

Marcin ADAMSKI¹, Khalid SAEED²

OFFLINE SIGNATURE VERIFICATION USING DIRECTION-BASED SHAPE CONTEXTS

In this paper we present a system for offline signature verification using direction-based Shape Contexts. Images of handwritten signatures were thinned using KMM algorithm and then represented by a set of Shape Context descriptors computed separately in 4 directions in pixel's 8-neighborhood. The distance measure used to compare Shape Contexts was based on L2 norm. The experiments were conducted using signatures from GPDS database.

1. INTRODUCTION

Automatic signature verification is still an active subject of many academic studies. The methods that have been developed already found their applications in commercial solutions. However, as demonstrated by the results of recent works, there is still room for improvements [8], [10]. One of the most difficult problems is the detection of skilled forgeries. Such forgeries are created by impostors who have access to genuine examples and can spend as much time as required to train how to imitate original signature shape. The shape of such imitations is very similar to authentic samples and in many cases it is almost impossible to differentiate them. One way to improve detection of such forgeries is to include information on dynamics of the signing process during comparison [7]. However, in many situations such data is not available and only static signature image can be analyzed. This article presents a method for offline signature verification applied to skilled and random forgeries. The proposed solution takes advantage of information on distribution of directions in the thinned signature image to reduce the system error rate.

2. PROPOSED SOLUTION

In this work we used images of handwritten signatures taken from GPDS database [4] The signatures in this database were collected using a paper form divided into 24 boxes. After collection the signatures were scanned at 300 dpi in 256 gray scale levels and binarized using heuristically selected threshold. In the last step additional preprocessing was applied to eliminate sort of "hair" sticking out from signature strokes that resulted from binarization procedure [4].

The thickness of signature lines depends on the type of pen used for signing and the resolution of the scanning process. In our work we used KMM thinning method [9] to reduce signature

¹ Faculty of Computer Science, Bialystok University of Technology, Bialystok, Poland

² Faculty of Physics and Applied Computer Science, AGH University of Science and Technology, Cracow, Poland

images to a 1-pixel wide skeletons. The process of thinning preserves all information about the signature shape and eliminates redundant pixels contributing to the line thickness. Figure 1 presents an example of a binarized signature image and its thinned version.

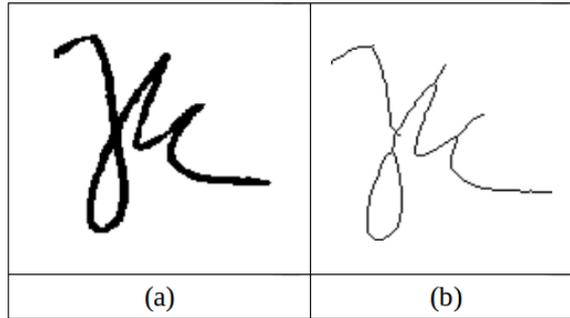


Fig. 1. An example of a binarized signature image (a) and its thinned version (b).

The extraction of features from thinned images was based on Shape Context algorithm [3]. In this approach, the signature is represented by a set of reference points selected along its skeleton. For each of these points a Shape Context descriptor is calculated, that describes the "role" of the point in the entire shape. As the result the signature is described by a set of descriptors, each computed for selected reference point. The following equations represent set of N reference points selected for a signature A (1) and corresponding set of descriptors (2).

$$A = \{a_1, a_2, \dots, a_i, \dots, a_N\} \tag{1}$$

$$A_h = \{h(a_1), h(a_2), \dots, h(a_i), \dots, h(a_N)\} \tag{2}$$

where a_i – i -th reference point selected from signature line, $h(a_i)$ – Shape Context descriptor computed for reference point a_i .

The selection of reference points was carried out by sampling procedure – the algorithm iteratively deletes the signature pixels until only the required number of N pixels remains in the image. The signature pixels selected for deletion in each iteration have the smallest distance from their neighboring pixel. The number of reference points used in this study is $N=150$ and was based on the results of our previous work [1]. An example of a signature and selected reference points can be seen in Fig. 2.

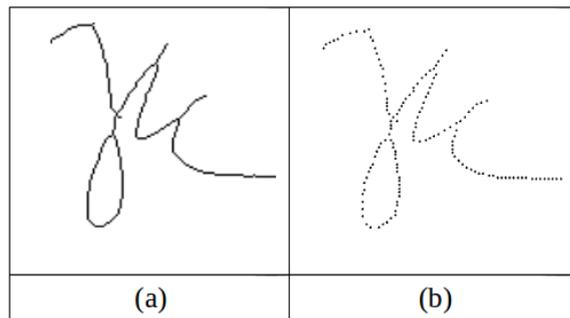


Fig. 2. An example of a thinned signature image (a) and reference points selected by sampling procedure (b).

