Typing Pattern Analysis for Fake Profile Detection in Social Media

Tapalina Bhattasali; Khalid Saeed

Abstract

Nowadays, interaction with fake profiles of a genuine user in social media is a common problem. General users may not easily identify profiles created by fake users. Although various research works are going on all over the world to detect fake profiles in social media, focus of this paper is to remove additional efforts in detection procedure. Behavioral biometrics like typing pattern of users can be considered to classify genuine profile and fake profile without disrupting normal activities of the users. In this paper, DEEP_ID model is designed to detect fake profiles in Facebook like social media considering typing patterns like keystroke, mouse-click, and touch stroke. Proposed model can silently detect the profiles created by fake users when they type or click in social media from desktop, laptop, or touch devices. DEEP_ID model can also identify whether genuine profiles have been hacked by fake users or not in the middle of the session. The objective of proposed work is to demonstrate the hypothesis that user recognition algorithms applied to raw data can perform better if requirement for feature extraction can be avoided, which in turn can remove the problem of inappropriate attribute selection. Proposed DEEP_ID model is based on multi-view deep neural network, where network layers can learn data representation for user recognition based on raw data of typing pattern without feature selection and extraction. Proposed DEEP_ID model has achieved better results compared to traditional machine learning classifiers. It provides strong evidence that the stated hypothesis is valid. Evaluation results indicate that Deep_ID model is highly accurate in profile detection and efficient enough to perform fast detection.

Keywords

typing pattern, keystroke, mouse click, touch stroke, fake profile deep_ID, social media