Metadata of the chapter that will be visualized in SpringerLink

Book Title	Quality of Information and Communications Technology
Series Title	
Chapter Title	NSP Dataset and Offline Signature Verification
Copyright Year	2020
Copyright HolderName	Springer Nature Switzerland AG

Corresponding Author	Family Name	**Bakhteev**
	Particle	
	Given Name	**Dmitry V.**
	Prefix	
	Suffix	
	Role	
	Division	Department of Criminalistics
	Organization	Ural State Law University
	Address	Yekaterinburg, Russian Federation
	Email	ae@crimlib.info
	ORCID	http://orcid.org/0000-0002-0869-601X
Author	Family Name	**Sudarikov**
	Particle	
	Given Name	**Roman**
	Prefix	
	Suffix	
	Role	
	Division	Institute of Formal and Applied Linguistics
	Organization	Charles University
	Address	Prague, Czech Republic
	Email	sudarikov@ufal.mff.cuni.cz
	ORCID	http://orcid.org/0000-0002-0276-3568

Abstract

Offline signature verification is a challenging task for both computer science and forensics. Skilled forgeries often cannot be recognized by humans, which leads to the need to develop automated forged signatures recognition methods, which in turn requires the creation of different datasets for training models, which include the NSP – the first dataset with Cyrillic offline signatures, including genuine signatures with their skilled and simple forgeries. The process of collecting data for this dataset is described in detail. In the process of collecting samples we reformulated the forensic classification of signatures by criterion of their structure and forgery vulnerability. Gathered database was evaluated using a Siamese neural network model and the results are compared with the same model trained on CEDAR dataset.

Keywords

Offline signature verification - Signature forensics - Siamese neural networks

NSP Dataset and Offline Signature Verification

Dmitry V. Bakhteev[1](✉) and Roman Sudarikov[2]

[1] Department of Criminalistics,
Ural State Law University, Yekaterinburg, Russian Federation
ae@crimlib.info

[2] Institute of Formal and Applied Linguistics,
Charles University, Prague, Czech Republic
sudarikov@ufal.mff.cuni.cz

Abstract. Offline signature verification is a challenging task for both computer science and forensics. Skilled forgeries often cannot be recognized by humans, which leads to the need to develop automated forged signatures recognition methods, which in turn requires the creation of different datasets for training models, which include the NSP – the first dataset with Cyrillic offline signatures, including genuine signatures with their skilled and simple forgeries. The process of collecting data for this dataset is described in detail. In the process of collecting samples we reformulated the forensic classification of signatures by criterion of their structure and forgery vulnerability. Gathered database was evaluated using a Siamese neural network model and the results are compared with the same model trained on CEDAR dataset.

Keywords: Offline signature verification · Signature forensics · Siamese neural networks

1 Introduction

In the history of mankind, dozens of different methods of remote identification of person have been created, introduced and lost. Handwritten signatures turned out to be the most stable and suitable for use as props for documents used in economic and law enforcement activities, mainly due to their comparative ease of execution and non-invasive methods of receipt. In forensics, the signature carries an identification and diagnostic value. Identification allows to establish a specific performer of signature, determine whether it is genuine or forged. Two objects are always involved in the identification process, the authenticity of one of which is always precisely known. Diagnostics of the signature allows to establish the characteristics of its performer: both their identity and some personality traits.

Forgeries from the point of view of the method of their performing can be divided into three types: auto-forgery, simple and skilled forgeries. In the case of auto-forgery, the performer is the owner of the signature, the purpose of such

M. Shepperd et al. (Eds.): QUATIC 2020, CCIS 1266, pp. 1–9, 2020.
https://doi.org/10.1007/978-3-030-58793-2_4

an action is the alleged future refusal to recognize the document as properly signed. In the case of simple forgeries within the framework of this study, we understand forgeries, for the creation of which forger had knowledge about the signer's name and examples of his handwritten signatures. We do not recognize as such signatures made without an images of the signer's signature [3]. Of course, in cases of law enforcement, such cases do occur, but their resolving is not a big problem due to the low similarity between existing genuine documents and forged ones. Skilled forgeries are performed not only in the presence of examples of genuine signatures, but also with the help of special skills of the forger.

