

Criminalistic conclusions on signature forgery process during building an offline signature verification intellectual system

DMITRY V. BAKHTEEV

ORCID: 0000-0002-0869-601X

Criminalistics Department of Ural State Law University,
Yekaterinburg, Russian Federation

Abstract

The article describes details of the NSP-SigVer project, such as qualitative indicators of humans' ability to identify a signature forgery, which can be used to build an offline signature verification system based on an artificial neural network. The average accuracy of this action is 69.29%. The article also provides a classification of signature forgery and some features of the forgery process which are important for its identification.

Keywords: offline signature verification, signature forgery, signature dataset

Among the objectives of examining questioned documents is defining the signature's genuineness as one of the key details of a legally significant document. The genuineness/authenticity/lack of forgery signs is revealed at two levels: during an operational verification of a document (including a comparison of a reliably authentic document with a disputed one) and during an expert examination of a questioned document. In the first case, the subject of signature verification is often a person who does not have the appropriate knowledge and skills. This necessitates either advanced training of such persons or the creation of some tool to help in this process.

Such an instrument potentially can be created with the methods of intellectual verification of signatures based on artificial neural networks. These methods can be realized in forms of online and offline signature verification.

Online verification takes into account dynamic signs of signature execution as a complex, three-dimensional process; not only the final signature is analyzed, but also the process of its performing. This type of verification requires using a video recording or a touchscreen able to measure the pen movement speed and the pressure depth.

In turn, offline verification more reflects the practice: only the signature as a final graphic image is examined.

Since 2018, researchers from the Department of Criminalistics of the Ural State Law University have developed an experimental model of an intellectual system based on Siamese artificial neural networks for offline verification of a signature forgery called NSP-SigVer. We test the following hypothesis. Genuine signatures of different people have different degrees of variation. Moreover, the more stable the general and particular features of a signature, the less varied they are. And in this case, they are more likely to reflect the features of a particular person's handwriting. When analyzing a large number of signatures, the average value of these variational changes can be determined – thus, it is possible to form a certain “normalized state” for each signature, at the same time reflecting most of its particular features. The normalized state of the forged signature will differ from one of the genuine signature. During the training process, a system based on an artificial neural network must learn to distinguish a genuine signature from a forged one through comparing a reliably genuine signature with a questioned one (that can be either genuine or forged).

The human person as the subject of the practice signature forgery verification is an obvious exemplar to set criteria for the effectiveness of any system which optimizes human activity. Accordingly, a special questionnaire was organized within the project, aimed at setting indicators of human ability to distinguish genuine and forged signatures.

The probability of success in this operation directly depends on the person's experience and specialized education as well as the quality of the forgery. Each of the 127 respondents was offered a form for collecting

basic data: sex, age, level of education, special knowledge in the handwriting and document examination or related fields, subjective self-assessment of the respondent's own skills in identifying forged signatures. The questionnaire was carried out with time measurement: the average time for comparing the signatures was recorded.

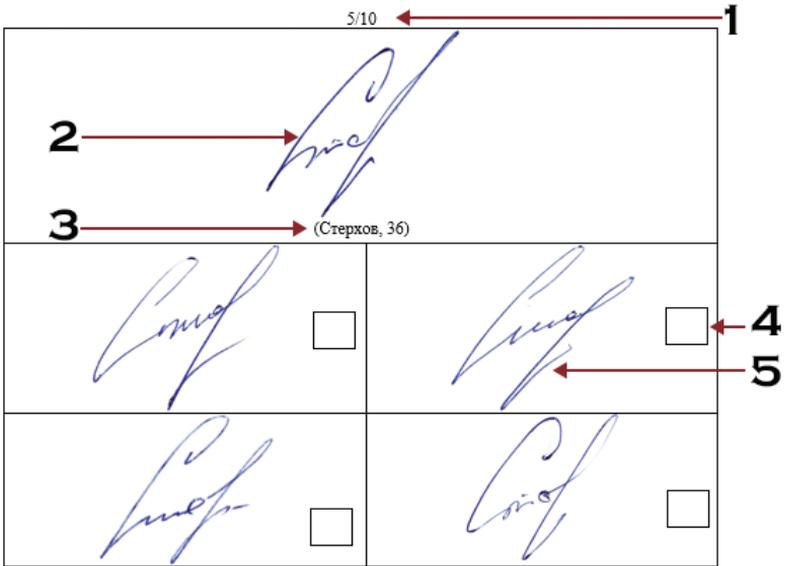
Every respondent was then given a form with 10 sets of signatures, one of which was genuine. The remaining four should be identified as either genuine or forged based on a visual comparison of the signatures (example of one such set in Figure 1). Of course, the selection is clearly not enough for a full-fledged experimental questionnaire; however, even conditionally accurate data is enough to formulate qualitative indicators for hypothesis; and if they are absent, the network quality can be evaluated even "against a coin toss" – the accuracy of the results should exceed 50%.

Based on the questionnaire results, the probability of correct verification of signatures does not exceed a 69% average (see Table 1), while women (see Table 2) show slightly better results than men (see Table 3). These data should also be evaluated critically: in real practice, a person assumes the document is genuine, while in this questionnaire the respondents could guess that among the presented signatures were some forged ones. The ratio of genuine and forged signatures in form was not known to the respondents.

