Handwritten Signature Verification: the State of The Art

Anastasia Beresneva, Anna Epishkina, Sergey Babkin, Alexey Kurnev and Vladimir Lermontov
National Research Nuclear University (Moscow Engineering Physics Institute), Moscow, Russia
anastasiya3161@gmail.com, AVEpishkina@mephi.ru, ssbbkn@ya.ru, simpleman383@gmail.com, 0rhast0@gmail.com

Abstract
Nowadays handwritten signature and its verification is utilized in a lot of applications including e-commerce. An analysis of verification algorithms and areas of their practical usage is provided. The focus of the investigation is on verification method based on neural network. This type of verification algorithm is realized as a mobile application and its main characteristics are obtained. The directions of further work are concluded including a modification of an algorithm and its realization in order to remove its disadvantages.

Keywords: **handwritten signature, verification, neural network, mobile application**

1 Introduction

Currently, the task of verification or identification of the user is one of the priority tasks in the field of information security. The most promising algorithms of verification based on the use of personal biometric data: fingerprints, iris, retina, DNA, handwriting signature. Verification a handwritten signature is a biometric technology that uses the signed for identification purposes with the aim of establishing the authority for making automated transactions, obtaining access to computer terminals, or physical access to the controlled area. Signatures are particularly useful for identification because the signature of each person is unique, especially if along with a static form are considered her dynamic performance. These features include time stamping the signature, size, speed, number of segments and the pressing force of the pen. Verification of a handwritten signature can be used to ensure the security of financial transactions. If the verification algorithm is guaranteed to be able to determine the identity of the signatory, a handwritten signature will replace e-due to more simple and human-readable mechanism for placing signatures.

In addition, such verification will be used in mobile application security. Modern mobile devices have the necessary hardware for online verification of a handwritten signature. Such identification does not require memorizing passwords or PIN codes, however, can provide the necessary level of security.

The rest of the paper is organized as follows. In section 2 we consider related works. In section 2 we consider related works. Section 3 is devoted to analysis of the main verification algorithms. In addition, the section considers the implementation of algorithms and test results. We give the conclusion and future research directions in section 4.

2 Related Works

Nowadays there are few approaches to handwritten signature verification. Algorithms of verification a handwritten signature can be divided into two groups:

- Online verification algorithms;
- Offline verification algorithms.

The system uses online verification algorithms can be implemented using graphical tablets and mobile devices to retrieve dynamic characteristics in the process of entering the signature. System based on algorithms offline verification, use only the static characteristics of signatures that are extracted from the image.

Nowadays developed several different approaches to the problem of verification a handwritten signature. Autonomous system of signature verification presented in [1], built on the basis of several statistical methods, in particular, uses hidden Markov models (HMM) in building reference model for each local object. A hidden Markov model consists of a sequence of states $S_1,...,S_n$ which are associated by probabilistic transitions with probability p_{ij}, i.e. the probability of transition from i -th state to j -th. Possible transitions only to the next state or looping. Each time the model performs a probabilistic transition from one state to another or in the same condition. Thus, there is a vector of observations y_k with the output probability distribution of $b_n(y_k)$ corresponding to the specific condition. This approach defines two concurrent random process, one of which is the main and unobservable (i.e., the sequence of HMM-States). Judge it is possible only with the help of another random process, i.e. a sequence of observations.

In the verification algorithm of a probabilistic comparison of the sample and the signature is based on the HMM. The signing process is modelled with several States that constitute a Markov chain. Each of these States corresponds to a separate part of the signature described by a set of characteristics that are not observed directly (i.e. hidden). There are only local features of a signature (such as tangents of angles). The observed data are associated statistically with state models and conditionally independent in each state. When training the model parameters are estimated for the set that contains the authentic signature. During verification, we compute the probability that the signature is genuine.

If this probability exceeds the threshold, the signature is accepted, otherwise it is considered tampered with. This approach can be viewed as a statistical conformity check of the signature and the signature based on the HMM.

Another system proposed in [2] was based on machine learning. For the application of machine learning for verification of signatures also required the training sample. In the process study examined the possibility of applying such algorithms as KNN classification algorithm [2], support vector machines, and logistic regression analysis. However, machine learning is on example of these algorithms has a major drawback for accurate recognition, the training required for a much larger sample than for the algorithm based on neural network.

In [3] described a technique for verification of signatures, which was based on the use of neural networks. For each object, it sets a special two stage perceptron and introduced structural classification. The application technology of neural networks is widely accepted to solve such kind of problems. It is possible to allocate following advantages of using neural networks to verify the signature:

- Class of multilayer networks as a whole can represent any desired function in the form of a set of attributes, and signatures can easily be modelled as a function from the set of characteristics;
- Neural networks are an excellent tool to summarize and help to cope with the diversity and variations inherent in handwritten signatures;
- Neural networks are very tolerant to noise in the input data;
- The performance of a neural network gradually decreases with a sharp deterioration in conditions of recognition.

