Template for Report

[redacted]

I. INTRODUCTION

This time, we act as the assistants of Agent 007, James Bond, who has already got the undistorted but encrypted image of his target. Our task is to help him to recover the received key interrupted by an unknown channel. The key is necessary for decoding the image and identifying the target. What we have is the correct version of the first 32 bits of the key, also known as "training sequence", along with the decoder. To accomplish this, we design a Causal FIR Weiner Filter to "equalize" the received key. The optimal order of the filter is discussed. Furthermore, we test the tolerance of the filter by introducing random bit errors.

II. METHODOLOGY

The original key, $w(k) \in \{0,1\}$, is the one of two outputs of the encoder. By pulse amplitude modulation, $w(k)$ is mapped to $x(k)$, the transmitted key, which takes values from the set $\{-1,1\}$ and can be directly transmitted in digital communication systems. $y(k)$ is the received key after passing a 4-tap FIR communication channel with unknown response $h_c(k)$ and additive white Gaussian noise (AWGN) $n(k)$. $y(k)$ can be expressed as

$$y(k) = \sum\nolimits_{l=0}^{3} h_c(l)x(k-l) + n(k),\ k = 1,2,\dots,N. \tag{1}$$

Recovering $w(k)$ is equivalent to recovering $x(k)$. To accomplish this, equalization is needed. The equalized key $\hat{z}(k)$ can be expressed as formula (2). We can recover the transmitted key by formula (3), which is a Maximum-Likelihood estimation process. Once $\hat{x}(k)$ is obtained, the image of the target can be decoded.

$$\hat{z}(k) = \text{Equalizer}[y(k)]. \tag{2}$$

$$\hat{x}(k) = \text{sign}[\hat{z}(k)]. \tag{3}$$

The crux of solving the problem is designing an appropriate equalizer. Our choice is a Causal FIR Weiner Filter, which is a type of Linear Minimum Mean Square Error (LMMSE) estimator. In the problem, $x(k)$ are distorted by a LTI channel with AWGN, and the first 32 bits of $x(k)$, the training sequence, is known. Therefore, using Causal Weiner FIR Filter to address equalization is feasible. Suppose a FIR filter with weights $\mathbf{h}$, if demanding estimating X over $\mathbf{Y}$, the mean square error (MSE) of estimation can be expressed as

$$\text{MSE}\big[\hat{X}(\mathbf{Y})\big] = \mathbb{E}[(X - \mathbf{Y}^T\mathbf{h})^2]. \tag{4}$$

To minimize MSE, we take the derivative of formula (4) with respect to $\mathbf{h}$ and let the equation equal to 0. The optimal filter response $\mathbf{h}_{opt}$ is given by

$$\mathbf{h}_{opt} = \mathbf{R}_Y{}^{-1}\mathbf{r}_{XY}. \tag{5}$$

Hence, to find the optimal filter response, the autocorrelation matrix of Y (can be viewed as received key), and the cross-correlation matrix of X (viewed as a part of transmitted key) and Y are required. Assume a FIR filter with order L, where $L < N = 32$, to calculate $\mathbf{R}_Y$ and $\mathbf{r}_{XY}$, it is necessary to estimate the value of r_Y and r_{XY} based on the following unbiased estimators

$$\hat{r}_Y(k) = \frac{1}{N-k}\sum\nolimits_{n=0}^{N-k-1} y(n+k)y(n), k = 0,1,\dots,L. \tag{6}$$

$$\hat{r}_{XY}(k) = \frac{1}{N-k}\sum\nolimits_{n=0}^{N-k-1} x(n+k)y(n), k = 0,1,\dots,L. \tag{7}$$

Then $\mathbf{R}_Y$ and $\mathbf{r}_{XY}$ can be derived from

$$\mathbf{R}_Y = \mathrm{diag}[\hat{r}_Y(0), \hat{r}_Y(1), \dots \hat{r}_Y(L)], \tag{8}$$

$$\mathbf{r}_{XY} = [\hat{r}_{XY}(0), \hat{r}_{XY}(1), \dots, \hat{r}_{XY}(L)]^T. \tag{9}$$

$\mathbf{h}_{opt}$ can be calculated via formula (5). The key after equalization is

$$\hat{z}(k) = \sum_{l=0}^{L} h_{opt}(l) y(k-l). \tag{10}$$

Finally, $\hat{x}(k)$ can be calculated from formula (3). All that requires to decode the image are in hand.