The Shape Context descriptor for a particular reference point can be computed as a log-polar histogram that describes the distribution of all pixels selected during sampling relative to this reference point [3]. The primary purpose of this description is to facilitate finding the corresponding reference points from two objects when assessing their similarity. In work [2] we also used Shape Context histogram computed as a distribution of all pixels on skeletonized

signature line. This allowed us to reduce the level of error while retaining the same number of descriptors. Figure 3 shows the shape of the histogram with $K=60$ bins that was used in this work.

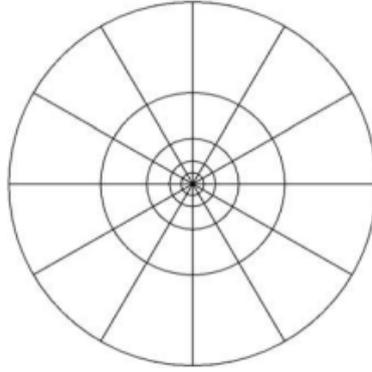


Fig. 3. Log-polar histogram with 60 bins.

In the original form the Shape Context descriptor is based on distribution of points and does not explicitly include information on direction of lines composing the shape of the object. In order to include this information, in this work we introduce direction-based Shape Contexts. For each pixel of the thinned signature image its 8-neighborhood is analyzed to determine if the pixel is positioned along lines in 4 separate directions (top to bottom, top-right to bottom-left, right to left, bottom-right to top-left). Figure 4 shows 8-neighborhood of pixel $p_{i,j}$ and lines in 4 directions.

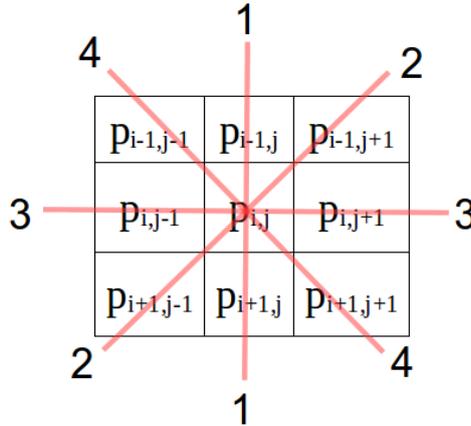


Fig. 4. Pixel 8-neighborhood with 4 directions.

Contributions to each of these directions is accounted in separate histograms according to equations (3-6).

$$h_k^1(a_i) = \sum_{p_{i,j} \in \text{bin}(k) \wedge p_{i,j} \neq 0} p_{i-1,j} + p_{i+1,j} \quad (3)$$

$$h_k^2(a_i) = \sum_{p_{i,j} \in \text{bin}(k) \wedge p_{i,j} \neq 0} p_{i+1,j-1} + p_{i-1,j+1} \quad (4)$$

$$h_k^3(a_i) = \sum_{p_{i,j} \in \text{bin}(k) \wedge p_{i,j} \neq 0} p_{i,j-1} + p_{i,j+1} \quad (5)$$

$$h_k^4(a_i) = \sum_{p_{i,j} \in \text{bin}(k) \wedge p_{i,j} \neq 0} p_{i-1,j-1} + p_{i+1,j+1} \quad (6)$$

where $h_k^l(a_i)$ – k-th bin of the histogram computed for reference point in direction l, $p_{i,j}$ – numerical value of the pixel (0 – background, 1 – signature line) in i-th row and j-th column of the image.

The measure used to compare descriptors of two reference points a_i and b_j from two signatures is given by (7). Here we used a square of L2 norm applied to histograms treated as K-dimensional vectors. Before computation the vectors were normalized to unit length.

$$d_h(a_i, b_j) = \sum_{l=1}^4 \|h^l(a_i) - h^l(b_j)\|^2 \quad (7)$$

where $h^l(a_i), h^l(b_j)$ – histograms of reference points a_i and b_j for direction l.

The total distance between two signatures is the sum of minimal distances between the descriptors of reference points a_i and b_j and is given in (8). This measure was used in this work to assess the similarity between compared signatures.

$$D_h(A, B) = \frac{1}{N} \sum_{a_i \in A} \min_{b_j \in B} d_h(a_i, b_j) \quad (8)$$

3. EXPERIMENTS

In order to assess the proposed method we conducted experiments using signatures from GDPS database. The subset of 640 signatures was used: 8 genuine signatures and 8 skilled forgeries given by 40 individuals randomly selected from GDPS. The training set consisted of 4 genuine signatures for each person (160 samples). The rest of the signatures were included in the test set: 4 genuine signatures and 8 forgeries per individual (480 samples).

During verification every test sample was compared to 4 genuine signatures of a particular individual contained in the training set using the proposed measure. Then, if the minimal value obtained from 4 comparisons was below the threshold, the signature was accepted as an authentic example. Otherwise, it was rejected as a forgery.

In the verification task the most commonly used measures to assess the level of errors are FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error Rate). In the case of signature verification FAR denotes percentage of forged signatures in the experiment accepted as genuine. FRR measures percentage of genuine signatures incorrectly rejected as imitations. The decision to accept or reject given signature depends on the value of threshold. FAR and FRR are functions of this parameter (called Receiver Operating Characteristic curves) and EER is a value of these curves at the point of their intersection.

