Abstract
This study analyzes the effectiveness of combining User-Adaptive and Mahalanobis Distance methods in keystroke biometrics authentication systems. Utilizing the Biomey Keystroke Dataset with 40 participants, the study aims to enhance the accuracy and reliability of keystroke-based authentication. The developed system includes enrollment and authentication phases, with User-Adaptive serving as the feature extraction method and Mahalanobis Distance used for feature matching. Decision level fusion techniques are applied to integrate results from various keystroke features. The findings indicate that fusion techniques using Mahalanobis Distance yield better results compared to non-fusion features, with an average error reduction of 8.73%. The optimal vector length (Fn) was found to be at n = 5, with an error rate of 12.07%. The search for the best threshold resulted in a False Acceptance Rate (FAR) of 15.6% and a False Rejection Rate (FRR) of 6% at n = 5. The results demonstrate a lower error rate with an average reduction of 9.9% compared to previous studies. This research validates the potential of Mahalanobis Distance and fusion techniques in improving the accuracy of keystroke biometrics authentication systems, paving the way for the development of more reliable security systems. Further studies are recommended to explore keystroke patterns on touch screens, utilize more diverse datasets, and incorporate real-time testing data.

Keywords: authentication, biometrics, digraph, keystroke dynamic, user-adaptive, mahalanobis distance