Automatic Signature Stability Analysis And Verification Using Local Features

Muhammad Imran Malik*, Marcus Liwicki*, Andreas Dengel*, Seiichi Uchida†, Volkmar Frinken†
* *German Research Center for AI (DFKI GmbH)*
Knowledge Management Department, Kaiserslautern, Germany
{*firstname.lastname*}*@dfki.de*
† *Faculty of Information Science and Electrical Engineering, Kyushu University, Japan*
{*lastname*}*@ait.kyushu-u.ac.jp*

***Abstract*—The purpose of writing this paper is two-fold. First, it presents a novel signature stability analysis based on signature's local / part-based features. The Speeded Up Local features (SURF) are used for local analysis which give various clues about the potential areas from whom the features should be exclusively considered while performing signature verification. Second, based on the results of the local stability analysis we present a novel signature verification system and evaluate this system on the publicly available dataset of forensic signature verification competition, 4NSigComp2010, which contains genuine, forged, and disguised signatures. The proposed system achieved an equal error rate of 15%, which is considerably very low when compared against all the participants of the said competition. Furthermore, we also compare the proposed system with some of the earlier reported systems on the said data. The proposed system also outperforms these systems.**

***Keywords*-Stability analysis, signatures verification, forensic casework, disguised signatures**

I. Introduction

Automatic signature verification is required in different fields of everyday life. The most important applications appear in banks, governmental, security, financial, and forensic document examination institutions. Since the last few decades, various automatic signature verification systems for both offline (where only spatial information of signatures, e.g., image, is available) and online (where both spatial and temporal information of signatures is available) are reported. In either case, online or offline, the verification problem is usually solved by classifying signatures into two classes, i.e., either as genuine or forged. This classification is helpful in many fields, e.g., banking, but in some areas, e.g., forensic handwriting/signature analysis, another important genre of signatures, i.e., disguised signatures, needs classification. Although in forensic examination, disguised signatures are of high importance [1], they are often neglected by PR researchers [2].

Disguised signatures are usually difficult to identify as they are written by genuine/specimen authors but with intention to deny the authorship later [3]. Signature disguises are mainly performed for fraud e.g., a disguised signature on a bank check can be used to withdraw cash and later on a claim can be made that the check did not contain the original signature. In such a case, it is very difficult for banks/financial institutions to distinguish between genuine and disguised signatures. In addition, it is also not possible to have an expert forensic examiner available in all of the institutes, which require authentication via signatures, who can first analyze signatures and then allow the next step in the routine work flow. It is, therefore, required to enable automatic systems classify the three different genres of signatures, i.e., genuine, forged, and disguised, so that different types of such frauds can be prevented.

In the recent past, various automatic signature verification are reported which perform quite well if the goal is to identify genuine and forged signature [4]. Some commercial systems are already available which are also being used in banking and other financial and institutions [5]. However, to the best of our knowledge, there are only a very few systems capable of disguise classification and most of them have appeared first time in the 4NSigComp2010 signature verification competition [2]. Note that, these systems performed quite poorly when disguised signatures were present in the test set. The best of these systems could reach an Equal Error Rate (EER) of 55%. Considering the above mentioned scenario, there is a strong need for a system which is capable of dealing with genuine, forged, and disguised signatures at the same time with reasonably low EER.

In this paper we propose a novel method for automatic signature verification, capable of dealing with genuine, forged, and disguised signatures at the same time, with comparatively low EER. The proposed method is based on part-based/local stability analysis of signatures, i.e., how consistently similar the signatures' local parts are among multiple genuine signatures written by an authentic author. We applied SURF for performing the local stability analysis and then categorized signature areas as more or less stable. Eventually, we use the knowledge obtained via local stability analysis to perform signature verification. We argue that the proposed method is well suited for such tasks and has provided one of the best results ever reported for the publicly available dataset of 4NSigComp2010, i.e., the first ever signature verification competition with data collected by forensic experts and containing disguised along with genuine and forged signatures [2].

