Handwritten Signature Verification Service

Sophia Vdovkina, Sergey Shibanov
Software and Computer Applications Department, Faculty of Computer Engineering
Penza State University
40 Krasnaya Str., Penza, 440026, Russian Federation
sophia.vdovkina@gmail.com, serega@pnzgu.ru

***Abstract*—The problem of implementing an online handwritten signature verification service for person identification in various information systems is considered in this article. As part of the service, an API for feature extraction, registration and verification of handwritten signatures has been developed. At the registration stage, the user and his reference signature are initialized on the service. At the verification stage, the submitted handwritten signature is compared with the template stored in the service database, and the probability of the entered signature being genuine is calculated. An experiment was conducted to assess the accuracy of identity verification with a handwritten signature. DeepSignDB was chosen as a test base in the experiment.**

***Index Terms*—handwritten signature verification, RESTfull architecture, signature verification library, MVP**

I. Introduction

From a practical point of view, a biometric system is a pattern recognition system that recognizes the identity of a user based on physiological (fingerprints, retina, vein pattern, face) or behavioral (signature, voice) characteristics. Biometric systems operate in two modes - identification and verification. In the identification mode, it is determined which user among the entire set of known users provides a biometric parameter (which is known to be correct). Verification mode checks whether the biometric parameter was provided by a specific known user or is a forgery.

Handwritten signature verification is one of the most common methods for identifying a person. Signature verification is actively used in workflow automation, for example, in application to government agencies, in banking or litigation. The main advantage of a handwritten signature for personal identification is a high index of trust among people. After implementing automatic handwritten signature verification into any business the usual workflow does not change significantly and is easily introduced into office work. Therefore, it is relevant to develop and put into practice permanently available handwritten signature verification services that will help automate the process of personality recognition for various fields of application. Such services can be targeted at interested individuals and organizations whose tasks include, among other things, registration and identification of a person by handwritten signature, in relation to customers, employees, contractors and other individuals. Such services can be targeted at individuals and organizations whose tasks include registration and identification of a person by handwritten signature, the technology can be applied to customers, employees, contractors and other individuals.

We can distinguish two types of signature verification: offline (static) or online (dynamic). In offline mode, a person signs on paper, after the signature is scanned or photographed the system extracts signature parameters from its image. In online mode, a person signs on a device (for example, a graphics tablet), while the system captures additional information (time, pressure, azimuth, etc.). Online signature verification methods are significantly superior to offline verification methods in terms of the quality of results.

In the online signature verification mode, functional and parametric methods of handwritten signature processing are used. In the functional approach, the signature is represented as a function of time, the values of which can be, for example, coordinates, speed, pressure, etc. In the parametric approach, the signature is represented as a vector, the elements of which correspond to individual characteristics (parameters) of the signature.

The characteristics of the signature in the parametric approach are divided into local and global. The local parameters describe each individual signature point. Global parameters describe the signature as a whole and the process of writing it, for example, the total elapsed time, average pressure, average speed, etc.

Handwritten signature representation methods, the quality and completeness of the obtained signature characteristics have a significant impact on the choice of a signature recognition algorithm. One of the most important tasks of signature recognition software is to support multiple verification algorithms and select the most efficient algorithm. In the course of the conducted research and development, a comparative analysis of modern software products, methods and algorithms for verifying a handwritten signature was carried out.

II. Project relevance

The project is dedicated to solve the problem of developing an online service for verifying a handwritten signature for personal identification in various areas of human activity (public services, banking, litigation, filing documents in organizations, etc.). Despite the achievements and developments in this area, the problem remains relevant for a number of reasons. These include the variety of approaches and algorithms for verifying a handwritten signature, the multi-criteria and non-triviality of choosing the most effective approach and algorithm. It is also worth noting the limitations of software products and solutions of this class. The complete absence of cross-platform products

with open source code, capable of development and adaptation by third-party developers, taking into account their own goals and objectives, specifics of the subject area.

III. State of the art

Modern works on the research topic can be divided into two main groups: 1) research and improvement of methods for verifying a handwritten signature; 2) development of software tools for identification and verification of a handwritten signature.