III. SELECTION OF FILTER ORDER

Causal FIR Weiner Filter is a linear estimation method. The performance is limited jointly by the length of training sequence and finite number of filter taps. It is impossible to recover the distorted key so that $\hat{z}(k)$ can reconstruct $x(k)$ in perfect. At this stage, it is required to make a trade-off between the filter complexity and the estimation accuracy of auto/cross correlations. Both will be affected by the choice of FIR filter order L. As L increases, the complexity of filter will increase since there is a greater number of weights included, but the estimation accuracy of $\mathbf{R}_Y$ and $\mathbf{r}_{XY}$ will decrease. This is because the estimations, $\hat{r}_Y$ and $\hat{r}_{XY}$ becomes less approximate to the actual values, $r_Y(k)$ and $r_{XY}(k)$, as k increases. For example, there are 32 pairs of $x(n)y(n)$ contributing to the estimation of $r_{XY}(0)$. For $r_{XY}(16)$, only 16 pairs of $x(n+16)y(n)$ are available. Thus, the estimation of $r_Y(k)$ and $r_{XY}(k)$ becomes less accurate for large k, as a small number of samples is less likely to possess ergodicity.

We vary the order of the proposed FIR filter from 1 to 31, to find the one with the best performance in this problem. Figure 1 only shows the recovered images using the equalized keys obtained from order 6-10 filters, due to constraints on report length. The image from filter order less than 5 and greater than 11 contains more interferences than those shown in Figure 1. The order of the optimal filter ranges from 7 to 9. The authors prefer the filter of order 8 from visual perspective. From the recovered image, the target is a blue-haired man, wearing white coat with blue T-shirt and drinking something from a green bottle, Rick Sanchez.

The selection of filter order can be further justified by calculating the MSE between the equalized key and the training sequence. For each order of filter, MSE of the first 32 bits can be calculated from

$$\mathrm{MSE}\big[\hat{Z}(X)\big] = \frac{1}{32}\sum_{k=0}^{31} [\hat{z}(k) - x(k)]^2 . \tag{11}$$

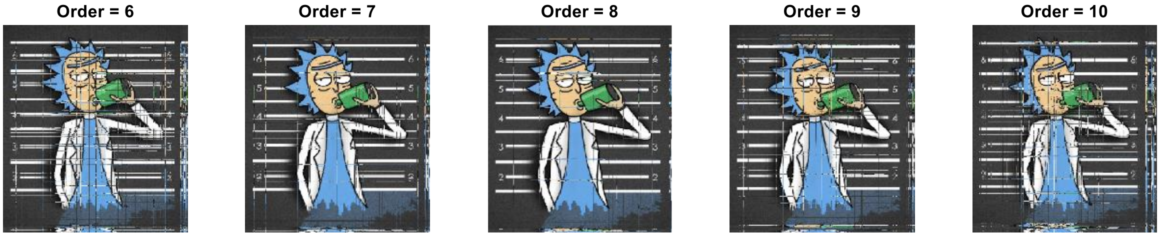

Figure 1. The decoded images corresponding to different orders of FIR filters.

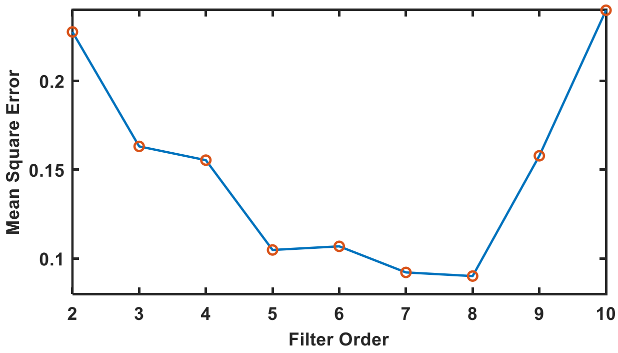

Figure 2. MSE with respect to Filter Order.

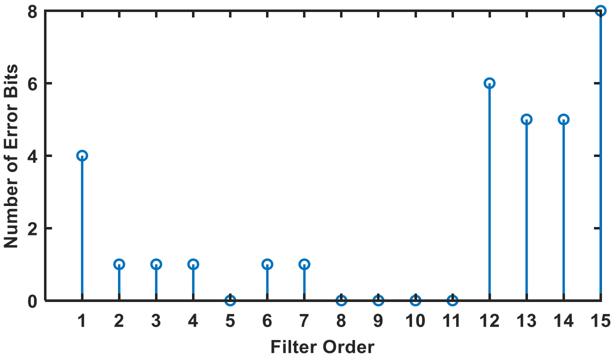

Figure 3. Total number of errors in the first 32 bits with respect to Filter Order.