2167-6445/14 $31.00 © 2014 IEEE
DOI 10.1109/ICFHR.2014.109

The rest of the paper is organized as follows. Section II overviews some of the most important related work. Section III provides details about the signature local stability analysis we performed. Section IV details how we applied the knowledge obtained from the local stability analysis to perform signature verification. Section V presents the dataset and evaluation results in terms of Equal Error Rates (EER). Finally, Section VI concludes the paper and provides hints for possible future improvements.

II. Related Work

Signature verification is an active research field since the last few decades. The state-of-the-art of signature verification through different years is summarized in [4], [6], [7]. Nearly all of the state-of-the-art methods have been tested for detection of genuine and forged signatures. However disguised signatures are generally neglected, apart from some initial research, like [6], in some comparative studies of local and global feature based methods, like [8], and in some most recent researches like [9].

[9] presents a system for online forgery and disguise detection which combines online signature features through several classifiers. This system is specific for online verification tasks only, though forensic experts are often interested in offline automatic verification [2].

Disguised handwriting, unlike disguised signatures in general, is previously considered in some PR-research like [10]. However, [10] only focuses disguised and genuine handwriting, without looking into the forgery attempts, and this does not completely suffice the needs of handwriting experts.

The SURF keypoint detector and descriptor, which we have used to initially identify the signatures' local regions of interest to estimate signatures' stable regions, have been previously used heavily for object and character recognition, such as in [11], [12], [13]. In the recent past some signature verification systems based on SURF have been reported, e.g., [14], but have not considered disguised signatures.

We have previously proposed a system which can distinguish between forged and disguised signatures [15]. This system classifies disguised signatures as non-genuine and later they have to be separated from the forged signatures. This system is based on the phenomenon of intention [1], i.e., when a writer wants to disguise her/his signatures, the aim is to make the signatures as far as possible from her/his original signatures but without doing much to the subjective similarities. The intention of a skilled forger, on the other hand, is to go as close to the genuine signature as possible, therefore, skillfully forged signatures should be closer to the genuine signatures while disguised signatures should be far from the genuine signatures.

In general, people (both genuine writers and forgers) follow the intention phenomenon. However, there can be cases where a genuine author knows the intention phenomenon and tries to disguise her/his signatures while keeping them close to her/his genuine signatures (only by adding a small additional stroke, etc.). In both the cases the system presented in [15] will need to first classify between genuine and forged signatures (considering disguised signatures as forgeries) and later in the second pass between forged and disguised signatures where a very bad forgery may be considered as a disguise attempt (if the system is influenced by intention phenomenon) or a very bad forgery is considered as a forgery (if the system is not affected by the intention phenomenon). Then, for a set of mixed disguised signatures (some authors intended to be far from genuine wile some others intended to be closer to the genuine signatures), this two pass scheme may perform poorly. The system proposed in the current paper is not influenced by the intention phenomenon.