Whole signature verification field can be divided into two main categories by acquisition type: online and offline verification. Online signature verification deals with analysis of the signatures while they are captured using a digitizing device and takes into the account sequence of the strokes over time, pen position, pen pressure, etc. Offline verification on the other hand acquires the signature after the process is finished, most commonly in a form of a digital image.

The practical scope of combining forensic methods with the possibilities of offline signature recognition expands the possibilities of identification processes in civil, commercial and law enforcement activities and expands communication between academic disciplines and practice.

The outline of the paper is the following: Sect. 2 is devoted to the review of related works in the field of signature verification, Sect. 3 describes the process of collecting NSP dataset and processing done around it. Section 4 discusses some of the forensic discoveries made during the dataset collection, and Sect. 5 details the assessment experiments carried out using collected dataset. Finally, Sect. 6 concludes the paper with future work.

2 Related Works

Most of the recent advancements in the field of offline signature verification including the researches of Deep Learning methods are described by [3]. The work reviewed both most commonly used datasets (CEDAR [4], MCYT [5] and GPDS [8]) and different approaches to offline signature verification, starting from classic Machine Learning algorithms such as Support Vector Machines (SVM) and Hidden Markov Models, followed by Deep Neural Networks and classifiers ensembles. Here it is also appropriate to mention two different types of verification models, which are *writer-independent* and *writer-dependent*. As it is clear from the names, the former models can be applied to any signature verification task, independently of whether or not they saw the subject's signatures in the training set. The latter models though need to be exposed to the subject's signatures during the training.

There are also different approaches in feature extraction and Convolutional Neural Networks (CNN) composition, as presented by [1] and [7]. The former introduced SigNet – convolutional Siamese neural network, which learns writer independent features and shows good performance on cross domain datasets. The latter showed performance improvements by combining CNN feature extraction with SVM writer-independent classifier.

As it was mentioned previously currently there are several benchmark datasets in the field of signature verification: CEDAR [4], MCYT[5], GPDS [8] and BHSig260 [6]. Characteristics of NSP dataset in comparison with some other existing datasets are presented in Table 1.

Table 1. Comparison of offline signature datasets

	Handwriting system	Signers	Signatures (genuine/forged)
NSP	Cyrillic	224	40 562 (12 596/28 056)
CEDAR	Latin	55	2640 (1320/1320)
MCYT	Latin	330	16 500 (8250/8250)
GPDS-960	Latin	960	51 849 (23 049/28 800)
BHSig260	Bangla, Hindi	260	14 040 (6240/7800)

3 NSP Dataset Collection

The NSP handwritten signature dataset contains 56 genuine signatures and from 112 to 224 corresponding forgeries for one signer. The genuine signatures were taken from signers in two-sheets form, each including 28 boxes for signatures and fields for some information about signer (name, age, dominant hand). Such a quantity is explained by the fact that, in order to obtain reliable knowledge about the degree of variational changes in the signature of one person, it is necessary to consistently receive at least 50 signatures according to the methods of production of handwriting examinations. In the end of this process, most signers lose focus, their hand gets tired, then control over the accuracy of movements decreases and the signature becomes more automatic, so we receive an almost full space of possible signatures variations. Smaller amounts of signatures may not give reliable results.

Table 2. Distribution of the NSP signature dataset.

	Signers	Avg age	Right-/Left-handedness	Genuine	Forgeries (skilled/simple)
Male	100	28	76/6	5 600	12 383 (6 212/6 171)
Female	123	29	92/6	6 940	15 561 (7 784/7 777)
Total	224	29	168/12	12 596	28 056 (14 052/14 004)

It should be noted that the signatures of the residents of the Russian Federation are usually Cyrillic (with rare exceptions), which distinguishes the NSP dataset from those described earlier in Sect. 2.

