Noctis: Descriptive Statistical Signature Recognition System

Andrea Sergas, Donato Meoli
Department of Computer Science
University of Bari "Aldo Moro"
70125 Bari, Italy
{a.sergas d.meoli1}@studenti.uniba.it

Abstract

We present a recognition system for online handwritten signature verification based on a descriptive statistical approach. Centrality and dispertion indices are the main focus for features extraction. Support Vector Machines are used for the train phase; in particular, there is a biunivocal correspondence between the SVMs and the users. FRR and FAR are, respectively, 3,35% and 4,35%.

1. Introduction[1]

Biometric authentication is gaining popularity as a more trustable alternative to password-based security systems. Signature is a behavioral biometric: it is not based on the physical properties, such as fingerprint or face, of the individual, but behavioral ones. As such, ones signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signatures widespread acceptance by the public make it more suitable for certain lower-security authentication needs.
Signature verification is split in two approaches, according to the input type of data:

(i) offline (static) signature verification takes as input the image of a signature; it is useful in automatic verification of signatures found on bank checks and documents;

(ii) online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature, in addition to its shape.

Dynamic features include the overall speed of the signature, the pen pressure at each point and other similar data. They make the signature more unique and difficult to forge. As a result, online signature verification is more reliable than offline signature verification.
In an online signature verification system, users are first enrolled by providing signature samples, called reference signatures. Then, when a user presents a signature claiming to be a particular individual, the test signature is compared with the reference signatures for that individual. If the similarity is under a certain threshold, the user is rejected, otherwise authenticated.

2. Features Extraction

For each signature the features extracted are represented as a vector of local and global statistical features:

$$S_i = \langle \mu(d_i), \mu(v_i), \mu(a_i), \mu(\Delta p_i), \mu(\Delta t_i), \mu(an_i), \mu(an_{0_i}),$$

$$\sigma(d_i), \sigma(v_i), \sigma(a_i), \sigma(\Delta p_i), \sigma(\Delta t_i), \sigma(an_i), \sigma(an_{0_i}), t, l \rangle$$

where μ is the **mean** - *centrality* index - and σ is the **standard deviation** - *dispersion* index.
Only mean and standard deviation are considered to make a drastic reduction of redundant data to pass to the classifier by reducing each feature to only one significant and discriminating value. For each signature of the user, the basic data which are provided by SUSIG dataset are:

(i) x coordinate: scaled cursor position along the x-axis;

(ii) y coordinate: scaled cursor position along the y-axis;

(iii) timestamp: system time at which the event was posted;

(iv) pressure: adjusted state of the normal pressure in milliseconds;

while, starting with these, the following features are extracted:

(i) displacement:

$$d_i = \begin{cases} \sqrt{(x_{i+1}-x_i)^2+(y_{i+1}-y_i)^2} & 1 \le i \le n-1 \\ d_n - d_{n-1} & i = n \end{cases}$$

(i) velocity:

$$v_i = \begin{cases} \frac{d_i}{t_{i+1}-t_i} & 1 \le i \le n-1 \\ v_n = v_{n-1} & i = n \end{cases}$$

(ii) acceleration:

$$a_i = \begin{cases} \frac{v_i}{t_{i+1}-t_i} & 1 \le i \le n-1 \\ v_n = v_{n-1} & i = n \end{cases}$$

(iii) angle between two consecutive points:

$$an_i = \begin{cases} \arctan(y_{i+1}-y_i, x_{i+1}-x_i) & 1 \le i \le n-1 \\ an_n = an_{n-1} & i = n \end{cases}$$

(iv) angle between a point and the origin:

$$an_{0_i} = \arctan(y_i - 0, x_i - 0) \quad 1 \le i \le n$$

(v) pressure variations between two consecutive points:

$$\Delta p_i = p_{i+1} - p_i$$

(vi) time variations between two consecutive points:

$$\Delta t_i = t_{1+1} - t_i$$

(vii) total time:

$$t = \sum_{i=1}^{n} t_i$$

(viii) total path length:

$$l = \sum_{i=1}^{n} d_i$$

where n is the number of the samples for each data in the user's signatures representation.