The MSE record are shown in Figure 2. When filter order is 8, the MSE is minimized to 0.0901. The result indicating the same conclusion as that drawn from visual evaluation. In addition, the remained number of bit errors in the first 32 bits of equalized key are demonstrated in Figure 3. Since 0-bit error are achieved in many orders of filter, the authors do not consider this as a strong criterion. In summary, the optimal order of FIR filter for this problem is 8.

IV. TOLERANCE FOR BIT ERROR

Now that we have determined the order of FIR filter to be 8, we can further test the tolerance of our design if random bit error occurs in the reconstructed key $\hat{x}(k)$. The total length of key is 9862. Figure 4 shows the decoded images after a certain number of bits are inversed at random positions.

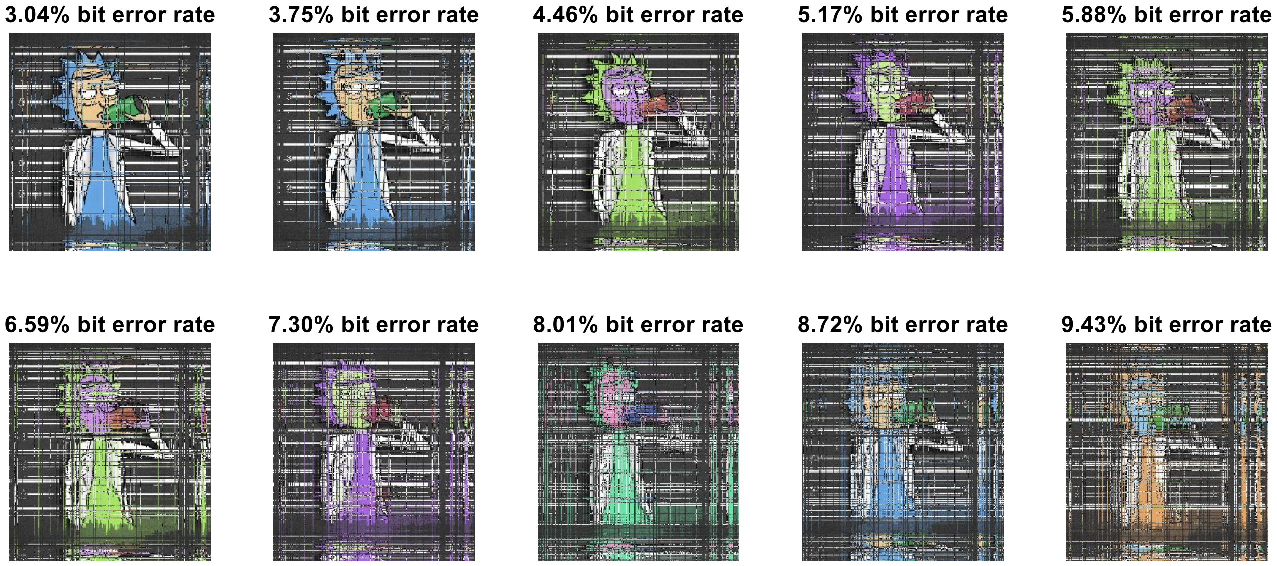

Figure 4. Decoded images when bit error occurs.

From Figure 4, when bit error rate is less than 5.17%, as though color distortion may occur, the target is recognizable. The images still possess critical features of target if 7.30% of bits go wrong. If more errors occur, 007 is likely to misidentify the target. To guarantee the success of our mission, the bit error rate should be no greater than 8%.

V. CONCLUSION

In this project, we successfully identify the target by recovering the encrypted image with the equalized and reconstructed key. The key step, equalization, is conducted using a causal FIR Weiner filter. The weights of the FIR filter are obtained from the famous Weiner-Hopf equation, which requires the estimations of the autocorrelation of received key, along with the cross-correlation between training sequence and received key. When selecting the order of filter order, one needs to make a balance between filter complexity and estimation accuracy. The optimal order of filter, 8, is jointly determined by visual inspection and MSE calculation. Furthermore, we explore the design tolerance of the filter by introducing random bit errors to the reconstructed key. Result shows that, if less than 700 bits are erroneous, the target can still be somehow recognized.

REFERENCES

[1] P. Handel, R. Ottoson, H. Hjalmarsson, *Signal Theory*, ch.9-10. KTH, 2012.