Another important aspect of developing an intelligent system is its training dataset. The quality of decision-making by a person largely depends on their experience. Similarly, the operation of an intelligent system is determined by the content of the dataset for training. As part of this project, the first known dataset containing Cyrillic signatures was collected. For this moment, it contains 33 988 genuine signatures from 606 persons and corresponding 71 003 forged signatures. The dataset collection still continues.

Based on their execution methods, forgeries can be divided into three types: auto-forgery, simple, and skilled forgery. In the case of auto-forgery, the performer is the owner of the signature, the purpose of such forgery is the alleged future refusal to recognize the document as properly signed.

Simple forgeries can be considered differently. In the first variant, the forger has information about the signer's name and examples of their sig-



1 – the number of the kit in the questionnaire

2 – original signature

3 – surname and age of signer

4 – checkbox (a check mark is put if the respondent believes that the signature is genuine, a cross – if they believe that the signature is fake)

5 – questioned signature

Figure 1. A sample set of signatures for comparison in the questionnaire

Source: author's archive.

natures.¹ But signatures copied without information about the signature author's identity cannot really be considered as an issue: in reality, forging a signature is not valuable in itself but as a means of achieving a certain external goal. The forger almost always has sufficiently detailed information about the person whose signature is forged. Different situations occur, but their identification is not a significant problem. The second approach, which we support, considers simple forgeries to be forged signa-

¹ L.G. Hafemann, R. Sabourin, L.S. Oliveira, "Offline handwritten signature verification – Literature review", *Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 28 November–1 December 2017, Montreal, Canada, p. 1.

Table 1. Summarized results

Number	Average age	Specialized knowledge	Self-assessment of skills (from 1 to 10), average	Time per set, sec.	Accuracy, average
127	24	5	4.89	51	69.29%

Table 2. Signature forgery verification: female

Age	Number	Self-assessment of skills (from 1 to 10), average	Time per set, sec.	Accuracy, average
18–29	68	4.92	52	70.36%
30–45	5	4.00	42	72.50%
45–60	3	3.66	27	65.00%
Total	76	4.80	50	70.23%

Table 3. Signature forgery verification: male

Age	Number	Self-assessment of skills (from 1 to 10), average	Time per set, sec.	Accuracy, average
18–29	47	4.76	56	67.02%
30–45	1	6.00	49	75.00%
45–60	3	7.30	103	80.60%
Total	51	4.90	54	67.90%

tures, performed by a person without special skills. Such forgeries often miss significant features of the initial genuine forgery.

Skilled forgeries in a given project not only are performed with examples of genuine ones present, but also require special skills on the part of the forgers, who are either professional artists or handwriting experts. In both cases, professional skills make it possible to very carefully copy the image of the signature.

Analyzing the forgery process draws a number of conclusions significant for criminalistics, both the science and the practice.

1. All our skilled forgers (and some of the unskilled ones) mentioned that it seemed to them they had seen the signatures they were forging before, which is absolutely impossible. Thus, we can conclude that from a non-expert's point of view, there are not so many options or types of sig-

natures. For one person, the signatures of two different individuals may seem identical and the difference between them can be possibly explained by variations in the signature, but not the difference between individuals.

2. The best results in forging appeared when using a small number of forged signature samples (1–3).² In this case, the variability in the forger's signature performance did not differ from the original signatures in terms of the variational change quality.

3. When using more signatures as samples, control over compliance with individual features was weakened. Presumably this can be explained by the fact that several alternative variants of the forged signature are “loaded” into the memory of the forger, after which a choice is made between these options. In this case, especially with the high pace of movements, random characteristics of the forger's own signature may get into the forged signature.

4. Slowing down the pace of the signature strokes reduces the number of misrepresented features, but at the same time reduced coordination of movements is a common signature forgery symptom.

5. Changes in the pressure on the new writing device, in its sliding ability on paper, or in its thickness together partially violate the finger movements, which also affects the temporarily developed skill of forgery.

6. The difference in the anatomical structure and size of the signer and the forger's hands in some cases does not allow the “appropriate” forging. This applies to large signatures made by a sweeping arc or oval movements. If the original signature is made by a person with a large palm size, the arc and oval elements can be presented as a compass, where one leg is a writing device and the palm plays the role of the other leg.

7. The most significant features – such as the placement of points characterizing the movement length relative to other signature elements, the placement of intersection movement points relative to other signature elements, or the shape and placement of connection points between elements relative to other signature elements – are rarely controlled when performing fakes.

² Forgers completed 28 forged signatures with 56 genuine ones provided.

8. A long-term attempt to form a temporary skill of performing a large signature while holding hand in weight does not give a positive result in the absence of drawing skills.

9. Signatures formed by separately written glyphs imitating the technical font or block letters did not cause difficulties in their forgery. People who graduate from technical educational facilities often have two handwriting patterns and all handwriting generated from technical fonts is very similar.

The above characteristics can be used in conducting handwriting examinations and in assisting employees who often encounter questioned documents. Thus, the automation of criminalistics processes, such as signature recognition, can also ensure the progress of classical criminalistics, providing data for traditional documentary research.

Acknowledgements

The reported study was funded by RFBR according to the research project no. 18-29-16001.

References

Hafemann L.G., Sabourin R., Oliveira L.S., “Offline handwritten signature verification – Literature review”, *Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 28 November–1 December 2017, Montreal, Canada.