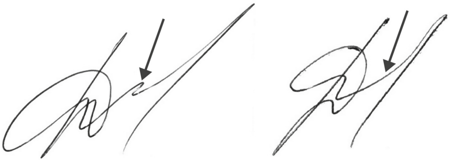

Fig. 1. Left signature (genuine) has a vertical stroke (marked), while the left one (unskilled forgery) lacks it.

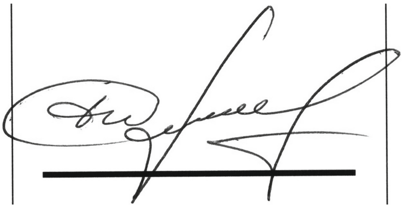

Fig. 2. Example of signature, crossing both signature line and vertical lines of the box.

Forgeries were made in both skilled and unskilled (simple) forms. Skilled forgeries were done by group of 12 people, each of them with an experience either in artistry or forensic examination of handwritten documents. Our hypothesis was that such skills will allow forger to make an almost exact copy of given signature, either on the basis of its graphical appearance – in case of artists, or by understanding forensic features of signature – for forensic experts. Unskilled (simple) forgeries were done by people with no experience in handwriting examination and/or signature forgery, so forgers often lost sight of one or another characteristic of the forged signature (see example on Fig. 1).

Every forger (in both skilled and unskilled situations) was provided by two sheets of genuine signatures, so they knew name of signer, his age, so they have an ability to transcript questioned symbols in a signature correctly. Signatures of left-handed signers were forged only by left-handed forgers; then both left-handed and right-handed forgers were involved in making forgeries for right-handed signatures. Forgers independently chose which exact signatures they would copy. This decision was made as a simulation of the situation of a real document forgery when it is not known exactly which signatures are used as a sample for forgery.

Forgeries were also done on the forms of 28 boxes, so the resulting set of signatures for one person contains 2 sheets of genuine signatures and from 4 to 8 sheets with forgeries. Forgeries were prepared without the use of special technical means, such as use of a plotter, transfer paper, wet copying, source of background lighting, etc.

After that, the resulting sheets with genuine signatures and forgeries were scanned at a resolution of 600 DPI; the digital images were divided into separate images with one signature per image. Individual images of signatures were obtained by automatically cutting the image of the sheet along the lines of the form and then manually trimming each signature to the borders of the rectangle at the extreme points of the signature. If the signature strokes cross the line of the box, such signature was left in the dataset. Additionally, in forms with later samples, we used imitation of the signature line in the bottom four rows of the form. Accordingly, both horizontal and vertical lines can be found on the obtained images (see an example in Fig. 2). In any case, offline signature verification technologies are practice-oriented, and signatures in practice are usually

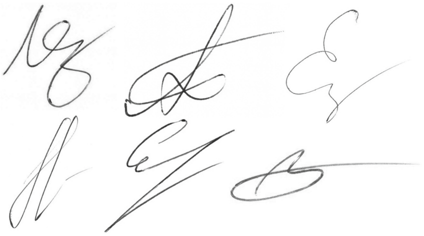

Fig. 3. Examples of signatures of type 1, containing several letters.

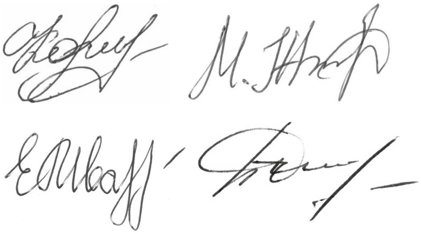

Fig. 4. Examples of signatures of type 2, containing some of the first letters of the last name of the signer with possible initials.

combined with other details of the document, like seals' imprints and lines of the form of the document.

Statistical data about the composition of NSP dataset are summarized in Table 2. Some signers did not provide information about themselves, this explains the inconsistencies in the Table 2.

