Wiener Filtering-Based Key Recovery for Encrypted Images and Fault Tolerance Analysis in Communication Systems

Biqi Liu, Divyayan Dey

I. Introduction

Visual data, while being transmitted via insecure links, is often encrypted to preserve confidentiality. Encrypting such data requires an encryption key, which also needs to be sent along with the data. Our problem statement lies in recovering the key so that it can be used for deciphering the original image data. However, transmission through communication channels is rarely noise-free, leading to signal ditortion and degradation. In this system, the communication channel is modeled as a time-invariant finite impulse response (FIR) filter, which introduces both deterministic distortion and additive white Gaussian noise (AWGN) to the transmitted signal. We aim to solve the task using the fundamentals of a digital communication system, particularly focusing on designing an equalizer to counteract the noise and distortion introduced by the channel. Additionally, we investigate the system's fault tolerance by introducing random bit errors and analyzing the impact on the image recovery process.

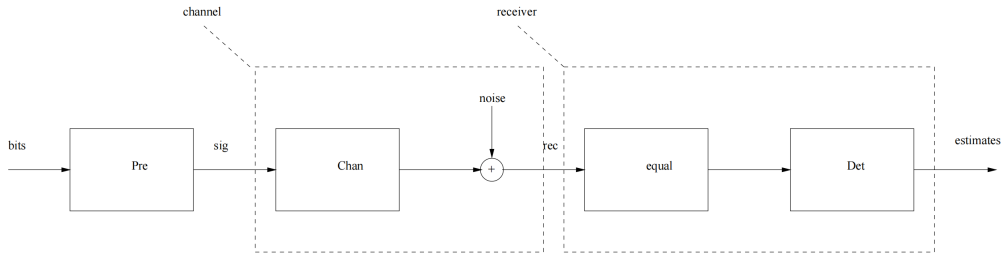

Fig. 1: Communication System

II. Theory and Implementation

Our task is to recover a noise-introduced key/sequence that will help in decoding an image (assumed to be uncorrupted). Recovering a noise-corrupted signal will require an FIR equalizing filter, which separates the channel distortions from the received signal as optimally as possible. The 32-symbol sequence present in **training.mat** serves as the training sequence for the equalizer. In our solution, we used Wiener Filter as the equalizer. The cost function is the Mean Squared Error(MSE), defined by -

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(X_i - \hat{X}_i)^2,$$

where X_i are the observed values and $\hat{X}_i$ are the predicted values of the sequence respectively.

A. Wiener Filter

The usual choice for a signal retrieval problem is to design an optimal Wiener Filter. The Wiener filter coefficients are determined using the Wiener-Hopf equation[2] -

$$R_Y h_{opt} = r_{YX}, \text{ where } R_Y = \mathbb{E}\{YY^T\},\ r_{YX} = \mathbb{E}\{YX\},$$

X and Y are the random variables for the desired and received sequences respectively. We iterate over filter orders 1 to 31 and determine which order minimizes the MSE, but also visually keeping track of which filter order best decodes the image.

B. Addition of random bit errors in the reconstructed key

In communication systems, the Bit Error Rate (BER) is an important measure of how reliable the system is. BER is defined as the ratio of the number of incorrect bits to the total number of bits transmitted. The formula is:

$$\text{BER} = \frac{N_{\text{errors}}}{N_{\text{total}}}$$

where, N_{errors} is the number of incorrect bits, N_{total} is the total number of bits.

When adding random bit errors, we choose an error rate e, which is used to calculate how many bits will be flipped:

$$N_{\text{errors}} = e \times N_{\text{total}}$$

These errors are spread randomly to simulate the effect of noise in the channel on the key.

The steps are as follows: First, we start with a low error rate (e.g., 1%) and slowly increase it until the image can no longer be correctly decoded.Second, random bit errors are introduced into the reconstructed key. The positions of these bits are chosen randomly, and their values are flipped by multiplying by -1, simulating the errors. Then, for each error rate, we use the corrupted key to try to decode the image and check if the image becomes "unrecognizable". Finally, we record the results for each error rate and find the maximum error rate at which the image can no longer be decoded correctly. And we get the number of bit errors.

