Haiqiang Zou

Biometric Security

Dr. Bon Sy

**Reflection**

In this class I learned how biometric systems work conceptually, technically, and basic idea of cryptography. I learned methods for identifying and verifying fingerprints, sampling voice and face recognition.

For the fingerprint identification and verification, we first need to find the minutiae points. After finding the minutiae points, we need to choose distance formula and the threshold value to use. I also learned how to use Hough transform to find out how many points are on same straight line or within the same circle.

For voice sampling, we first apply the Nyquist theorem to determine the highest frequency that we can sample without any information lost. By setting a frame time we will be able to determine how many samples are within each frame. After know the sampling frequency and frame, we will be able to apply Fourier transform to transform the discrete graph of S(n) into a discrete graph of S(k) to tell if they are or not the same.

For face recognition we use feature vectors to compare if two faces are the same. In order to find the feature vector, we use the Eigen based approach to determine the feature vector of each face image and use it to compare if the faces are the same or not.

There are two types of cryptosystem, which are the symmetric system and asymmetric system. In symmetric system, there is only 1 key which the key is use for both encryption and decryption of the cipher text. In asymmetric system there are two different keys for encryption and decryption which 1 key is public key and the other 1 is a private key. I also learned the RSA algorithm, which is widely used on the Internet for online banking certificate. It is a very simple algorithm that involves 5 steps to generate the public and private key. However, the advantage of this algorithm is homomorphic multiplicative property that means that without exposing the encrypted data, you will be able to determine if 2 datas are the same.

After this class I have a good understanding of how biometric security works in our daily use gadgets and the secure level of the technology. Moreover, when we are designing a biometric system, there are a lot factors that we will need to consider to make a perfect system for different purpose such as Universality, Uniqueness, Constancy, Collectability, Performance and Acceptability. I think that designing a good system for the real world will be a lot more complex then the systems that we use in school because there are a lot of security professionals or computer science nerds out there that will be breaking your system. For example, in the voice recognition experiment that we did in class, the result seems to be pretty neat since all the participants for this experiment were the students from the class and students tend to just follow the steps that we are told.