The whole process of gathering genuine signatures was accomplished under the supervision of a project team member. Forgers (both categories) were given instructions, and the results of their work were carefully checked. All participants in the experiment were instructed on the rules for working with personal data, the corresponding confirmation was taken from them.

4 Types of Signatures

According to the design and composition of signatures of residents of the Russian Federation such signatures can be conditionally differentiated into four types:

1. Signatures based on the performance of several letters (usually from 1 to 3), which have low readability and low resistance to forgery methods (Fig. 3).
2. Signatures containing some initials and the first few letters of the surname, most characters are readable. This archetype is dominant in Russia, because it combines the speed of execution and the overall complexity sufficient to counter simple forgery methods, expressed in a significant number of private features displayed in the signature. Usually such signatures are stretched horizontally (Fig. 4).
3. Signatures, which are the spelling of a last name (often together with the name and patronymic) without complicating or simplifying elements, the usual handwriting for the performer (Fig. 5). Those signatures are usually not well defended against forgery due to their slower pace of performance, while other types of signatures are performed with an increased pace compared to regular writing of the signer.
4. Signatures-drawings of complex design, consisting of conditional elements that do not form letters and having mainly superscript-subscript elegant,

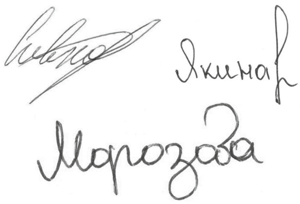

Fig. 5. Examples of signatures of type 3, containing full last name of the signer.

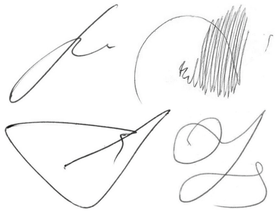

Fig. 6. Examples of letterless signatures of type 4.

Table 3. Experiment datasets

	Signers	Genuine (per signer)	Forgeries (per Genuine)	Total pairs
CEDAR				
Train	40	24	24	34 080
Validation	10	24	24	8 520
Test	5	24	24	4 260
NSP				
Train	138	56	30	444 360
Validation	40	56	30	128 800
Test	10	56	30	32 200

elaborate strokes of a complex structure. They are complex systems of multidirectional movements overlapping each other, movements of a complicated structure, usually with continuous connectivity. Their resistance to forging methods varies (Fig. 6).

5 Experiments

To demonstrate the relative complexity of the dataset, it was decided to take one of the best performing models, namely convolutional Siamese neural network model [1] and show it's performance on NSP dataset as well as CEDAR [4] dataset.

For the experiments, we have separated NSP dataset described above into 3 parts: training, validation and test. Distribution was the following - 138 signers used in the training, 40 – in validation and 10 in test. Signers were assigned randomly at the beginning of each experiment run, to provide more consistent and reliable results. For each signer we have used 56 genuine signatures and for each genuine signature we have picked 30 forgeries at random to have a balanced number of genuine-genuine and genuine-forged samples.

An experiment was carried out using CEDAR [4] dataset, to serve as a reference point for the used model. For CEDAR dataset we have used 40 signers for training, 10 for validation and 5 for test. For each signer we have used all 24 available genuine signatures and 24 available forgeries

Final setup for experiments on both NSP and CEDAR datasets is shown in Table 3. For both experiments, signature samples were resized to 220 × 155 pixels to normalize signature sizes and keep the input vector space reasonably small.

Models setup followed [1] approach with similar layer configuration with implementation done using Keras framework with Tensorflow as backend. To show that trained model is comparable with the results in [1], it was evaluated first on CEDAR [4] dataset and then on NSP dataset.

Both experiments were following the same evaluation steps. The best epoch was selected based on contrastive loss function [2] value on the validation set. The output of a model is a distance metric, which doesn't directly predicts the class of images, but rather the distance between them. Thus a threshold is needed to be determined to decide if the input images belong to the same class or not, i.e. if both signatures are genuine or one is forged. In the experiments the same validation set was used to estimate the best threshold to map output distance value to binary classes. This estimated threshold was then used to translate the output of the model on the test set samples into the binary classes.