III. Results and Analysis

A. Wiener filter

The task is best performed when a Wiener filter of order=**8** is used. Although the MSE plot shows even further decrease in MSE upto order 16, the image clarity decreases as we go further beyond 8. The decoded image as well as MSE curve is shown in Fig. 2 and Fig. 3 respectively.

$$h_{opt} = [0.7593, -0.0841, -0.4680, 0.2593, 0.2091, -0.3321, -0.0172, 0.1601]$$

$$MSE_{L=8} = 0.1473$$

After decoding, the image reveals a cartoon character, most identical to a *Simpson*[3] character.

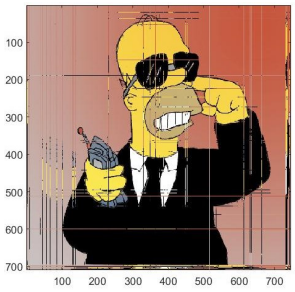

Fig. 2: Wiener filter decoded image

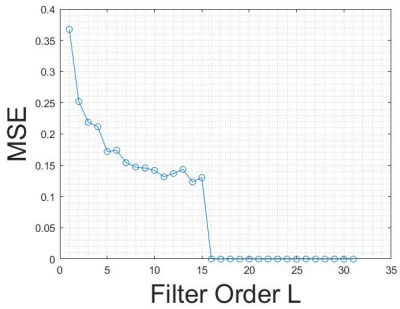

Fig. 3: Mean Squared Error for different orders of Wiener filter

B. Addtion of random bit errors in the reconstructed key

The bit error rate (BER) is calculated using the formula:

$$\text{BER} = \frac{\sum_{i=1}^{N_{\text{total}}} \mathbf{1}_{\{k_i \neq \hat{k}_i\}}}{N_{\text{total}}}$$

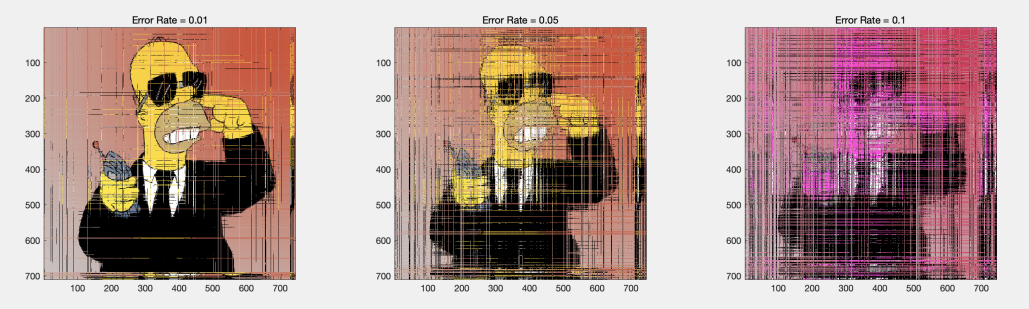

Fig. 4: Image after maximum error addition

where k_i is the i-th bit of the original key, $\hat{k}_i$ is the i-th bit of the recovered key with errors, $\mathbf{1}_{\{k_i \neq \hat{k}_i\}}$ is 1 when $k_i \neq \hat{k}_i$, and 0 otherwise.

In the end, we find the maximum error rate is 0.05, after which the image was "unable" to be decoded. So the max number of bit errors equal to 0.05*14602=730.1.

IV. Conclusion

In this project, we design an equalizer to recover the key in encrypted communication and test the system's ability to handle errors. First, we use a Wiener filter for decoding and find that the best filter order is 8, observing the MSE as well as the graphical clarity. The image is successfully decoded, showing a clear cartoon character. Additionally, we introduce random bit errors into the recovered key and calculate the bit error rate (BER). The result shows that the maximum tolerable bit error rate was 0.05. Based on this maximum error rate, we calculate that the system can tolerate up to approximately 730 erroneous bits. Once this error threshold is exceeded, the image becomes unrecognizable during decoding.

References

[1] P. Handel, R. Ottoson, H. Hjalmarsson, *Signal Theory*, KTH, 2012
[2] Wiener, Norbert. "Uber eine klasse singularer integralgleichungen." Sitz. Ber. Preuss. Akad. Wiss., Phys.-Math. 1 (1931): 696-706.
[3] Groening, Matt, and Scott M. Gimple. "The Simpsons forever: a complete guide to our favorite family continued." (No Title), 1999.