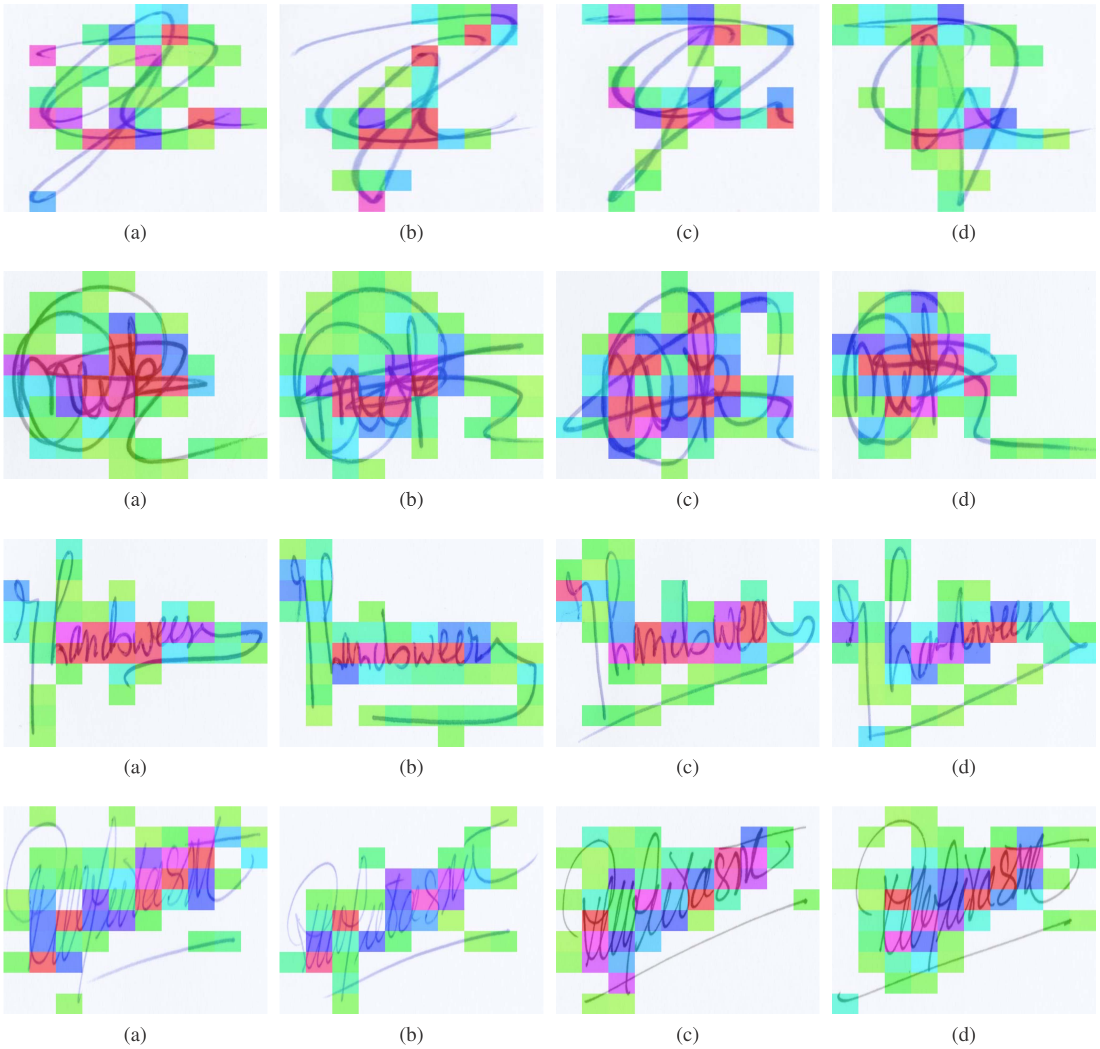
Stability analysis has been studied heavily in the past [16], [17], [18], [19], [20]. Some static signature stability analysis techniques have been proposed that are later used for performing signature verification. For example, [17] uses the regions on the upper and lower contours of the specimen signatures assuming that the upper and lower contours of a signature usually are crucial for performing verification. Similarly, [19] an equi-mass segmentation approach to non-uniformly split signatures into a standard number of regions. Successively, a multiple matching technique is adopted to estimate stability of each region, based on cosine similarity.

All of the above mentioned stability analysis methods are either for online signatures, e.g., [20], or they do not consider disguised signatures. The current paper presents a novel stability analysis method by introducing the use of local methods, like SURF, to the domain of signature stability analysis and applies them for signature verification cases involving disguised signatures. This paper is an initial attempt to take the analysis of local stability of signatures to the much realistic domain of signature verification involving disguised signatures.

III. Local Stability Analysis

Humans generally show the intra-writer or within-writer variations when they write signatures. It is a common observation that if a person writes her/his signatures 'X' times, even by keeping the writing positions, paper, pen, postures, and etc., similar, the signatures vary to a lesser or a greater extent. The analysis of these variations, or more specifically the stability of signatures, is very important and has been previously studied heavily [16], [17], [18], [19]. The signature stability analysis can provide us with various insights into the actual signing processes. In general the stability analysis is performed on global level (by looking at the overall shape changes in the signatures) or on part-based/local level (by looking at the signatures' finer details specific to portions of signatures).

