Online Signature Recognition

Indrani Chakravarty
Indian Institute of Technology, India

Nilesh Mishra
Indian Institute of Technology, India

Mayank Vatsa
Indian Institute of Technology, India

Richa Singh
Indian Institute of Technology, India

P. Gupta
Indian Institute of Technology, India

INTRODUCTION

Security is one of the major issues in today's world and most of us have to deal with some sort of passwords in our daily lives; but, these passwords have some problems of their own. If one picks an easy-to-remember password, then it is most likely that somebody else may guess it. On the other hand, if one chooses too difficult a password, then he or she may have to write it somewhere (to avoid inconveniences due to forgotten passwords) which may again lead to security breaches. To prevent passwords being hacked, users are usually advised to keep changing their passwords frequently and are also asked not to keep them too trivial at the same time. All these inconveniences led to the birth of the biometric field. The verification of handwritten signature, which is a behavioral biometric, can be classified into off-line and online signature verification methods. Online signature verification, in general, gives a higher verification rate than off-line verification methods, because of its use of both static and dynamic features of the problem space in contrast to off-line which uses only the static features. Despite greater accuracy, online signature recognition is not that prevalent in comparison to other biometrics. The primary reasons are:

- It cannot be used everywhere, especially where signatures have to be written in ink; e.g. on cheques, only off-line methods will work.
- Unlike off-line verification methods, online methods require some extra and special hardware, e.g. electronic tablets, pressure sensitive signature pads, etc. For off-line verification method, on the other hand, we can do the data acquisition with optical scanners.
- The hardware for online are expensive and have a fixed and short life cycle.

In spite of all these inconveniences, the use online methods is on the rise and in the near future, unless a process requires particularly an off-line method to be used, the former will tend to be more and more popular.

BACKGROUND

Online verification methods can have an accuracy rate of as high as 99%. The reason behind is its use of both static and dynamic (or temporal) features, in comparison to the off-line, which uses only the static features (Ramesh & Murty, 1999). The major differences between off-line and online verification methods do not lie with only the feature extraction phases and accuracy rates, but also in the modes of data acquisition, preprocessing and verification/recognition phases, though the basic sequence of tasks in an online verification (or recognition) procedure is exactly the same as that of the off-line. The phases that are involved comprise of:

- Data Acquisition
- Preprocessing and Noise Removal
- Feature Extraction and
- Verification (or Identification)

However, online signatures are much more difficult to forge than off-line signatures (reflected in terms of higher accuracy rate in case of online verification methods), since online methods involve the dynamics of the signature such as the pressure applied while writing, pen tilt, the velocity with which the signature is done etc. In

case of off-line, the forger has to copy only the shape (Jain & Griess, 2000) of the signature. On the other hand, in case of online, the hardware used captures the dynamic features of the signature as well. It is extremely difficult to deceive the device in case of dynamic features, since the forger has to not only copy the characteristics of the person whose signature is to be forged, but also at the same time, he has to hide his own inherent style of writing the signature. There are four types of forgeries: random, simple, skilled and traced forgeries (Ammar, Fukumura, & Yoshida, 1988; Drouhard, Sabourin, & Godbout, 1996). In case of online signatures, the system shows almost 100% accuracy for the first two classes of forgeries and 99% in case of the latter. But, again, a forger can also use a compromised signature-capturing device to repeat a previously recorded signature signal. In such extreme cases, even online verification methods may suffer from repetition attacks when the signature-capturing device is not physically secure.

MAIN THRUST

Although the basic sequence of tasks in online signature verification is almost the same as that of off-line methods, the modes differ from each other especially in the ways the data acquisition, preprocessing and feature extraction are carried out. More specifically, the submodules of online are much more difficult with respect to off-line (Jain & Griess, 2000). Figure 1 gives a generic structure of an online signature verification system. The online verification system can be classified into the following modules:

- Data Acquisition,
- Preprocessing,
- Feature Extraction,
- Learning and Verification.

Data Acquisition

Data acquisition (of the dynamic features) in online verification methods is generally carried out using special devices called transducers or digitizers (Tappert, Suen, & Wakahara, 1990, Wessels & Omlin, 2000), in contrast to the use of high resolution scanners in case of off-line. The commonly used instruments include the electronic tablets (which consist of a grid to capture the x and y coordinates of the pen tip movements), pressure sensitive tablets, digitizers involving technologies such as acoustic sensing in air medium, surface acoustic waves, triangularization of reflected laser beams, and optical sensing of a light pen to extract information about the number of strokes, velocity of signing, direction of writing, pen tilt, pressure with which the signature is written etc.

Preprocessing

Preprocessing in online is much more difficult than in off-line, because it involves both noise removal (which can be done using hardware or software) (Plamondon & Lorette, 1989) and segmentation in most of the cases. The other preprocessing steps that can be performed are signal amplifying, filtering, conditioning, digitizing, resampling, signal truncation, normalization, etc. However, the most commonly used include:

- **External Segmentation:** Tappert, Suen and Wakahara (1990) define external segmentation as the process by which the characters or words of a signature are isolated before the recognition is carried out.
- **Resampling:** This process is basically done to ensure uniform smoothing to get rid of the redundant information, as well as to preserve the required information for verification by comparing

Figure 1. Modular structure of a generic online verification system