A. Research

Theoretical work in the field of handwritten signature verification is mainly related to the study and improvement of the verification methods themselves. Methods for online verification of a handwritten signature can be divided into three main categories [1]: pattern matching methods, statistical methods, structural methods.

In pattern matching methods, verified signature is matched against signature patterns. In particular, A. K. Jain et al. [2] used the method of comparing trajectories, which was previously used for recognition of handwritten characters. Comparison of full time sequences results in a higher computational load, as well as loss of information related to the structural organization of signatures. Asymmetric DTWs have been developed to avoid deformation of reference signatures when compared with test samples [3], [5]. Despite the fact that DTW was first proposed for signature verification a long time ago, it is still popular and many articles are devoted to its improvement [4]–[7], [10], [15], [19].

Statistical methods evaluate one or more parameters calculated by statistical algorithms. When using a parametric approach to signature representation, statistical signature verification methods are used, such as neural networks [8], hidden Markov models (HMM) [9], [11], support vector machine (SVM), random forest algorithm, nearest neighbors method. The most common statistical algorithms use Mahalanobis and Euclidian distances. When calculating the Mahalanobis distance, the full covariance matrix is considered for each set of signatures [12]. When using the Euclidean distance, the average value for the set [13] is considered.

Currently, several different topologies of hidden Markov models have been implemented: hidden Markov models with left-right topology [11], [20], [21], ergodic [22], ring, in which the transition from the last state to the first state is allowed, but the latter topology is more used in offline verification.

Support Vector Machines (SVM) is a classification technique in the field of statistical learning theory that has been successfully used in many applications for pattern recognition. SVM can map input vectors to a higher dimensional space where classes are defined by a maximum separating hyperplane [26].

The use of neural networks in the field of signature verification was difficult for a long time, since there was not a large enough database available for researchers to train models, since signatures are not information publicly available on the Internet, like other biometric characteristics, for example, faces [14]. Currently, there is great progress in this area, researchers have proposed LSTM networks [15], RNN [16], Siamese networks [17], MLP [18], CNN [19], TA-RNN [14].

Structural signature verification methods include string, graph, and tree matching methods that are commonly used in combination with other methods. For example, string matching [2], [23] can be used in combination with a neural network approach [22]. In some studies, the structural description graph is used to check the structural organization of a dubious signature [24]–[26].

Online signature verification methods are noticeably getting more complicated and improve their quality. Currently, the latest developments in the field of machine learning are actively used. The quality of the models is also improving due to the availability of more databases for researchers. In the development of signature verification, there is a tendency to switch to the use of complex neural network models, and the number of studies on this topic will clearly prevail in the coming years.

B. Software

Among the most well-known software tools for identifying and verifying a handwritten signature are Wacom Ink SDK for verification from Wacom[1], solutions from Progress Soft[2][3], SIGNificant from Namirial S.p.A.[4]

a) The Wacom Ink SDK: The Wacom Ink SDK for verification software is a set of paid handwritten signature verification software tools that supports two verification modes that can be used individually and/or in combination:

1) Dynamic verification of the signature by comparing with 4-12 reference versions of the signature;
2) Static verification after the fact by comparing signature images with images of known samples.

The SDK validator compares the incoming signature with signature reference instances that must have been previously registered in the database. The reference signature template can be updated. It is possible to adjust the tolerance of the program to forgery signatures, for example, to increase the probability of accepting a signature, sacrificing a growing type II error.

b) Progress Soft solutions: Progress Soft offers two paid specialized solutions for verification of handwritten signatures aimed at financial institutions (banks, fund companies, etc.):

1) Solution "Automated Verification and Signature Management" (PS-SIG) automates the process of verifying signatures and provides tools for extracting from the database, managing and storing an unlimited number of signatures. PS-SIG allows financial institutions to

[1]https://www.wacom.com/ru-ru/for-business/products/will-sdk-for-verification

[2]https://www.progressoft.com/ru/products/signature-verification-recognition/ps-asv

[3]https://www.progressoft.com/ru/products/signature-verification-recognition/ps-sig