We have performed signature stability analysis in this paper and then combined our findings to design a complete


(a) (b) (c) (d)

(a) (b) (c) (d)

(a) (b) (c) (d)

(a) (b) (c) (d)

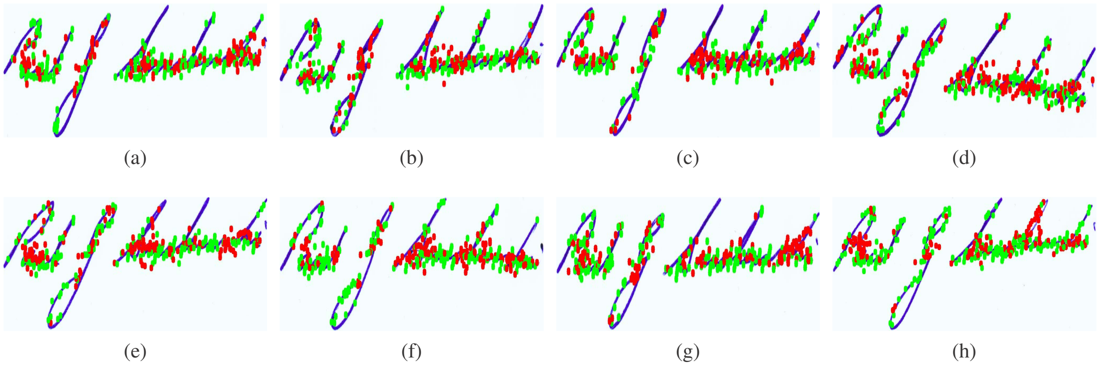
Figure 1. Heat maps of some example specimen (genuine) signatures from four different authors (one genuine author in each row) showing the most stable (green) and the most unstable (red) parts along with the moderately stable parts (colors varying from green to red through blue).

signature verification system. The first important decision about performing such an analysis is to whether perform it at global, or local, or both the levels simultaneously. We opted to perform the stability analysis at local level since we wanted to explicitly consider disguised signatures and it is a common practice of authors, while disguising their signatures, to keep the entire signature similar to their original signatures except adding or removing a tiny portion or certain strokes. We, therefore, chose to perform local stability analysis of signatures as local features are least affected by such changes [8], [21].

We analyzed the local stability of signatures via Speeded Up Robust Features (SURF) [11]. SURF represent an image/signature as a set of keypoints. SURF is a robust, translation, rotation, and scale invariant representation method. It is partially inspired by Scale Invariant Feature Transform (SIFT) [22]. SURF detects blob like structures from images and uses integral images to compute Hessian matrix. Like other part based approaches, SURF extract keypoints/points of interest from parts of image (which represent local features) where the determinant of Hessian is maximum, thus bringing robustness against different variations in the image [12], [13]. A 128 bit descriptor is extracted, for each of the keypoints, that represents the keypoint. This descriptor is used to find similarity between different keypoints. For the extraction of SURF features we used a Hessian threshold of 1000, i.e., all the keypoints having a Hessian value less than 1000 were neglected. This filtering was done to neglect potentially unimportant features from the signatures.

The following hypotheses framed the foundation of our analysis.

- H1: The stability is not homogeneously distributed across the signature. In other words, keypoints from some areas will give more stable results than those from



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 2. Example genuine reference signatures of one author. Green points are considered to be stable and are added to the reference keypoints database for performing verification. Red points are considered unstable and are not included in the reference keypoints database.

the other areas.

- H2: The stability behavior is generalizable to other authors.

