Real-Time Feature-Based Automatic Signature Verification

M. Shridhar, G. Houle, R. Bakker, F. Kimura

Real-Time Feature-Based Automatic Signature Verification

M. Shridhar
University of Michigan-Dearborn, USA
mals_97@yahoo.com

G. Houle
Kappa Image LLC
gilles.houle@kappaimage.com

R. Bakker
DIA Europe BV
ron.bakker@diaeurope.com

F. Kimura
Mie University, Japan
kimura@hi.info.mie-u.ac.jp

Abstract

Automated signature verification is an important capability when doing fraud detection from high volumes of document images. The challenge is mainly caused by the combination of inherent writer variations and the conscious attention placed by the fraudster on imitating a legitimate signature. Getting good signature references is the first and most important step affecting verification accuracy. Typical production systems use signature cards which have one or more signature variations. In this paper, we show the improvement in verification accuracy from increasing the number of signature references used in verification processing. As many as 20 signature references were used. In production operations, comparing a sample signature to more than one or two reference signatures using current methods requires too much processing time. The main contribution of this paper is the description of a feature-based approach that allows for matching of a sample signature against a large number of reference signatures in real-time thereby achieving improved accuracy without a significant performance penalty.

Keywords: Signature, Verification, Forgeries, Checks.

1. Introduction

The primary motivation for this study arose from the need of financial institutions to stem the rising tide of significant losses due to fraudulent financial instruments. The financial institutions needed a verification system that would detect at least 80% of fraudulent checks or giros (financial instrument used in some European countries) while rejecting no more than 10-12% of all genuine checks.

In real live production when using one ore two signature references (i.e. signatories) the false positive rate is too high to detect skilled forgery. In applications such as check or giro processing, extracting a clean signature is often a challenge because of the printed text added by transport to mark and track items. Recent efforts by some financial institutions have lead to collection of historical data to better capture signature variations for a specific account. It may contain one or more signature writers, and it may contain instances where more than one signature is required on the given documents depending on the amount or other account parameters.

Keeping more than two signatories is a concern because of the memory requirements (2K-5K per snippet) and privacy issues. Furthermore current image-based signature verification are too slow (0.5-2 sec per verification) to consider using a large number of references. This leads to the proposed approach where each reference signatures is converted to a small number of pre-computed features resulting in verification speeds in excess of 60 verifications per second.

A survey of existing literature reveals a vast amount of research directed towards automatic signature verification (ASV) with a focus on detection of forgeries. There are far too many papers to cite in this area [1 – 14]. However, the authors refer the reader to the works of Sabourin et al [1], Fang et al [2], Plamondon et al [4-7] for some insightful ideas and methodologies. It is difficult to do a fair comparison unless a common signature reference database is provided. Most researchers have created databases using "controlled"/"ideal" conditions, which serves some analytical purposes. However the current paper is entirely based on real fraud cases that caused major losses to US banks. In successful fraud cases, most of the signatures are skilled forgeries, where the forgers practice to achieve a genuine representation of the account holder's signature.

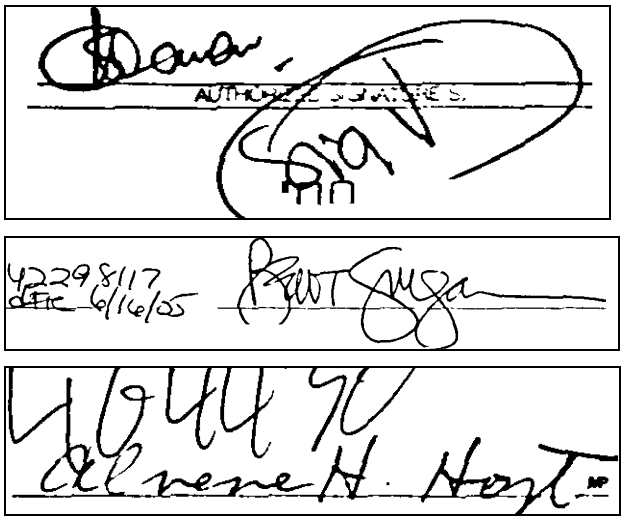

Figure 1. Images that have signature fields with artifacts

In this paper the authors emphasize the importance of using multiple references to capture the inherent signature variations that a signer normally exhibits when signing a document. Figure 1, illustrates typical signature artifacts that may be present in the field. The major challenge with addressing detection of forgeries start with the capture of a "clean" signature image from a given document without including overhangs from other fields in a document, printed text that overlaps with the signature and other artifacts introduced by the processor of checks or giros.

This paper is organized into multiple sections. Section 2 describes the basic concepts behind our automated signature verification approach. Section 3 describes the global and local features used in the ASV system as well as the algorithm to determine quantitatively a confidence measure for verification of the test signature. Section 4 presents the results of extensive testing with real-world signatures extracted from financial documents including bank checks. Section 5 summarizes our findings and proposes future directions.

