**ABSTRACT**

The Multimodal Biometric based user authentication systems are highly secured and efficient to use and place total trust on the authentication server where biometric verification data are stored in a central database. Such systems are, prone to dictionary attacks initiated at the server side. In this paper, we propose an efficient approach based on multimodal biometrics (Iris and fingerprint) based user authentication and key exchange system. In this system, minutiae points and texture properties are extracted from the fingerprint and iris images are stored in the encrypted form in the server’s database, to overcome the dictionary attacks mounted by the server. The image processing techniques are used to extract a biometric measurement from the fingerprint and iris. During login procedure the mutual authentication is done between the server and user and a symmetric key is generated on both sides, which could be used for further secure communication between them. Thus meet-in-the middle attack that happens between the user and the server can also be overcome. This system can be directly applied to strengthen existing password or biometric based systems without requiring additional computation.