To verify our hypotheses we performed experiments on the genuine reference signatures of various authors. The stability analysis is performed as follows. First of all, for every author available in the dataset, we took one genuine signature, let it be ’A’, from the set and extracted keypoints from the remaining genuine signatures of that author. This made the reference signature database for comparing the distances of keypoints of signature ’A’ with that of its database. SURF keypoints are extracted from signature ’A’ and these distances are compared with the concerned keypoints database. The Euclidean distance of every keypoint is calculated from the database and is assigned to a matrix. We repeated this in an ’n-1 cross validation’ manner and get the distances of each keypoint from the concerned reference keypoints dataset. After normalizing the values, we took the sum of these values as the actual color of a bin in the histogram (each bin contains the sum of individual keypoint distances from the reference authors dataset for that author).

Figure 1 shows some example heat maps along with the superimposed original genuine signatures from four different specimen authors. It highlights the areas of signatures which are most stable and which are most unstable for each of the four genuine signatures of the specimen authors. Note that for each genuine signature, different areas can be stable or unstable. The goal is to identify regions, whose keypoints can confidently be used for classification. We define how stable a region is, by the proximity of the keypoints to a reference keypoints dataset. The white colored bins show the absence of any keypoints in that particular bin while the colors varying from green through blue to red indicate the bins having keypoints. The green color shows the stable regions, i.e., the regions having the keypoints which are at a minimum distance from the reference keypoints dataset. The red color shows the portions of the examined signature which are at the maximum distance from the reference keypoint database. If a part of a query signature has more similar parts in the reference (genuine) signature database, the heat map value at that part becomes closer to green. By inspecting the genuine specimen signatures of various authors, it is revealed that:

- The first hypothesis, ’H1’, can only be partially proved. The intersection parts for most of the genuine signatures are often unstable (so, shape around the intersection is unstable). However, this is not generalizable to all the intersection cases.
- The second hypothesis, ’H2’, is also verified partially where we found that the ascending and descending parts are often stable (even though they show a keen curve). Further analysis is required to solidify these findings.

Note that this heat map representation was directly realized because the presented analysis is based on a part-based method. If not, we need an elaborated non-linear registration method to evaluate this local stability. The basic idea for utilizing the results of this analysis for the classification task is thus to use the keypoints in the regions which are known to have higher stability in general observation, e.g., a classification excluding most of the keypoints in the middle areas of reference genuine signatures.

IV. Signature Verification

The following procedure is followed to perform signature verification.

1) Compute the keypoints from all the genuine specimen signatures of an author except only one genuine reference signature and make a temporary keypoints database.
2) Compute the keypoints from the remaining genuine reference signature and compare the distances of all of its keypoints from the temporary keypoints database.
3) Find the average distance and then mark all keypoints having distance less than or equal to the average distance as green and all other keypoints red. Figure 2 shows these examples for eight different genuine

Table I
SUMMARY OF THE COMPARISONS PERFORMED.

System	Features	FAR	FRR	EER
1 [23]	Contour features	1.1	90	80
2 [2]	Different global statistics	41.1	90	58
3 [2]	Local and global combination	20.0	70	70
4 [2]	Gradient features	0.0	80	70
5	Unknown-commercial product	13.3	80	55
6	Unknown-commercial product	87.0	10	60
7 [2]	Local and global combination	1.1	80	70
8 [24]	SURF-FREAK	30	30	30
9 [24]	FAST-FREAK	30	30	30
10 [21]	Local sliding window	20	20	20
Proposed	Locally stable SURF	15	15	**15**

specimen signatures of an author. The final reference keypoints database will contain only the green (stable) keypoints.

4) Repeat this process for every genuine specimen signature in an 'n-1 cross validation manner' and populate a final reference keypoints database using only the stable keypoints from different reference/specimen signatures.
5) Once the final reference keypoints database is created, keypoints and descriptors are extracted for the query/questioned signature. A comparison is made between the query signature keypoints and the keypoints present in our final reference keypoints database for that particular author.
6) Find the local keypoints from the query signature by using SURF. Then take the first keypoint of the query Image and compare it with all the features present in the final reference keypoints database, one by one. If a query signature keypoint is at a distance less than an empirically found threshold θ, note the keypoint. Keep this process going until all the query signature's keypoints are traversed.
7) Finally, calculate the probability of each query signature being genuine by considering the total number of query keypoints and the query keypoints matched with the final reference keypoints database. This represents the average local features of the questioned signature that are present in final reference keypoints database of that author.

