Analyzing features learned for Offline Signature Verification using Deep CNNs

Luiz G. Hafemann, Robert Sabourin
Lab. d’imagerie, de vision et d’intelligence artificielle
École de technologie supérieure
Université du Québec, Montreal, Canada
lghafemann@livia.etsmtl.ca, robert.sabourin@etsmtl.ca

Luiz S. Oliveira
Department of Informatics
Federal University of Parana
Curitiba, PR, Brazil
lesoliveira@inf.ufpr.br

Abstract—Research on Offline Handwritten Signature Verification explored a large variety of handcrafted feature extractors, ranging from graphology, texture descriptors to interest points. In spite of advancements in the last decades, performance of such systems is still far from optimal when we test the systems against skilled forgeries - signature forgeries that target a particular individual. In previous research, we proposed a formulation of the problem to learn features from data (signature images) in a Writer-Independent format, using Deep Convolutional Neural Networks (CNNs), seeking to improve performance on the task. In this research, we push further the performance of such method, exploring a range of architectures, and obtaining a large improvement in state-of-the-art performance on the GPDS dataset, the largest publicly available dataset on the task. In the GPDS-160 dataset, we obtained an Equal Error Rate of 2.74%, compared to 6.97% in the best result published in literature (that used a combination of multiple classifiers). We also present a visual analysis of the feature space learned by the model, and an analysis of the errors made by the classifier. Our analysis shows that the model is very effective in separating signatures that have a different global appearance, while being particularly vulnerable to forgeries that very closely resemble genuine signatures, even if their line quality is bad, which is the case of slowly-traced forgeries.

I. INTRODUCTION

The handwritten signature is a widely accepted means of authentication in government, legal, and commercial transactions. Signature verification systems aim to confirm the identity of a person based on their signature [1], that is, they classify signature samples as “genuine” (created by the claimed individual) or “forgery” (created by an impostor). In offline (static) signature verification, the signatures are acquired after the signature writing process is completed, by scanning a document containing the signature. This is in contrast with online (dynamic) signature verification, where the signature is captured directly on a device (such as a pen tablet), and therefore the dynamic information of the signature is available, such as the velocity of the pen movements. The lack of dynamic information in the offline case makes it a challenging problem, and much of the effort in this field has been devoted to obtaining a good feature representation for signatures [2].

The area of offline signature verification has been investigated for a few decades, and remains an open research problem. The problem consists in: given a query signature for a claimed individual, determine if the signature is genuine or a forgery. There are two main approaches for the problem in the literature: in a Writer-Dependent approach, for each user, a training set of genuine signatures of the user (and, often, genuine signatures from other users as negative samples) is used to train a binary classifier. In a Writer-Independent approach, a single global classifier is trained using a dissimilarity approach, by using a training set consisted of positive samples (a difference vector between two genuine signatures from the same author), and negative samples (a difference vector between a genuine signature and a forgery). At test time, a distance vector is calculated between the query signature and one or more reference signatures (known to be genuine signatures of the claimed individual), and then classified using the Writer-Independent classifier. For a comprehensive review on the problem, refer to [3], and for a recent review, see [4].

Recent work on the area explore a variety of different feature descriptors: Extended Shadow Code (ESC) and Directional-Probabilistic Density Function (DPDF) [4], [5]; Local Binary Patterns (LBP), Gray-Level Co-occurrence Matrix (GLCM) and Histogram of Oriented Gradients (HOG) [6], [7]; Curvelet transform [8], among others. Instead of relying on hand-engineered feature extractors, we investigate feature learning algorithms applied to this task. In previous research [9], we have shown that we can learn useful features for offline signature verification, by learning Writer-Independent features from a development dataset (a set of users not enrolled in the system). Using this formulation, we obtained results close to the state-of-the-art in the GPDS dataset, when compared against models that rely on a single feature extractor technique. In the same vein, Ribeiro et al. [10] used Restricted Boltzmann Machines (RBM) for learning features from signature images. However, the authors considered only a small set of users (10), and did not use the features to actually classify signatures, only reporting a visual representation of the learned weights. Khalajzadeh [11] used Convolutional Neural Networks for Persian signature verification, but did not considered skilled forgeries.