[4]https://www.xyzmo.com/e-signature-products/signature-verification

display withdrawal limits and account limits that limit the rights of each signatory. In addition, during signature verification, the solution automatically checks the signer's credentials. PS-SIG includes a client profile module that stores signatures and customer data for financial institutions. The solution allows a bank employee to maintain signature cards and manage customer signatures, as well as set account limits and payment rules.PS-SIG stores all changes to the data for each instance of the signature and determines the expiration date for each signer. Users of the PS-SIG solution can perform various actions in the system with two levels of authorization: "creator" and "verifier";

2) The Automated Signature Verification (PS-ASV) compares signatures extracted from electronic checks or official documents with existing samples of genuine signatures. The PS-ASV solution works in automated mode and uses pattern recognition algorithms, in particular machine learning, to match signatures. Acceptance or rejection of the extracted signature is based on the security policies and procedures of the financial institutions.

c) SIGNificant: Paid product SIGNificant from Namirial S.p.A. designed to collect behavioral biometric data of a handwritten signature (speed, acceleration, rhythm, air movements and pressure) and embed the signature in an electronic document. Up to six signatures are needed to register the user. The system can handle multiple profiles for each user, allowing, for example, one profile to be used for a standard signature and another for a signature with only initials.Each time a user accesses the system to verify their signature, the biometric server compares the current signature against signature profiles. With each authentication, the server continues to learn and configure the user's profile. This allows the system to track gradual changes in the handwritten signature over time. The result of the automatic signature verification is provided as a signed response, which guarantees its authenticity.

It can be concluded that the considered software products have basic functions for verifying a handwritten signature. However, the following problems and limitations of these products should be noted:

1) limited integration with third-party applications and systems;
2) the lack of opportunities for the development of applications by third-party developers to adapt them to the specifics of their own tasks and features of subject areas;
3) paid licenses for the distribution of products and the absence of open source code.

IV. Software implementation

A. The main goals

The main goal of the online handwritten signature verification service is to provide a convenient API for implementation in any information system. To compile a virtual image of a signature, a person needs to provide several examples of it (5-15 examples). After that, he is registered in the system. After his registration, the organization that provided the data of the individual has the right to send a request for the verification or identification of this person. An organization can also request a signature template for a specific person. Thus, by registering a signature, the system initializes the user in the database for the first time. Verification compares already known data about the user with the provided signature and calculates the probability that the entered signature belongs to the user. During identification, a multi-class classification occurs among all users of the system, i.e., user data is displayed based only on his signature.

RESTful architecture will be used to create these services.

B. Software structure

To meet all the requirements of the handwritten signature verification application market, the following requirements for the application have been highlighted:

1) Organization can register, verify or identify any individual;
2) Organization can re-register a person's signature if it was changed;
3) Organization can request template signatures of an individual;
4) Administrator can change the entry threshold of any user and delete signatures.

A use case diagram for the online signature verification service is shown in Fig. 1.

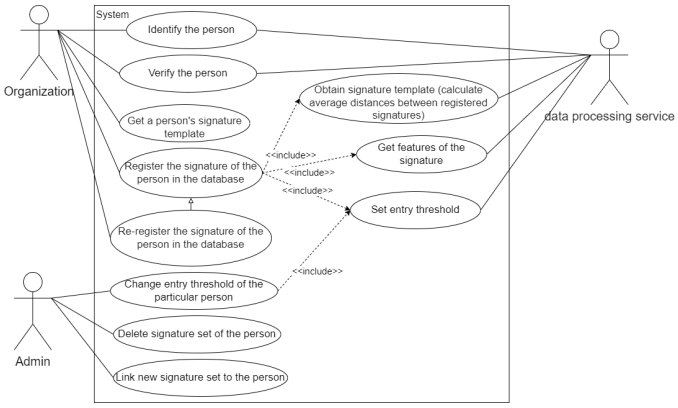

Figure 1. User case diagram

The main component of the online service is the RESTful API server, which is built on the basis of the MVC (Model-View-Controller) architectural pattern. MVC architecture is the most common in designing web applications, since the division into Model, View, Controller layers naturally matches the structure of such services. Fig. 2 shows the interaction diagram of the RESTful API components in the MVC architecture.