Figure 2 shows that for curved lines/strokes (intersections) usually a large number of keypoints mismatched. Hence, our initial findings point that genuine specimen authors themselves, in most of the cases, do not write very stable intersecting strokes and, therefore, these strokes can be neglected while performing verification.

V. EVALUATION

A. Dataset

The evaluation set of the 4NSigComp2010 signature verification competition was used. This is the first ever publicly available dataset containing disguised signatures. The collection contains 125 offline signatures. There are 25 reference signatures by the same reference/specimen writer and 100 questioned signatures by various writers. The 100 questioned signatures comprise 3 genuine signatures written by the reference writer in her/his normal signature style and 7 disguised signatures written by the reference writer where s(he) tried to disguise herself/himself (the reference writer provided a set of signatures over a five day period); and 90 simulated signatures (written by 34 forgers freehand copying the signature characteristics of the reference writer. The forgers were volunteers and were either 'lay-persons' or calligraphers.). All writings were made using the same make of ball-point pen and using the same make of paper.

B. Results

As mentioned above, our evaluation data contained 3 genuine, 7 disguised, and 90 forged signatures. This is not a problem for the evaluation since we computed the Equal Error Rates (EER), calculated when the False Reject Rate (rate at which genuine and/or disguised signatures are misclassified as forged by a system) is same as the False Accept Rate (rate at which forged signatures are misclassified as genuine by a system).

We used the same experimental protocol as was used in the 4NSigComp2010. For training, 25 genuine reference signatures were available and after training on these 25 genuine reference signatures our systems had to classify correctly the 100 questioned signatures (the test set). Note that, no forgery sample was used for training the proposed system. This is a realistic forensic scenario [2] and is posed in the 4NSigComp2010. We performed various tests and in total we provide a comparison of our newly proposed system with ten other systems (seven systems are the participants of the 4NSigComp2010 signature verification competition while the remaining three are the later reported systems on the same data).

As shown in Table I, our newly proposed system outperforms all the participants of the 4NSigComp2010 signature verification competition as well as all the other systems. The best system from the competition could achieve an EER of 55% in presence of disguised signatures in the test set while the best later reported system achieved an EER of 20%. The newly proposed system however achieves an EER of 15% which is remarkable when compared to the other systems.

A potential reason for the better performance of the proposed system can be that the proposed system exclusively considers the information available in the local areas of genuine reference signatures and while making a model for an author removes all the unstable features already. This sort of feature selection provides a good opportunity for the proposed system to base the final output strictly on the features which are very stable for an author.

VI. Conclusion and Future Work

In this paper we have presented a novel part based system based on local stability analysis for forensic signature verification involving disguised signatures. Local stability analysis provides various clues about the stable and unstable regions of genuine signatures. Therefore, while making a genuine reference model, the features from unstable regions can be neglected and a better user model could be formed for performing signature verification. We used SURF for local stability analysis and proposed signature verification system based on the results of this analysis. The proposed systems outperformed all the participants of the 4NSigComp2010 signature verification competition by achieving an EER of 15%. Whereas the EER of the best participant in the said competition was 55%. Furthermore, the proposed system has also outperformed all the systems that have been reported on the publicly available 4NSigComp2010 signature verification competition data to date.

In the future, we plan to use larger data sets where disguised signatures from large number of authors are present in the test set. Regarding the systems' outcomes, we plan to enable them produce likelihood ratios according to Bayesian approach, which will make these systems even more useful in the real world forensic casework.

References

[1] L. Michel, "Disguised Signatures," *Journal of the Forensic Science Society*, vol. 18, pp. 25–29, 1978.

[2] M. Liwicki, C. E. van den Heuvel, B. Found, and M. I. Malik, "Forensic signature verification competition 4NSigComp2010 - detection of simulated and disguised signatures," in *ICFHR*, 2010, pp. 715–720.