In this paper, we further analyze the method introduced in [9], investigating the impact of the depth (number of layers) of the Deep Convolutional Neural Network (CNN), and the size of the embedding layer on learning good representations for signatures, as measured by the classification performance on a different set of users. Using better training techniques (in particular, using Batch Normalization [12] for training the network), we can improve performance significantly, achieving a
The central idea is to learn a feature representation (a function $\phi(.)$) for offline signature verification in a Writer-Independent format, using this function to extract features from signatures $X$ of the users enrolled in the system ($\phi(X)$), and use the resulting feature vectors to train a binary classifier for each user. The rationale for learning the feature representation in a Writer-Independent format is two-fold: 1) learning feature representations directly for each user is impractical, given the low number of samples available for training (around 5-10 signatures); and 2) having a fixed representation useful for any user makes it straightforward to add new users to the system, by simply using the model to extract features for the new user’s genuine signatures, and training a Writer-Dependent classifier.

In order to learn features in a Writer-Independent format, we consider two separate sets of signatures: a development set $D$, that contains signatures from users not enrolled in the system, and an exploitation set $E$ that contains a disjoint set of users. The signatures from set $D$ are only used for learning a feature representation for signatures, with the hypothesis that the features learned for this set of users will be relevant to discriminate signatures from other users. On the other hand, the set $E$ represents the users enrolled to the system. We use the model trained on the set $D$ to “extract features” for the signatures of these users, and train a binary classifier for each user. It is worth noting that we do not use skilled forgeries during training, since it is not practical to require forgeries for each new user enrolled in the system.

Overall, the method consists in the following steps:

- Training a deep neural network on a Development set $D$
- Using this network to obtain a new representation for signatures on $E$ (i.e. obtain $\phi(X)$ for all signatures $X$)
- Training Writer-Dependent classifiers in the exploitation set, using the learned representation

Details of these steps are presented below.

### A. Convolutional Neural Network training

As in [9], we learn a function $\phi(.)$ by training a Deep Convolutional Neural Network on a Development set, by learning to discriminate between different users. That is, we model the network to output $M$ units, that estimate $P(y|x)$ where $y$ is one of the $M$ users in the set $D$, and $X$ is a signature image. In this work we investigate different architectures for learning feature representations. In particular, we evaluate the impact of depth, and the impact of the size of the embedding layer (the layer from which we obtain the representation of the signature). Multiple studies suggest that depth is important to address complex learning problems, with both theoretical arguments [13], and as shown empirically (e.g. [14]). The size of the embedding layer is an important factor for practical considerations, since this is the size of the feature vectors that will be used for training classifiers for each new user of the system, as well as performing the final classification.

In our experiments, we had difficulty to train deep networks, with more than 4 convolutional layers and 2 fully-connected layers, even using good initialization strategies such as recommended in [15]. Surprisingly, the issue was not that the network overfit the training set, but rather both the training and validation losses remained high, suggesting issues in the optimization problem. To address this issue, we used Batch Normalization [12]. This technique consists in normalizing the outputs of a layer, for each individual neuron, so that the values have zero mean and unit variance (in a mini-batch of training data), and showed to be fundamental in our experiments in obtaining good performance. Details of this technique can be found in [12]. In the experiments for this paper, we only report the results using Batch Normalization, since for most of the proposed architectures, we could not train the network without this technique (performance on a validation set remained the same as random chance).

Table I shows the architectures we evaluated in this research. The models are based on AlexNet [16] and VGG [14], which are two architectures that perform remarkably well in Computer Vision problems. Each row specifies a layer of the network. For convolutional layers, we include first the filter-size, followed by number of convolutional filters. For

