ABSTRACT

Gait is a unique walking pattern for each individual that is influenced by factors such as weight, height, and leg length, among others. One application of gait is as a biometric modality to enhance security. By utilizing Inertial Measurement Unit (IMU) sensors, gait analysis can be leveraged to create a smart-key wearable that is easy to carry, comfortable to use, and protected from potential misuse.

This study aims to develop an identification system that utilizes gait analysis as a method to improve security. Gait data generated by IMU sensors will be collected and processed to identify unique patterns for each individual. A classification model using Hidden Markov Model (HMM) will be developed, and data processing methods in the form of statistical parameters and data segmentation will be applied so that the system can be applied to wearable devices.

Models with 11–15 hidden states and 300 data segments were able to produce a minimum training accuracy of 88.75% across all feature types. However, when implemented in a real-time system, accuracy dropped dramatically to only 11.11%, due to the dominance of data from one subject and differences in conditions between the training and testing processes, such as the types of clothing and footwear used. This indicates that while the model performs well on training data, its generalization ability on new data still needs improvement to ensure the system's reliability in real-time systems.

Keyword: *Gait, IMU sensor, smart-key, wearable device, security, Hidden Markov Model*.