View is a client part in the form of a web, IOS or Android application. The main task of the client application is to generate and send signature data to the server. Currently, the project has implemented a 'stub application' that reads data from the public signature database file and sends it to the server.

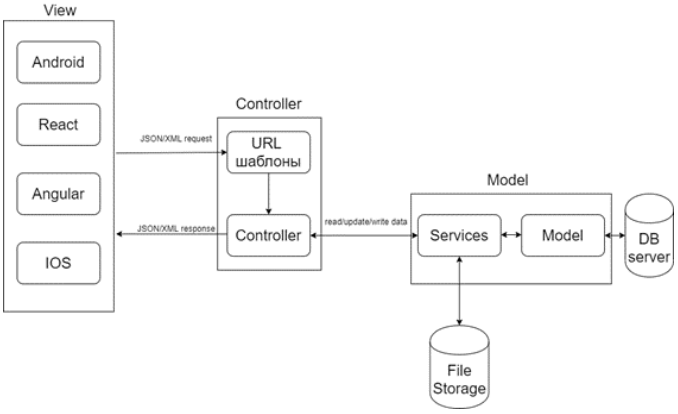

Figure 2. Scheme of the interaction between applications and API in MVC architecture

API interactions are done via JSON or XML. JSON and XML are a standardized data format that a web application receives, processes, and sends back. In this case, a web application is an API built on web services. The JSON format was chosen as the data exchange.

The PostgreSQL relational DBMS was used to store data about users and signatures. ORM SQLAlchemy is used to interact with the database. To create database queries, the Facade design pattern will be used to encapsulate the logic of accessing the database. Fig. 3 shows a diagram of service components.

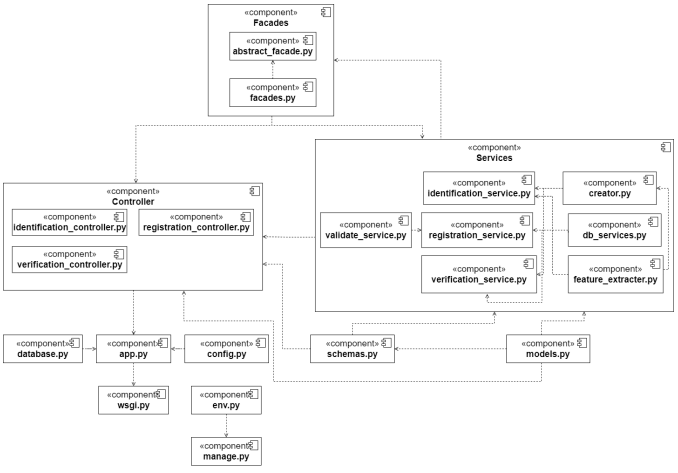

Figure 3. Service component diagram

The software was implemented in Python using the Flask web application framework.

C. Experiment

When testing the API, signatures from DeepSignDB [27] were loaded into the database. The DeepSignDB database includes a total of 1526 users from five different databases. The points of each signature are transmitted to the server, obtained by drawing the signature in the following format:

$$[(x_1, y_1, p_1, t_1), (x_2, y_2, p_2, t_2), \ldots, (x_n, y_n, p_n, t_n)] \quad (1)$$

In (1) x, y, p, t represent x and y coordinates, pressure from the graphics tablet and timestamp respectively.

After the data is received, the features are extracted from them and entered into the database. Also, signatures are interpolated up to 256 points, normalized and standardized.

During the experiment, the training signatures of the DeepSignDB database were preliminarily loaded into the database.

After that, for all signatures of each user, the login parameters were calculated according to the following algorithm:

1) The principal components method was applied to each signature, where the number of components was equal to two;
2) The resulting parameters of all user signatures were analyzed using the dynamic time warping, and pairwise distances between all reference signatures were calculated;
3) Minimum, average and maximum distances were calculated and entered into the database.

Thus, the service was ready for the verification experiment.

During verification, the test data of the DeepSignDB database was sent to the server. The results are presented in table I.