3. Train And Tuning Phase

3.1. Train Phase

For the users' signatures modeling phase it has been used one Support Vector Machine for each user. The train set for each SVM has been mostly auto generated: from the 10 genuine signatures' features vectors other 80 features vectors have been created by adding small noises, in order to maintain consistency.

No forgery signatures' features have been used in the train set. Because of the features' statistical nature, it is possible to generate noise maintaining some certain amount of consinstency by multiplying the given genuine features by a certain number of certain multipliers. The solution is given by creating a linearly spaced vector. Supposing that the creation of the vector is a function with three parameters: range start, number of elements and range end, then it has been empirically proven that the best consistency for the generation of genuine features, for n genuine signatures, is given by:

(i) *range start* to be 1, so that the first n signatures are the ones in the given dataset;

(ii) *number of elements* to be n - 1;

(iii) *range end* to be the lower integer nearest to:

$$\frac{number\,of\,elements}{2} \cdot 0.1$$

3.2. Tuning Phase

In order to set a specified threshold for each user right after the train phase 90 features vectors have been created by adding each feature used in the train set by the variance of that signature's features, excluding total time and total path.
The user's threshold is then obtained by getting the maximum score predicted from the trained SVM given the 90 auto-generated features vectors. A small constant is then added: the obtained threshold represents an average forgery signature's score.

4. Results

4.1. SUSIG Dataset[2]

For the train and test phases it has been used an online handwritten signature database called SUSIG, which collects signatures for 94 person classified in two classes:

(i) 20 *genuine* signatures for user divided in two sessions:

  (i) *session 1* for the train phase;

  (ii) *session 2* for the test phase.

  and vice versa in the 2-fold cross-validation approach used.

(ii) 10 *forgery* signatures for user divided in two classes:

(i) *skilled* forgery is signed by a person who has had access to a genuine signature for practice;

(ii) *highly skilled* forgery is signed is signed by a signatures' forgery professionist who has had access to a genuine signature for practice.

4.2. Baseline Evaluation

For the sake of comprehension, another system has been evaluated without using the statistical approach. In this case the features vectors are composed by all the values given in the dataset, with no further preprocessing. The results are the following:

(i) *False Acceptance Rate* of forgery signatures which is defined as:

$$FAR = \frac{Number\,of\,accepted\,forgery\,attempts}{Total\,number\,of\,forgery\,attempts} \approx 1,54\%$$

(ii) *False Rejection Rate* of genuine signatures which is defined as:

$$FRR = \frac{Number\,of\,rejected\,legitimate\,attempts}{Total\,number\,of\,legitimate\,attempts} \approx 23,94\%$$

4.3. Noctis Evaluation

In evaluating the performances of a signature verification system, there are two important factors:

(i) *False Acceptance Rate* of forgery signatures which is defined as:

$$FAR = \frac{Number\,of\,accepted\,forgery\,attempts}{Total\,number\,of\,forgery\,attempts} \approx 4,35\%$$

(ii) *False Rejection Rate* of genuine signatures which is defined as:

$$FRR = \frac{Number\,of\,rejected\,legitimate\,attempts}{Total\,number\,of\,legitimate\,attempts} \approx 3,35\%$$

5. Future Development

This recognition system can be further improved by following two approaches, independent one from the other:

(i) using a signature dataset which provides *more features* about signatures such as:

(i) *azimuth*: clockwise rotation of cursor about the z-axis;

(ii) *altitude*: angle upward toward the positive z-axis;

(ii) using *hyper-parameterization algorithms* which prevent the phenomenon of overfitting through the use of the learning rate in a preventive manner: the system, at each step of optimizing its loss function, declines the learning rate.

References

[1] D. Impedovo, Models and Methods for Application Security course, 2017

[2] SUSIG, http://biometrics.sabanciuniv.edu/susig.html, 2009