[3] J. Sita, B. Found, and D. Rogers, "Forensic handwriting examiners' expertise for signature comparison," *Journal of Forensic Sciences*, vol. 47, pp. 1117–1124, 2002.

[4] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Trans. on Systems, Man, and Cybernetics (Part C)*, vol. 38, no. 5, pp. 609–635, Sep. 2008.

[5] D. Impedovo, G. Pirlo, and R. Plamondon, "Handwritten signature verification: New advancements and open issues," in *ICFHR*, 2012, pp. 367–372.

[6] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification – the state of the art," *Pattern Recognition*, vol. 22, pp. 107–131, 1989.

[7] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: A comprehensive survey," *IEEE TPAMI*, vol. 22, pp. 63–84, 2000.

[8] M. I. Malik, M. Liwicki, and A. Dengel, "Evaluation of local and global features for offline signature verification," in *AFHA*, 2011, pp. 26–30.

[9] A. Hassaine and S. Al-Maadeed, "An online signature verification system for forgery and disguise detection," in *Neural Inf. Process.*, ser. LNCS, 2012, vol. 7666, pp. 552–559.

[10] C. D. Stefano, A. Marcelli, and M. Rendina, "Disguising writers identification: an experimental study," in *IGS*, 2009, pp. 99–102.

[11] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-Up Robust Features (SURF)," *Comput. Vis. Image Underst.*, vol. 110, no. 3, pp. 346–359, Jun. 2008.

[12] W. Song, S. Uchida, and M. Liwicki, "Comparative study of part-based handwritten character recognition methods," in *ICDAR*, 2011, pp. 814–818.

[13] D.-N. Ta, W.-C. Chen, N. Gelfand, and K. Pulli, "Surftrac: Efficient tracking and continuous object recognition using local feature descriptors," in *CVPR*, 2009, pp. 2937–2944.

[14] S. Pal, S. Chanda, U. Pal, K. Franke, and M. Blumenstein, "Off-line signature verification using g-surf," in *ISDA*, 2012, pp. 586–591.

[15] M. I. Malik, M. Liwicki, and A. Dengel, "Part-based automatic system in comparison to human experts for forensic signature verification," in *ICDAR*, 2013, pp. 872–876.

[16] G. Pirlo and D. Impedovo, "On the measurement of local stability of handwriting: An application to static signature verification," in *BIOMS*, 2010, pp. 41–44.

[17] D. Impedovo and G. Pirlo, "Stability analysis of static signatures for automatic signature verification," in *ICIAP*, ser. LNCS, 2011, vol. 6979, pp. 241–247.

[18] D. Impedovo, G. Pirlo, L. Sarcinella, E. Stasolla, and C. Trullo, "Analysis of stability in static signatures using cosine similarity," in *ICFHR*, 2012, pp. 231–235.

[19] G. Pirlo and D. Impedovo, "Cosine similarity for analysis and verification of static signatures," *Biometrics, IET*, vol. 2, no. 4, pp. 151–158, 2013.

[20] A. Parziale, S. Fuschetto, and A. Marcelli, "Exploiting stability regions for online signature verification," in *ICIAP*, ser. LNCS, 2013, vol. 8158, pp. 112–121.

[21] M. Liwicki and M. I. Malik, "Surprising? power of local features for automated signature verification," in *IGS*. International Graphonomics Society, 6 2011, pp. 18–21.

[22] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. J. Comput. Vision*, vol. 60, no. 2, pp. 91–110, Nov. 2004.

[23] A. Gilperez, F. Alonso-Fernandez, S. Pecharroman, J. Fierrez, and J. Ortega-Garcia, "Off-line signature verification using contour features," in *ICFHR*, 2008.

[24] M. Malik, S. Ahmed, M. Liwicki, and A. Dengel, "Freak for real time forensic signature verification," in *ICDAR*, Aug 2013, pp. 971–975.