Table I
EXPERIMENT RESULTS

Evaluation parameter	Result
Average server response time	2.9 sec
Verification quality	96,4%

It should be noted that the average number of signatures per person in the test database used was 7. In the verification experiment, 2567 signatures were used.

Verification quality was calculated using the following formula:

$$q = \frac{k}{all} \quad (2)$$

In (2) k is the number of correctly verified users and all – the number of signatures verified. Thus, we can conclude that the experiment was carried out successfully. The algorithm can also be improved, making it more resistant to forgery.

The main advantage of the project over analogues is its open source code and the ability to supplement the existing system with its own verification methods.

V. CONCLUSION

As a result of the conducted research and development, the following stages were completed:

1) A comparative analysis of software tools for handwritten signature verification and identification was carried out. It made possible to identify the relevant products, determine their strengths and weaknesses;
2) A comparative analysis of approaches and algorithms for handwritten signature was carried out, which made it possible to classify the algorithms, determine the principles of their operation, and application limits;

3) The main functionalities of the developed online service were determined, taking into account their importance and the order of implementation;
4) An object-oriented conceptual data model of the online service subject area has been built;
5) The object-oriented conceptual data model is mapped into the relational schema of the online service database on the PostgreSQL platform;
6) A software prototype of an online service was developed, including a library for verifying and identifying a handwritten signature based on the dynamic time warping algorithm;
7) An experimental evaluation of the online service software was carried out to study the accuracy and speed of verification results using the DeepSignDB database.

A service can be considered as an API to implement in any information system. In the future, it is planned to develop a client application prototype, expand the set of supported algorithms and include them in the library, develop signature quality analysis tools and automated selection tool for the verification algorithm. It is also planned to conduct load regression complex testing of the response time and accuracy of signature verification, taking into account the automatic selection of the algorithm.

REFERENCES

[1] Vdovkina S. A., Shibanov S. V. Obzor metodov onlajn-verifikacii rukopisnoj podpisi // Analiticheskie i chislennye metody modelirovanija estestvenno-nauchnyh i social'nyh problem : sb. st. po materialam XVI Mezhdunar. nauch.-tehn. konf. (g. Penza, Rossija, 1–4 dekabrja 2021 g.) / pod red. prof. I. V. Bojkova. – Penza : Izd-vo PGU, 2021. - pp. 108-113.

[2] K. Jain, F. D. Griess, S. D. Connell. On-line Signature Verification. // Pattern Recognition, vol. 35, no. 12, pp. 2963–2972, 2002

[3] F. Hao, C. C. Chan. Online Signature Verification Using a New Extreme Points Warping Technique // Pattern Recognition Letters, 2003, vol. 24, no. 16, pp. 2943-2951

[4] R. Martens and L. Claesen, "On-line signature verification by dynamic time-warping," Proceedings of 13th International Conference on Pattern Recognition, 1996, pp. 38-42 vol.3, doi: 10.1109/ICPR.1996.546791.

[5] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," Pattern Recognition, vol. 40, pp. 981-992, 3// 2007.

[6] S. Rashidi, A. Fallah, and F. Towhidkhah, "Authentication based on signature verification using position, velocity, acceleration and Jerk signals," in Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on, 2012, pp. 26-31.

[7] A. Q. Ansari, M. Hanmandlu, J. Kour, and A. K. Singh, "Online signature verification using segment-level fuzzy modelling," Biometrics, IET, vol. 3, pp. 113-127, 2014.

[8] P. Jain and J. Gangrade, "Online Signature Verification Using Energy, Angle and Directional Gradient Feature with Neural Network," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, pp. 211-216, 2014.

[9] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: Feature extraction and signature modeling," Pattern Recognition Letters, vol. 28, pp. 2325-2334, 12/1/ 2007.

[10] K. Barkoula, G. Economou, and S. Fotopoulos, "Online signature verification based on signatures turning angle representation using longest common subsequence matching," International Journal on Document Analysis and Recognition (IJDAR), vol. 16, pp. 261-272, 2013/09/01 2013

[11] R. S. Kashi, J. Hu, W. L. Nelson and W. Turin, "On-line handwritten signature verification using hidden Markov model features," Proceedings of the Fourth International Conference on Document Analysis and Recognition, 1997, pp. 253-257 vol.1, doi:10.1109/ICDAR.1997.619851.

