Human users find difficult to remember long cryptographic keys. Therefore, researchers, for a long time period, have been investigating ways to use biometric features of the user rather than memorable password or passphrase, in an attempt to produce tough and repeatable cryptographic keys. Our goal is to integrate the volatility of the user's biometric features into the generated key, so as to construct the key unpredictable to a hacker who is deficient of important knowledge about the user's biometrics. In our earlier research, we have incorporated multiple biometric modalities into the cryptographic key generation to provide better security. In this paper, we propose an efficient approach based on multimodal biometrics (Iris and fingerprint) for generating a secure cryptographic key, where the security is further enhanced with the difficulty of factoring large numbers. At first, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used for generating a 256-bit cryptographic key. For experimentation, we have used the fingerprint images obtained from publicly available sources and the iris images from CASIA Iris Database. The experimental results have showed that the
generated 256-bit cryptographic key is capable of providing better user authentication and better security.

Reference

- N. Lalithamani and K.P. Soman, "Irreversible Cryptographic Key Generation from

**Index Terms**

Computer Science  
Security

**Key words**

Biometrics

Multi-modal

Fingerprint

Minutiae points

Iris

Rubber Sheet Model

Fusion

Cryptographic key
Chinese Academy of Sciences Institute of Automation (CASIA) iris database