3 Analysis of the Main Verification Algorithms

Common online verification algorithm of a handwritten signature consists of the following steps:

- Obtaining source data using the hardware;
- Preprocessing of the handwritten signature;
- Extraction of the characteristics of a handwritten signature;
- Build a model of a signature on its characteristics;
- Computation of the similarity measure of the test signature to the sample;
- The decision on the authenticity of the signature.

The advantages of using dynamic features in that they are much more difficult to forge because they are not visible when reviewing a paper copy of the signature.

The test results of the algorithms verify the signature is represented in a ratio of type I error and type II error. Type I error associated with denial of access to legitimate user, type II error – of a false identification.

Used for further processing signature:

- Graphic display (in graphic or vector form);
- Number of touches;
- Temporal characteristics (minimum, maximum, average, total time without lifting the pen from the screen);
- The characteristics of the pen movement speed (minimum and maximum values of the projections of the velocities on the axis and module speed).

Analyzed the following approaches, allow for the verification of handwritten signatures:

- KNN algorithm;
- Range Classifier algorithm;
- Algorithm based on hidden Markov models;
- The simplest perceptron neural network.

The KNN classification algorithm [2] (*k*-nearest neighbor), the input accepts a vector containing the values of the characteristics of the signature, and the output issues a decision, a genuine signature or a forgery. To classify each of characteristics from the training samples, you must execute the following operations:

- Calculate the distance to each of objects of training set;
- To select k objects in the training set, the distance to which is minimal.

Next, a decision is made, if the characteristics are within acceptable tolerances. This algorithm has the following disadvantages:

- Low accuracy;
- Type I error and type II error at turns, scaling, shifts the signature.

Range Classifier algorithm verify the signature consists of the following steps:

- For each signature is calculated the centroid
- For each signature vector is formed from the angles and lengths of the radius vectors from centroid to each point
- Overlap of a sequence of test vectors of the training sample feature with an error.
- Determined the range of values of each vector according to the training sample

If the threshold number of parameters within the specifications and applying vectors match, the signature is determined genuine.

Algorithm based on hidden Markov models input also accepts a vector of characteristics of the signature, they are as follows:

- The signing process is modelled with several States that constitute a Markov chain;
- Each of these states corresponds to a separate part of the signature that are not observed directly (i.e. hidden);
- The observed data are associated statistically with state models and conditionally independent in each state;
- When training the model parameters are estimated for the set that contains the authentic signature.

At the time of verification to calculate the probability that the signature is genuine. If this probability reaches a preset threshold, the signature is accepted, otherwise, it is rejected. This approach can be viewed as a statistical conformity check signatures and signatures based on hidden Markov model.

The following algorithm is neural network, it takes the input vector containing the values of the characteristics of the signature. It has 12 inputs, 2 hidden layers of 6 neurons each and 1 output. The network operates on the principle of "learning with a teacher".

In the first stage to the inputs of the neural network serves signature:

- The proportion of matching points in the vector sequence;
- The temporal characteristics (total time, maximum, minimum and medium time without interruption);
- Number of breaks pen;
- Projections of the minimum and maximum speeds on the coordinate axes;
- Modules maximum and minimum speed.

Then, the logistic activation function sets the weight of the synapses of the neural network. After that, the signature is deemed to be correct if the output of the neural network value is greater than threshold

This verification algorithm is recognition accuracy and insensitivity to changes in scale and offset of the signature. However, this algorithm showed the most accurate results for the task of verification.

The algorithms were implemented in the form of a Java mobile application for the Android platform. While testing a sample of 100 signatures for the considered algorithms the obtained results are shown in Table 1. All implemented algorithms are based on prior learning. The user makes several signatures from which to retrieve the necessary characteristics. Each handwritten signature of the user is different from the previous one. As a result, some characteristics, such as changing speed, different dimensions or the collars of the pen must be removed from several samples of the signature to account possible error. The extracted features from digitized signatures are stored in a matrix, and then can be used for verification.

Algorithm	Type I error	Type II error	Computation time, ms
KNN algorithm	0.13	0.20	3.37
Range Classifier	0.04	0.20	5.17
Hidden Markov Model based algorithm	0.10	0.17	4.80
Neural Network	0.08	0.12	2.16

Table 1: The results of testing the developed algorithms

4 Conclusion

The study revealed that the most promising methods for further work is the algorithm based on hidden Markov model and neural network, since the proportion type I and type II errors for these algorithms is minimal relative to the others. In addition, they are less sensitive to noise and can be scaled. In the future studies on this topic assume to develop an improved algorithm for verification of a handwritten signature, taking into account the pressing force of the pen, reduce the number of errors and time of learning.

Acknowledgement

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Kashi, R.S., Hu, J., Nelson, W.L., Turin, W. (1997). On-line Handwritten Signature Verification using Hidden Markov Model Features», in *IEEE Proceedings 4th International Conference Document Analysis and Recognition*, pp. 253-257.

[2] McCabe, A., Trevathan, J., Read, W. (2008). Neural Network-based Handwritten Signature Verification, in *Journal of Computers*, Vol.3, No. 8, pp. 9-22.

[3] Beatrice, D., Thomas, H. (2015). *On-line Handwritten Signature Verification using Machine Learning Techniques with a Deep Learning Approach, Master's Theses in Mathematical Sciences*.