Soft Biometrics For Keystroke Dynamics

Syed Zulkarnain Syed Idrus*[1], Estelle Cherrier[1], Christophe Rosenberger[1], and Patrick Bours[2]

[1]Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen (GREYC) – Ecole Nationale Supérieure d'Ingénieurs de Caen, Université de Caen Basse-Normandie, CNRS : UMR6072 – Boulevard du Maréchal Juin - 14050 CAEN Cedex, France

[2]Norwegian Information Security Laboratory (NISlab) – Department of Computer Science and Media Technology, Gjøvik University College, P.O.Box 191, N-2802 Gjøvik, Norway

Abstract

Keystroke dynamics is a viable and practical way as an addition to security for identity verification. It can be combined with passphrases authentication resulting in a more secure verification system. This paper presents a new soft biometric approach for keystroke dynamics. Soft biometrics traits are physical, behavioral or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color etc.). Those attributes have a low discriminating power, thus not capable of identification performance. Additionally, they are fully available to everyone which makes them privacy-safe. Thus, in this study, it consists of extracting information from the keystroke dynamics templates with the ability to recognise the hand(s) used (i.e. one/two hand(s)); the gender; the age category; and the handedness of a user when he/she types a given password or passphrase on a keyboard. Experiments were conducted on a keystroke dynamics database of 110 users and our experimental results show that the proposed methods are promising.

*Speaker