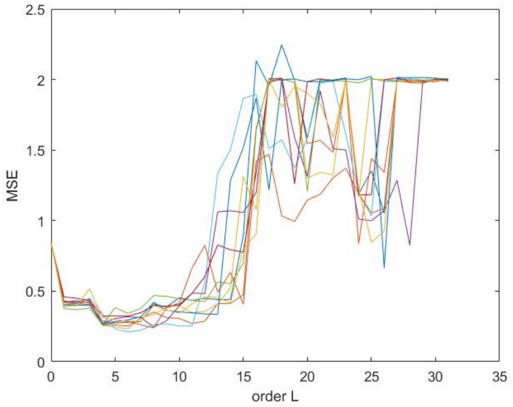
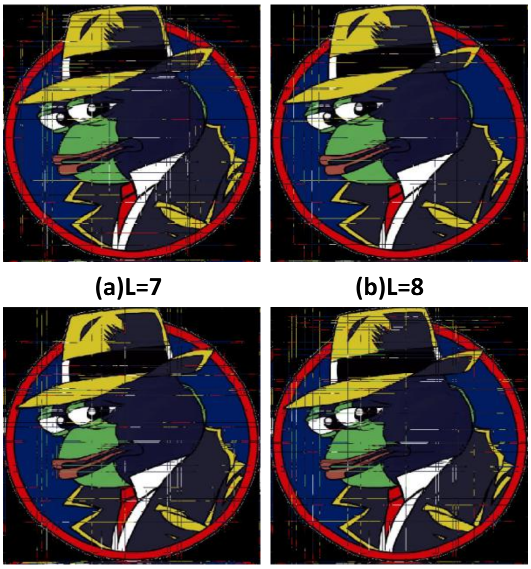


Figure 1: MSE between the recovered signal and the original key

As shown in Figure 1, the MSE can be minimized when the order L is in the interval from 4 to 11. Note that the number of orders L and the number of coefficients $\mathbf{w}$ are the same, and the number of equations is 32-L in equation (3). Too large an order L would allow too few equations to determine a large number of coefficients $\mathbf{w}$, which would lead to an infinite number of solutions. Therefore, the MSE becomes large when the order L is greater than 15.

B. Image decoding

After determining the range of order L, b(k) is reduced using the method in Part II and we use it to decode the image. Figure 2 shows the decoded image of order L from 7 to 10. Although there is no great difference in the recovery of the four images, Figure 2 (b) performs the best among them, i.e., L=8 is the best choice of filter order.

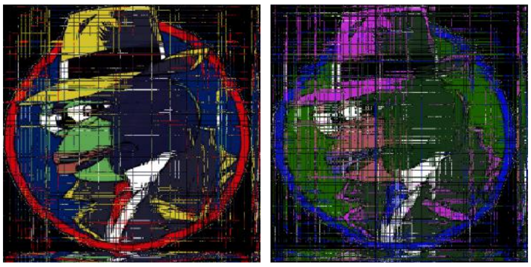


(a)L=7 (b)L=8

(c)L=9 (d)L=10

Figure 2: Decoded images of order L from 7 to 10

When the order L is not within the range selected in part A, the picture has poor recovery quality, as shown in Figure 3, which confirms our hypothesis.



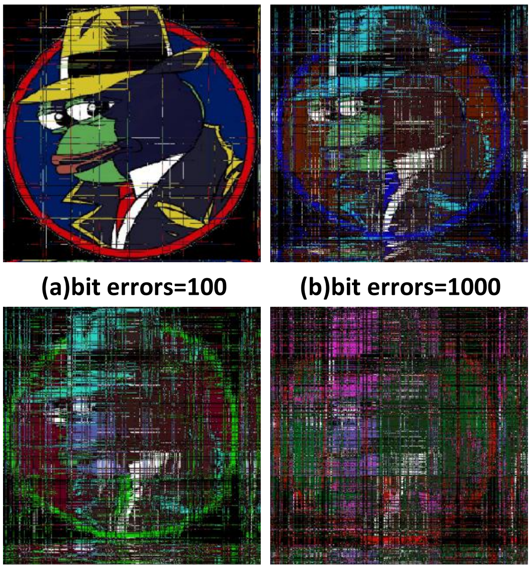
(a)L=3 (b)L=12

Figure 3: Decoded images of order L=3 and 12

C. Influence of bit errors

Next, we will investigate the effect of the number of bit errors on the decoding of images. We set L=8 and use function *randperm(n,k)*, which returns a row vector containing k unique integers selected randomly from 1 to n.

We introduce different numbers of bit errors to compare the quality of the recovered images, as shown in Figure 4. When the number of bit errors is 100, the image is still well recovered. When the number of bit errors is 1500, the outline of the frog detective can only be barely distinguished, but when the number of bit errors reaches 2000, the image is already almost unrecognizable.



(a)bit errors=100 (b)bit errors=1000

(c)bit errors=1500 (d)bit errors=2000

Figure 4: Decoded images of different bit errors

IV. CONCLUSIONS

In this project we have carried out the following work: designing an equalizer with appropriate filter order L and a detector to reconstruct the key to decode the encrypted image. We find that image recovery is best at L=8. We also introduce bit errors in the reconstructed key to find the threshold where an image cannot be restored. When the number of bit errors reach 2000, the image is difficult to distinguish.

REFERENCES

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

[2] Fundamentals of Statistical Signal Processing, Steven M. Kay, University of Rhode Island, 2014.