[12] Nyssen, E., Sahli, H. and Zhang, K. A Multi-stage Online Signature Verification System. Pattern Analysis and Applications, 288–295 (2002). https://doi.org/10.1007/s100440200025

[13] Kashi, R. S. (1996). On-line handwritten signature verification using stroke direction coding. Optical Engineering, 35(9), 2526. doi:10.1117/1.600857

[14] Tolosana, Ruben and Vera-Rodriguez, Ruben and Fierrez, Julian and Ortega-Garcia, Javier. (2021). DeepSign: Deep On-Line Signature Verification. IEEE Transactions on Biometrics, Behavior, and Identity Science. PP. 10.1109/TBIOM.2021.3054533.

[15] S. Otte, M. Liwicki and D. Krechel, "Investigating Long Short-Term Memory Networks for Various Pattern Recognition Problems," Machine Learning and Data Mining in Pattern Recognition, Springer, 2014.

[16] Lai, S., Jin, L., and Yang, W. (2017). Online Signature Verification Using Recurrent Neural Network and Length-Normalized Path Signature Descriptor. 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), 01, 400-405.

[17] Ahrabian, Kian and Babaali, Bagher. (2019). On Usage of Autoencoders and Siamese Networks for Online Handwritten Signature Verification. Neural Computing and Applications. 31. 10.1007/s00521-018-3844-z.

[18] A. Hefny and M. Moustafa, "Online Signature Verification Using Deep Learning and Feature Representation Using Legendre Polynomial Coefficients," in Proc. International Conference on Advanced Machine Learning Technologies and Applications, 2019.

[19] X. Wu, A. Kimura, B.K. Iwana, S. Uchida and K. Kashino, "Deep Dynamic Time Warping: End-to-End Local Representation Learning for Online Signature Verification," in Proc. International Conference on Document Analysis and Recognition (ICDAR), 2019.

[20] J. J. Igarza, I. Goirizelaia, K. Espinosa, I. Hernaez, R. Mendez, and J. Sanchez, "Online handwritten signature verification using hidden Markov models," (Lecture Notes in Computer Science 2905), in Proc. CIARP 2003, A. Sanfeliu and J. Ruiz-Shulcloper, Eds. Berlin, Germany:Springer-Verlag, pp. 391–399.

[21] Mingfu Zou, Jianjun Tong, Changping Liu and Zhengliang Lou, "Online signature verification using local shape analysis," Seventh International Conference on Document Analysis and Recognition, 2003. Proceedings., 2003, pp. 314-318 vol.1, doi: 10.1109/ICDAR.2003.1227680.

[22] Z.-H. Quan and K.-H. Liu, "Online signature verification based on the hybrid HMM/ANN model," Int. J. Comput. Sci. Netw. Secur. (IJCSNS), vol. 7, no. 3, pp. 313–321, Mar. 2007.

[23] Yan Chen and Xiaoqing Ding "On-line signature verification using direction sequence string matching", Proc. SPIE 4875, Second International Conference on Image and Graphics, (31 July 2002); https://doi.org/10.1117/12.477063

[24] Bovino, L. and Impedovo, S. and Pirlo, Giuseppe and Sarcinella, L.. (2003). Multi-Expert Verification of Hand-Written Signatures. Document Analysis and Recognition, International Conference on. 2. 932. 10.1109/ICDAR.2003.1227796.

[25] Dimauro, Giovanni and Impedovo, S. and Pirlo, Giuseppe. (2011). Component-oriented algorithms for signature verification. International Journal of Pattern Recognition and Artificial Intelligence. 08. 10.1142/S0218001494000401.

[26] Huang, Kai and Yan, Hong. (2003). Stability and style-variation modeling for on-line signature verification. Pattern Recognition. 36. 2253-2270. 10.1016/S0031-3203(03)00126-2.

[27] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepSign: Deep On-Line Signature Verification", IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021.