6. MULTIMODAL BIOMETRICS BASED AUTHENTICATION AND KEY EXCHANGE SYSTEM

6.1 Introduction

The previous chapters proposed the biocryptosystem techniques, which use the unimodal biometric features like fingerprint, iris and retina. In general, unimodal biometric systems [122] have several issues and limitations such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. Some of these drawbacks can be overcome by using multimodal biometric systems that incorporate the evidence presented by multiple sources of information. Multimodal biometrics can be performed in several ways [123]. Recently, multimodal biometric fusion technique is observed to provide effective and significant results when compared to other multimodal approaches [124]. Therefore, this chapter proposes a novel multimodal biocryptosystem for better security and authentication.

Multimodal biometric system employs two or more individual modalities, namely, gait, face, iris and fingerprint, to enhance the recognition accuracy of conventional uni-modal methods. The multimodal based authentication can aid the system in improving the security and effectiveness in comparison of uni-modal biometric authentication, and it might become challenging for an adversary to spoof the system owing to two individual biometrics traits. In this paper, the
fingerprint and iris are considered for providing mutual authentication between the server and the user. At first, the fingerprint texture features are obtained. Likewise, the texture features are acquired from the iris images by segmentation, estimation of iris boundary and normalization. The extracted texture features the two are then fused at feature level to build the multimodal biometric template. Fusion at the feature level is achieved by means of concatenation, shuffling and merging. Thus the user’s fingerprint and iris images are converted and stored as encrypted binary template, which is used for authentication by the server. Thus the user’s biometric verification data are translated into a secret code and stored in the server’s database during registration. During log-in procedure authentication is done at client and server side without transmitting the biometric measurement from the user to the server. Further the user and the server communicate with each other with a secret session key that is generated from the biometric for the rest of the transactions. This concept can also be applied to strengthen the existing single server password based authentication systems.

6.2 Proposed Multimodal Biometric Systems

In recent times, multimodal biometrics fusion methods have attracted much awareness as the additional information among various modalities could enhance the recognition accuracy. Several techniques have been proposed in this field. In common, they can be separated into three types:
- Fusion at the feature level
- Fusion at the match level
- Fusion at the decision level

In the proposed approach, the fusion at the feature level technique is used. The fusion at the feature level performs the mixing of feature sets equivalent to multiple modalities. As the feature set consists of richer data about the raw biometric data than the match score or the final decision, the integration at this level is estimated to afford better recognition results. On the other hand, the fusion at this level is very hard to achieve in practice because of the following reasons:

- The feature sets of multiple modalities may be incompatible (e.g., minutiae set of fingerprints and Eigen coefficients of face).
- The relationship between the feature spaces of different biometric systems may not be known.
- Concatenating two feature vectors may result in a feature vector with a very large dimensionality leading to the ‘curse of dimensionality’ problem.

When the feature sets are non-homogeneous (e.g., feature sets of different biometric modalities like face and iris), these features can be concatenated to form a single feature set. Feature selection schemes can then be applied to reduce the dimensionality of the resultant feature set. In this proposed technique, fingerprint-iris, fingerprint-retina and retina-iris are used as multi-modal biometrics features. Using the feature level fusion technique, the two biometric features like fingerprint
and iris are fused to obtain a single feature points. Then this feature point is given to the mapping function and authentication protocol.

(i) Feature Extraction of Fingerprint Biometric:

The features of the fingerprint are extracted as described in the chapter 4. The obtained minutiae points are kept as

\[
F_1 = [x_1, x_2, \ldots, x_n]
\]

\[
F_2 = [y_1, y_2, \ldots, y_n]
\]

(ii) Feature Extraction of Iris Biometric:

The features of the iris template are extracted as described in the chapter 5. The obtained minutiae points are kept as

\[
I_1 = [x_1, x_2, \ldots, x_n]
\]

\[
I_2 = [y_1, y_2, \ldots, y_n]
\]

(iii) Feature Extraction of Retinal Biometric:

The features of the retinal tree template are extracted as described in the chapter 5. The obtained minutiae points are kept as

\[
R_1 = [x'_1, x'_2, \ldots, x'_n]
\]

\[
R_2 = [y'_1, y'_2, \ldots, y'_n]
\]
6.2.1 Fusion of Biometric Features

This phase will perform the fusion process for the gathered biometric features. Three types of combinations are possible, namely: Fingerprint-Iris Fusion, Fingerprint-Retina Fusion and Iris-Retinal Fusion. The input to the fusion process will be four vectors: $F_1$, $F_2$, $I_1$ and $I_2$, which are obtained from fingerprint and iris. Similarly, the input vectors for the Fingerprint-Retinal Fusion would be $F_1$, $F_2$, $R_1$ and $R_2$ and for the Iris-Retinal Fusion would be $I_1$, $I_2$, $R_1$ and $R_2$.

The steps involved in Fingerprint-Iris Fusion are as follows:

i. **Shuffling of Individual Feature Vectors:**

The initial step in the fusion process is the shuffling of all the individual feature vectors $F_1$, $F_2$, $I_1$ and $I_2$. The steps for performing the shuffling of vector $F_1$ are:

i. A random vector $R$ of size $F_1$ is created. The random vector $R$ is controlled by the seed value.

ii. For shuffling the $i^{th}$ component of the fingerprint feature vector $F_1$,

a) The $i^{th}$ component of the random vector $R$ is multiplied with a large integer value.

b) The product value resulted is modulo operated with the size of the fingerprint feature vector $F_1$.

c) The obtained value is the index say ‘$j$’ to be interchanged with. The components in the $i^{th}$ and $j^{th}$ indexes are interchanged.
iii. Step (ii) is repeated for all the component of $F_i$. The shuffled vector $F_i$ is indicated as $S_i$.

This procedure is repeated for all other vectors $F_2, I_1$ and $I_2$ and represents as $S_2, S_3$ and $S_4$ respectively, where $S_2$ is shuffled with $F_2$, $S_3$ is shuffled with $I_1$ and $S_4$ is shuffled with $I_2$. The shuffling process results in four vectors $S_1, S_2, S_3$ and $S_4$.

ii. Concatenation of Shuffled Feature Vectors:

The next process is to concatenate the shuffled vectors process $S_1, S_2, S_3$ and $S_4$. In this process, the shuffled fingerprints $S_1$ and $S_2$ are concatenate with the shuffled iris features $S_3$ and $S_4$ correspondingly. The concatenation of the vectors $S_1$ and $S_3$ is performed as follows:

i. A vector $M_1$ of size $|S_1| + |S_3|$ is generated and its initial $|S_3|$ values are filled with $S_3$.

ii. For all the components in $S_1$,

a) The equivalent indexed component of $M_1$ say ‘$t$’ is selected.

b) Logical right shift operation is performed in $M_1$ from index ‘$t$’.

c) The component of $S_1$ is inserted into the emptied $t^{th}$ index of $M_1$.

The above mentioned procedure is performed between shuffled vectors $S_2$ and $S_4$ to obtain a vector $M_2$. In this manner, the concatenation process yields two vectors $M_1$ and $M_2$. 
iii. *Merging of the Concatenated Feature Vectors:*

The final process in creating the biometric template $B_T$ is the merging of two vectors $M_1$ and $M_2$. The process for merging the concatenated feature vectors are provided below.

i. For all the component of $M_1$ and $M_2$,

   a) The components $M_{11}$ and $M_{21}$ are converted into their binary form.

   b) Binary NOR operation is carried out between the components $M_{11}$ and $M_{21}$.

   c) The obtained binary value is then transformed back into a decimal form.

ii. These decimal values are stored in the vector $B_T$ that serves as a biometric template.

Using the feature level fusion technique, the two biometric features such as fingerprint and iris are fused to obtain a single feature point. Then this feature point is given to the mapping function and authentication protocol.

### 6.3 Summary

Multimodal biometric fusion is used in this approach for providing better security. Multimodal biometrics and the need for using it have been discussed in this chapter. Several fusion scenarios have also been studied. Using the feature level fusion technique, the two biometric features such as fingerprint and iris are fused to obtain a single feature point. The features obtained from the biometric
features are combined using fusion techniques. From these fused features, a key is generated by the authentication protocol, which is secuer than any other technique.