| Table I. CNN architectures evaluated in this paper |
|-----------------|-----------------|-----------------|-----------------|
| AlexNet_N reduced | AlexNet_N | VGG_N reduced | VGG_N |
| conv11-96-s4-p0 | conv11-96-s4-p0 | conv3-64 | conv3-64 |
| pool3-s2-p0 | pool3-s2-p0 | pool3 | pool3 |
| conv5-256-p2 | conv5-256-p2 | conv3-128 | conv3-128 |
| pool3-s2-p0 | pool3-s2-p0 | pool4 | pool3 |
| conv3-384 | conv3-384 | conv3-256 | conv3-256 |
| conv3-256 | conv3-256 | conv3-256 | conv3-256 |
| pool3-s2-p0 | pool3-s2-p0 | pool4 | pool3 |
| FC1-N | FC1-N | FC1-N | FC1-N |
| FC2-N | FC2-N |
| FC-531 + softmax |
pooling layers, we include the size of the pooling region. Unless otherwise indicated, we use stride 1 and padding 1. For instance, conv11-96-s4-p0 refers to a convolutional layer with 96 filters of size 11x11, with stride 4 and no padding. For the Fully Connected (FC) layers, we just indicate the name of the layer (that we refer later in the text), and the number of output units. For instance, FC1-N refers to a Fully connected layer named “FC1”, with N output units. The network AlexNet_N\_reduced contains 9 layers: 6 layers with learnable parameters (convolutions and fully connected layers), plus 3 pooling layers, where the VGG_N network contains 24 layers: 19 layers with learnable parameters plus 5 pooling layers. We used Batch Normalization for each learnable layer in the network, before applying the non-linearity (ReLU, except for the last layer, which uses softmax). We considered 4 types of networks: AlexNet: a network similar to [10], but without Local Response Normalization and Dropout (which we found unnecessary when using Batch Normalization); AlexNet\_reduced: a similar network but with reduced number of layers; VGG: An architecture similar to [14]; VGG\_reduced: a similar network but with reduced number of layers. For each network, we consider a different size N for the embedding layer, N \in \{512, 1024, 2048, 4096\}. This is the size of the feature vectors that will be used for training the Writer-Dependent classifiers, and therefore they impact the cost of training classifiers for new users that are enrolled to the system, as well as the classification cost. Considering the different architectures, and size of the embedding layer, we tested in total 16 architectures.

The images were pre-processed by: centralizing the signatures in a 840x1360 image according to their center of mass; removed the background using OTSU’s algorithm; inverted the images so that the background pixels were zero valued; and finally resizing them to 170x242 pixels. More details on these preprocessing steps can be found in [9].

B. Training the Writer-Dependent classifiers

After training a Deep CNN on the development set D, we use the network to extract feature representations for signatures from another set of users (E) and train Writer-Dependent classifiers. To do so, we resize the images to 170x242 pixels, perform feedforward propagation until a fully-connect layer, and used the activations at that layer as the feature vector for the image. For the architectures marked as “reduced” (see table I), that contained only two fully-connected layers, we consider only the last layer before softmax as the embedding layer (FC1). For the architectures with three fully-connected layers, we consider both layers FC1 and FC2, that is, the last two fully-connected layers before the softmax layer.

For each user in set E, we build a training set consisted of r genuine signatures from the user as positive samples, and 14 genuine signatures from users in D as negative samples. We train a Support Vector Machine (SVM) classifier on this dataset, considering both linear SVM, and SVM with an RBF kernel. Similarly to [3], we use different weights for the positive and negative class to account for the imbalance of having many more negative samples than positive. We do so by duplicating the positive samples, so that the dataset is roughly balanced. For testing, we use 10 genuine signatures from the user (not used for training), 10 random forgeries (signatures from other users in E), and the 30 skilled forgeries made targeting the user’s signature.

III. EXPERIMENTAL PROTOCOL

We conducted experiments in the GPDS-960 dataset [17], which is the largest publicly available dataset for offline signature verification. The dataset consists of 881 users, with 24 genuine samples per user, and 30 skilled forgeries.

We divide the dataset into an exploitation set E consisting of the first 300 users, and a development set consisting of the remaining 581 users. Since in this work we evaluate many different architectures, we split the Development set into a training and validation set, using a disjoint set of users for each set. We use a subset of 331 users for training the CNN models, and a subset of 50 users for validation. We use the same protocol above to train Writer-Dependent classifiers for the validation set, to obtain an estimate of how well the features learned by the models generalize to other users. Finally, we use the best models to train WD classifiers for users in the exploitation set E. We performed 10 runs, each time training a network with a different initialization, and using a random split of the genuine signatures used for training/testing, when training the Writer-Dependent classifiers. We report the mean and standard deviation of the errors across the 10 runs. To compare with previous work, we use exploitation sets of size 160 users (to compare with work that used the dataset GPDS-160), and 300 users (to compare with work that used GPDS-300). To assess the impact of the number of genuine signatures for each user in training, we tested with 5 and 14 training signatures (r \in \{5,14\}). We evaluate the results in terms of False Rejection Rate (FRR - the fraction of genuine signatures misclassified as forgery), False Acceptance Rate (FAR - the fraction of forgeries misclassified as genuine signatures). For completeness, we show the FAR results for both random and skilled forgeries. We also report Equal Error Rates (EER), which is the error when FAR = FRR. In this case, we use only genuine signatures and skilled forgeries, to enable comparison with other work in the literature. We considered two forms of calculating the EER: EER_{user-thresholds} using user-specific decision thresholds; and EER_{global-threshold} using a global decision threshold. Lastly, we also report the Mean Area Under the Curve (Mean AUC), by averaging the AUCs of Receiving Operating Curves (ROC curves) calculated for each user. For calculating FAR and FRR in the exploitation set, we used a decision threshold selected from the validation set (the threshold that achieved EER using a global decision threshold).

