Abstract

Biometric technology for identification and authentication is currently being developed and used in everyday life. Biometric technology can use data that comes from patterns when someone types, which is known as keystroke dynamics-based authentication (KDA). KDA's previous research focused on building a KDA system that uses fixed-length text data such as passwords and PINs. However, that method cannot prevent successful impersonators from breaking into the login system. To correct this, a KDA system was examined which uses text data with variable lengths. This study implements the FACT method, which is a biometric authentication system that uses three main features, namely accelerometer (A), touch coordinates (C) and time (T). From the existing data, feature extraction is carried out and then the similarity of the new data is calculated with valid data using the TT measure. The performance of the system built is calculated using the Equal Error Rate (EER). The use of the FACT method is able to produce an average EER of 20.77%. The FACT method is proven to be able to increase the performance of an authentication system based on biometric keystrokes when compared to its basic features, namely features A, C, and T.

Keywords: anomali detection, biometric authentication, FACT, keystroke dynamic, mobile user authentication