Abstract No: SC-03 **Smart Computing**

Handwritten signature verification

***H. M. H. P. Abewardana and L. Ranathunga**

Faculty of Information Technology, University of Moratuwa, Sri Lanka
**hasi.prasanga@gmail.com*

Abstract

A number of biometric methods can be used to authenticate a human identity such as using fingerprint detection, face detection, iris inspection and voice recognition. The verification of the signature of a human is the most prominent and prevalent method among those. The banking and insurance sector manually uses this verification method. It is a critical biometric attribute, which may differ from time to time due to the age and emotional state of the person. Because of the absence of the time feature of the signature, offline signature verification has a risk than online signature verification. The paper introduces six features for an alternate solution. They include scale and rotation invariant such as signature pixel ratio of concentric circles and number of cross points while others are rotation variant such as baseline slant angle, aspect ratio, normalized area and slope of the line connecting center of gravities of left and right halves of the bounding box of the signature. Back-propagation neural network is used to train and test the signature images. Experimentation and results of this methodology presents the possibility of using this system in relevant sectors.

Keywords: ANN, Feature extraction, Forgeries, Image processing, Offline signature verification

Introduction

Signature of a particular person is a unique behavioral biometric feature used to identify a particular individual. The identity is crucial in most sectors but is very important in the finance and banking context. Many advantages are there for using personal signature as the primary authenticity because the signature is not needed to be stored in a particular place. Therefore, the signature cannot be stolen and not forgotten, as in the case of using passwords. However, the use of human signature is not a completely fool proof mechanism. Mimicing of someonelse's signature is a frequent issue that is faced by organizations. There are three types of forgeries, namely random, simple and skilled (Zaher & Abu-rezq, 2010). The forger has no idea about the name and the style of the signature in random forgery and it take less effort to identify it. In simple forgery name of the signature is known without knowing the style of it and this is most widespread. The forger has the name and the style of the signature in skilled forgery and this is most difficult to identify. However, there are three methods according to the data acquisition variations to identify and verify personal signature, which are called online, offline or hybrid signature verifications. In online signature verification, dynamic features, such as pressure, angle, number of pen lifts and time taken are taken are measured with the help of a digitizing tablet and a pen (Kumar & Dhandapani, 2016). For simplicity and user friendliness use of offline signature verification process is most common.

The following approaches are used for signature verification. Euclidean distance between questionable signature image and corresponding template (Zaher & Abu-rezq, 2010); Window-formed skeleton (Zimmer & Ling, 2003); Circle Masking Model (CCM) (Kumar & Dhandapani, 2016); Longest Common Subsequence algorithm (Salama & Hussein, 2016); Cumulative Distribution Function (CDF) (Devnath & Islam, 2016). Twenty five percent of of a data set in an offline signature