IV. RESULTS

We first consider the results of the experiments varying the depth of the networks, and the size of the embedding layer. In these experiments, we trained the CNN architectures defined in table I; used them to extract features for the users in the validation set, and trained Writer-Dependent classifiers for these users, using 14 reference signatures. We then analyzed the impact in classification performance of the different architectures/sizes of the embedding layer, measuring the average Equal Error Rate of the classifiers in the validation set. Figures 1 and 2 show the classification results on the validation set using Linear SVMs and SVMs with an RBF kernel, respectively.
The first thing we notice is that, contrary to empirical results in object recognition (ImageNet), we did not observe improved performance with very deep architectures. The best performing models were the AlexNet architecture (with 8 trainable layers) and the AlexNet_reduced (with 6 trainable layers) when using the features to training linear SVMs and SVMs with RBF kernel, respectively. We also notice that the performance with a linear classifier is already quite good, demonstrating that the feature representations learned in a writer-independent way seems to generalize well to new users.

Another aspect that we investigated is how the signatures from the users in the validation set are represented in the embedding layer of the CNN. For this analysis, we took one of the models (AlexNet_2048, at layer FC2), obtained the representations for signatures of all 50 users in the validation set, and analyzed this representation. We started by analyzing how well separated are the signatures from each user in this feature space, as well as compared to skilled forgeries targeted to the users. To do so, we measured the euclidean distance between genuine signatures of the same user, genuine signatures from different users (i.e. a genuine signature vs. a random forgery), and the distance between pairs of a genuine signature and a skilled forgery made for this user. Figure 3 plots the cumulative frequency of pairs of signatures within a given distance, that is, the fraction of pairs that are closer than a given euclidean distance in the embedding space. For the genuine-genuine pairs, we show the inverse of the cumulative frequency (i.e. the fraction of pairs further than a given distance), to better show the overlap between the curves. For a particular distance, the y axis is the expected False Rejection Rate (on the genuine-genuine pairs) and False Acceptance Rate (on the genuine-forgery pairs) if we used a distance-based classifier, with a single genuine signature as reference. We can see that in the space projected by the CNN, the genuine signatures from different users very well separated: there is a very small overlap between the curves of genuine-genuine pairs and genuine-random forgery pairs. A similar behavior
The zoomed area on the left shows a region where three skilled forgeries (on the top-left) are close to four genuine signatures for user 394 in the GPDS dataset. The zoomed area on the right shows three skilled forgeries for the same user that are far from the genuine signatures in the embedding space. We can see that the skilled forgeries are more scattered around, and for several users, the skilled forgeries are close to the representation of the genuine signatures.

The zoomed-in area in figure 5 shows skilled forgeries made for a particular user that were represented close to genuine signatures from this user. We can see that these forgeries have a close resemblance to the genuine signatures of the user in its overall shape. This is further examined in figure 6, where we take a genuine signature and a skilled forgery from this user, that were close in the embedding space. We can notice that the overall shape of the skilled forgery is similar to the genuine signature, but looking in the details of the strokes we can see that the line quality of the skilled forgery is much worse. We have noticed the same behavior with other users / signatures. This suggests that the features learned by the network are useful in distinguishing the signatures in an “overall shape”, but do not capture important properties of forgeries, such as the quality of the pen strokes, and therefore are particularly not discriminative to slowly-traced forgeries.

Table II shows the detailed result of the experiments in the exploitation set. We noticed that the performance was very good in terms of equal error rates, but that the global decision thresholds from the validation set are only effective in a few situations - in particular, when using the same number of samples as used in the validation set, where the threshold was selected. We also notice that the performance using a global threshold is significantly worse than using per-user thresholds. Note that the values of EER refer to the scenario where the decision threshold is optimally selected, which in itself is a hard task (given the low number of samples per user), and which we did not explore in this paper. Finally, table III compares our best results (using EERuser-thresholds) with the state-of-the-art. We noticed a big drop in classification errors (as measured by Equal Error Rate) compared to the literature, even when using only 5 samples per user for the Writer-Dependent training.

V. CONCLUSIONS

In this work, we presented a detailed analysis of different architectures for learning representations for offline signature verification. We showed that features learned in a writer-independent format can be very effective for signature verification, achieving a large improvement of state-of-the-art performance in the GPDS-160 dataset, with 2.74% Equal Error Rate compared to 6.97% reported in the literature. We also showed that writer-dependent classifiers trained with these features can perform very well even with limited number of samples per user (e.g. 5 samples) and linear classifiers.