Table 4. Experiment results

Dataset	FAR	FRR	Accuracy
CEDAR	8.33	0.00	94.37
NSP (9-runs mean)	17.80 ± 2.22	20.56 ± 2.60	80.87 ± 1.39

5.1 Experiment Results

The results for both NSP and CEDAR datasets are presented in the Table 4, with the following metrics: False Rejection Rate (FRR), False Acceptance Rate (FAR) and accuracy. FRR is computed as a ratio of false negative samples divided by the total number of positive samples. FAR is computed as a ratio of false positive samples divided by the total number of negative samples. Accuracy is computed as a ratio between a sum of all true positive and true negative predicted pairs and a sum of all number of pairs examined.

For CEDAR experiment, FRR is the same as in the results by [1], but FAR and accuracy differ, which can be attributed to the way loss function threshold is estimated in current experiment, since validation set is specifically used to estimate the threshold value for output separation. Table 5 shows resulting confusion matrix with the exact numbers. The results show that the model performs on a comparable level to the similar works.

Table 5. CEDAR confusion matrix

		True	
		Genuine	Forged
Predicted	Genuine	1 380	240
	Forged	0	2 640

Table 6. NSP confusion matrix

		True	
		Genuine	Forged
Predicted	Genuine	12 995	3 496
	Forged	2 405	13 304

NSP experiment was run nine times and the mean results with 95% confidence interval were reported in the Table 4. For NSP experiment, the results are lower than CEDAR ones, which could be attributed to higher complexity and diversity of the signatures in NSP dataset. Confusion matrix presented in Table 6 shows the results for one of the experiment runs just to give an idea of the predictions distribution.

6 Conclusion/Discussion

Siamese neural network model showed promising results as well as left the room for potential improvements.

In out future work on the models we are planning to evaluate different model architectures on NSP dataset as well as work more on cross-dataset experiments where models would be trained on NSP dataset and then tested on GPDS and MCYT datasets to see how well the model can generalize features which could be transferred between different script.

The collection of signature samples for the dataset is not completed (and, hopefully, will not be), several hundred new signatures are included in it weekly, which allows increasing both the size and variety of data.

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

References

1. Dey, S., Dutta, A., Toledo, J.I., Ghosh, S.K., Lladós, J., Pal, U.: Signet: convolutional siamese network for writer independent offline signature verification. arXiv preprint arXiv:1707.02131 (2017)
2. Hadsell, R., Chopra, S., LeCun, Y.: Dimensionality reduction by learning an invariant mapping. In: 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2006), vol. 2, pp. 1735–1742. IEEE (2006)
3. Hafemann, L.G., Sabourin, R., Oliveira, L.S.: Offline handwritten signature verification–literature review. In: 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 1–8. IEEE (2017)
4. Kalera, M.K., Srihari, S., Xu, A.: Offline signature verification and identification using distance statistics. Int. J. Pattern Recogn. Artif. Intell. **18**(07), 1339–1360 (2004)

5. Ortega-Garcia, J., et al.: MCYT baseline corpus: a bimodal biometric database. IEE Proc.-Vision Image Signal Process. **150**(6), 395–401 (2003)
6. Pal, S., Alaei, A., Pal, U., Blumenstein, M.: Performance of an off-line signature verification method based on texture features on a large indic-script signature dataset. In: 2016 12th IAPR Workshop on Document Analysis Systems (DAS), pp. 72–77 (2016)
7. Souza, V.L., Oliveira, A.L., Sabourin, R.: A writer-independent approach for offline signature verification using deep convolutional neural networks features. In: 2018 7th Brazilian Conference on Intelligent Systems (BRACIS), pp. 212–217. IEEE (2018)
8. Vargas, F., Ferrer, M., Travieso, C., Alonso, J.: Off-line handwritten signature GPDS-960 corpus. In: Ninth International Conference on Document Analysis and Recognition (ICDAR 2007), vol. 2, pp. 764–768. IEEE (2007)