Evaluasi *User-Adaptive* Fitur dalam *Keystroke Biometric* menggunakan Beragam Metode *Distance Similarity*

Irsyad Muhamad Al Anshori[1], Prasti Eko Yunanto[2], Farah Afianti[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]irsyadlibra@student.telkomuniversity.ac.id, [2]gppras@telkomuniversity.ac.id, [3]farahafi@telkomuniversity.ac.id,

Abstract

The global smartphone user base is projected to reach 5.25 billion by 2023, increasing the demand for secure authentication systems. While conventional methods like PINs and passwords are easy to implement, they rely on text-based recognition, which poses security risks. As a solution, biometric authentication systems have been introduced. Keystroke biometric, a behavioral-based biometric, has been widely researched and is the focus of this study. This research evaluates user-adaptive features in keystroke biometrics using various distance similarity methods. The keystroke model, built using digraphs that represent key information and typing times (e.g., DD, UD, UU, DU, Duration), is compared to the legitimate user model to determine similarity scores. Performance is evaluated using Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR). The results show that the Euclidean method provides the best performance balance, with the lowest EER of 0.4588 in Scenario I and 0.4598 in Scenario II. Other methods, such as Soergel, Canberra, Matusita, and Manhattan, perform better in preventing impostor acceptance but increase legitimate user rejection risk. Therefore, method selection should be aligned with the priority between security and user convenience in keystroke biometric systems.

Keyword*: biometric, biometric behavioral, keystroke biometric, user-adaptive feature, distance similarity.*