The following results are shown separately for distance measure using Shape Contexts (denoted as SC and included here for comparison from our previous studies [2]) and direction-based Shape Contexts (denoted as direction-based SC). The experiments were repeated for different selections of reference and test signatures and the average values were computed.

- *Skilled forgeries with shared threshold.*

In this experiment the same threshold value was applied to every individual. Using direction-based SC for skilled forgeries the level of error was reduced from EER=20.6% (obtained with SC) to EER=16.2%

- *Random forgeries with shared threshold.*

The second series of experiments utilized random forgeries. In this case genuine signatures belonging to other individuals are used as imitations. This kind of forgeries are much easier

to detect because they usually have different shape from authentic samples. However, they can be used to assess the verification error in cases where the forger do not know the shape of genuine signatures [6]. The results showed that by applying direction-based SC with shared threshold one can also slightly lower the error rate from EER=4.4% (obtained with SC) to EER=4.1%. However, the improvement is smaller than the one obtained for skilled forgeries. This may result from the fact that the shape of random forgeries significantly differs from the shape of the genuine signatures and basic descriptor is sufficient depict these differences.

- *Skilled forgeries with user-specific threshold.*

We also conducted additional series of experiments with user-specific threshold. In this case the threshold value was computed separately for each individual to adjust for variability among its genuine signatures. The results obtained with user-specific threshold for skilled forgeries showed significant improvement as the error (the average of errors computed separately for each individual) was lowered from EER=8.4% for SC method to EER=3.0% obtained with direction-based SC. It can be also noticed that both methods gave much lower error compared to the results with shared threshold value.

- *Random forgeries with user-specific threshold.*

For random forgeries with user-specific threshold both methods gave almost the same level of error – EER=0.5%. As mentioned earlier this may be attributed to the fact, that random forgeries are easier to detect and basic descriptor can discriminate them as good as direction-based version.

4. CONCLUSIONS

In this paper we presented direction-based Shape Context descriptor applied to signature verification. The results are promising and encourage to further work. The level of error was significantly lowered when using direction-based Shape Contexts. The maximal reduction was obtained for skilled forgeries (EER is reduced from 8.4% to 3.0% with user-specific threshold and from 20.6% to 16.2% with shared threshold). This is an important result because skilled forgeries are most difficult to detect especially in offline systems. Our further work will imply investigating methods for encoding signature line directions and combining them with various classifiers.

ACKNOWLEDGEMENT

This work is partially supported by the Rector of Bialystok University of Technology (grant no. S/WI/2/2013).

BIBLIOGRAPHY

- [1] ADAMSKI M., SAEED K., Offline Signature Identification and Verification using Noniterative Shape Context Algorithm, Journal of Medical Informatics and Technologies, 2009, Vol. 13, pp. 47-58.
- [2] ADAMSKI M., SAEED K., TABEDZKI M., RYBNIK M., Offline signature verification based on shape contexts using shared and user-specific thresholds, Journal of Medical Informatics and Technologies, 2013, Vol. 22, pp. 195-201.
- [3] BELONGIE S., MALIK J., PUZICHA J., Shape Matching and Object Recognition Using Shape Contexts, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, Vol. 24, No. 4, pp. 509-522.
- [4] BLUMENSTEIN M., FERRER M., VARGAS J. F., The 4NSigComp2010 Off-line Signature Verification Competition: Scenario 2, International Conference on Frontiers in Handwriting Recognition, 2010, pp. 721-726.
- [5] IMPEDOVO D., PIRLO G., Automatic Signature Verification: The State of the Art, IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, 2008, Vol. 38, No. 5, pp. 609-635.

- [6] OLIVERA L. S., JUSTINO E. J. R., FREITAS C., SABOURIN R., The Graphology Applied to Signature Verification, 12th Conference of the International Graphonomics Society, 2005, pp. 286-290.
- [7] PALYS M., DOROZ R., PORWIK P., On-line signature recognition based on an analysis of dynamic feature, IEEE International Conference on Biometrics and Kansei Engineering, Tokyo, 2013, pp. 103-107.
- [8] PIRLO G., IMPEDOVO D., Verification of Static Signatures by Optical Flow Analysis, IEEE Transactions on Human-Machine Systems, 2013, Vol. 43, No. 5, pp. 499-505.
- [9] SAEED K., TABDZKI M., RYBNIK M., ADAMSKI M., K3M - A Universal Algorithm for Image Skeletonization and a Review of Thinning Techniques, International Journal of Applied Mathematics and Computer Science, 2010, Vol. 20, No. 2, pp. 317-335.
- [10] SHETE S. S., PATEL S., PANDIT R., Comparative Analysis of Different Approaches for Offline Signature Verification, International Journal of Advanced Electronics and Communication Systems, 2014, Vol. 3, No. 1.