Our analysis of the signature representations showed that the learned features are mostly useful to distinguish signatures on a “general appearance” instead of finer details. This make
these features relevant for distinguishing random forgeries and skilled forgeries that are made with quick motion (but do not perfectly capture the overall aspect of the genuine signature). On the other hand, it makes these features less discriminant to slowly-traced skilled forgeries, where the forgery looks like a genuine signature in the overall shape, but has a poor line quality. Future work can investigate the combination of such features with features particularly targeted to discriminate the quality of pen strokes.

ACKNOWLEDGMENT

This research has been supported by the CNPq grant #206318/2014-6.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pp. 4–20, 2004.

[2] L. G. Hafermann, R. Sabourin, and L. S. Oliveira, “Offline Handwritten Signature Verification-Literature Review,” arXiv preprint arXiv:1507.07909, 2015.

[3] D. Impedovo and G. Pirlo, “Automatic signature verification: the state of the art,” Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. 38, no. 5, pp. 609–635, 2008.

[4] D. Rivard, E. Granger, and R. Sabourin, “Multi-feature extraction and selection in writer-independent off-line signature verification,” International Journal on Document Analysis and Recognition, vol. 16, no. 1, pp. 83–103, 2013.

[5] G. Eskander, R. Sabourin, and E. Granger, “Hybrid writer-independent-writer-dependent offline signature verification system,” IET Biometrics, vol. 2, no. 4, pp. 169–181, Dec. 2013.

[6] M. B. Yilmaz, “Offline Signature Verification With User-Based And Global Classifiers Of Local Features,” Ph.D. dissertation, Sabanci University, 2015.

[7] J. Hu and Y. Chen, “Offline Signature Verification Using Real Adaboost Classifier Combosimation of Pseudo-dynamic Features,” in Document Analysis and Recognition, 12th International Conference on, Aug. 2013, pp. 1345–1349.

[8] Y. Guerba, Y. Chibani, and B. Hadjadji, “The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters,” Pattern Recognition, vol. 48, no. 1, pp. 103–113, Jan. 2015.

[9] L. G. Hafermann, R. Sabourin, and L. S. Oliveira, “Writer-independent feature learning for offline signature verification using convolutional neural networks,” in Neural Networks, The 2016 International Joint Conference on, 2016.

[10] B. Ribeiro, I. Gonçalves, S. Santos, and A. Kovacec, “Deep learning networks for off-line handwritten signature recognition,” in Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. Springer, 2011, pp. 523–532.

[11] H. Khalajzadeh, M. Mansouri, and M. Teshnehlab, “Persian Signature Verification Using Convolutional Neural Networks,” in International Journal of Engineering Research and Technology, vol. 1. ESRSA Publications, 2012.

[12] S. Ioffe and C. Szegedy, “Batch normalization: Accelerating deep network training by reducing internal covariate shift,” arXiv preprint arXiv:1502.03167, 2015.

[13] Y. Bengio, “Learning Deep Architectures for AI,” Foundations and Trends in Machine Learning, vol. 2, no. 1, pp. 1–127, Jan. 2009.

[14] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014.

[15] X. Glorot and Y. Bengio, “Understanding the difficulty of training deep feedforward neural networks,” in Artificial Intelligence and Statistics, International conference on, 2010, pp. 249–256.

[16] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” in Advances in Neural Information Processing Systems 25, 2012, pp. 1097–1105.

[17] J. Vargas, M. Ferrer, C. Travieso, and J. Alonso, “Off-line Handwritten Signature GPDS-960 Corpus,” in Document Analysis and Recognition, 9th International Conference on, vol. 2, Sep. 2007, pp. 764–768.

[18] L. Van der Maaten and G. Hinton, “Visualizing data using t-sne,” Journal of Machine Learning Research, vol. 9, no. 2579-2605, p. 85, 2008.

[19] J. Vargas, C. Travieso, J. Alonso, and M. Ferrer, “Off-line Signature Verification Based on Gray Level Information Using Wavelet Transform and Texture Features,” in 2010 International Conference on Frontiers in Handwriting Recognition (ICFHR), Nov. 2010, pp. 587–592.

[20] J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, “Off-line signature verification based on grey level information using texture features,” Pattern Recognition, vol. 44, no. 2, pp. 375–385, Feb. 2011.