2. Feature-Based ASV

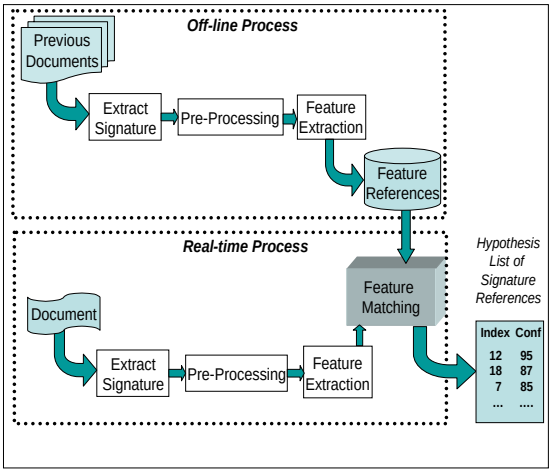

Figure 2: Feature-based ASV adapted to each account.

A big challenge faced by financial institutions is that would-be fraud perpetrators may find ways to acquire critical image data containing valuable information about the account holder, such as images of legitimate signatures. This data exists primarily because machine recognition of signatures and other fields in a document necessarily requires storage of document images in computers that are subject to unauthorized access. Furthermore, current ASV methods of detecting forgeries by comparing signatures to multiple reference images is generally slow, often limited to one or two verifications per second.

A novel solution to the problem is derived. If only features derived from signature reference images rather than the signature images themselves are stored in the computers, then the actual signatures are not exposed to unauthorized access. Forgers have very little use for feature data since those features do not help them to make signature forgeries. Secondly, since only the features from a test signature are required to be computed, automatic recognition with multiple reference signatures is much faster and more reliable. Finally, the amount of storage required to store the features from a large number of signature references is no larger than a typical image snippet for a single signature.

2.1. Description of Features

The selection of features from a given signature is very critical to the overall performance of the verification system. A survey of existing literature reveals a wide diversity of features that have been proposed for signature matching. These include regional features such as

- pixel distribution in a rectangular grid superimposed on the image
- chain code distribution in a rectangular grid superimposed on the image
- top and bottom profiles of the signature image
- height distribution across the image
- white run distribution in a horizontal scan of the image
- peaks in the top and bottom profile
- distribution of zero crossings in the binarized signature image
- curvature distribution in the binarized image

In addition to regional features, global features also play a key role in verification. These include

- an estimate of the slant of the signature
- aspect ratio of the signature image
- overall pixel density
- maximum zero crossing in horizontal scans
- presence or absence of underlines in the signature image

While many of these features work well if the signature images are relatively clean, they generally perform poorly if the images include artifacts that are not part of the signature. Also global features are generally only useful for rejecting a signature providing little help in a decision to accept a signature as legitimate.
It is also important to realize that some form of normalization (either in the image space or the feature space) is often required to compensate for the size variations of test and reference signatures. The underlines that frequently appear in the signature areas of documents may often have to be erased from the images if bottom profiles of the signature are to be extracted.

The study described in this paper deals with signature images extracted from bank checks. The reference signatures are extracted from previously processed checks and confirmed to be legitimate. The binary images were generated by a camera with a resolution set at 240 dpi. The main observation with regard to the captured images is the presence of significant noise and

artifacts in the signature area. It is therefore very important that these artifacts be suppressed as much as is feasible prior to signature verification processing. Another observation is the inconsistency in the signature patterns. These inconsistencies may stem from the mood for when the check was signed.

The actual features used in this study consisted of regional features and global features as listed below:

- pixel distribution in a rectangular grid superimposed on the image
- edge (or chain code) distribution in a rectangular grid superimposed on the image
- slant
- pixel density
- aspect ratio

The global features (slant, pixel density and aspect ratio) were only used to decrease the verification confidence, based on observed differences. Dynamic warping was used to match the signature being analyzed against the reference signatures before a verification score was derived. A score was derived for each of the features and a composite score was then obtained as a weighted average of the individual scores.

2.2. ASV Based on Dynamic Feature Matching

We now describe the match function $f(x, y)$ between a reference and unknown. The features used are labeled as follows:

1. Pixel distribution over a grid of (MxN) – PixRef[i, j] and PixTest[i, j] for i = 1,2, …, M and j = 1, 2, …, N
2. Four-directional chain code distribution over a grid of (KxL) – EdgeRef[i, j] and EdgeTest[i, j] for i = 1,2, …, M and j = 1, 2, …, N (shown in Figure 4)
3. Pixel Density across image –PixRef and PixTest
4. Aspect Ratio – AspREf and AspTest
   Slant of image – SlantRef and SlantTest

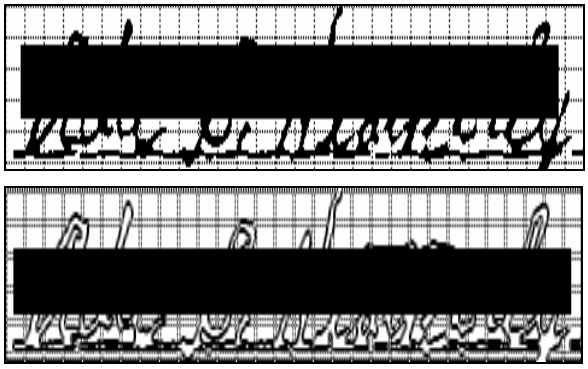

Figure 3 Signature Image with a Superimposed Grid for Extraction of Pixel and Chain Code Features (Signature Masked for Privacy)

Figure 3 shows the signature image with superimposed grid. All the images were normalized to a standard size of (75x300) pixels before the features were extracted from the images. The features for reference images were pre-computed and stored for use in verification. Pre-computing the reference image features resulted in considerable savings of CPU time during ASV processing.

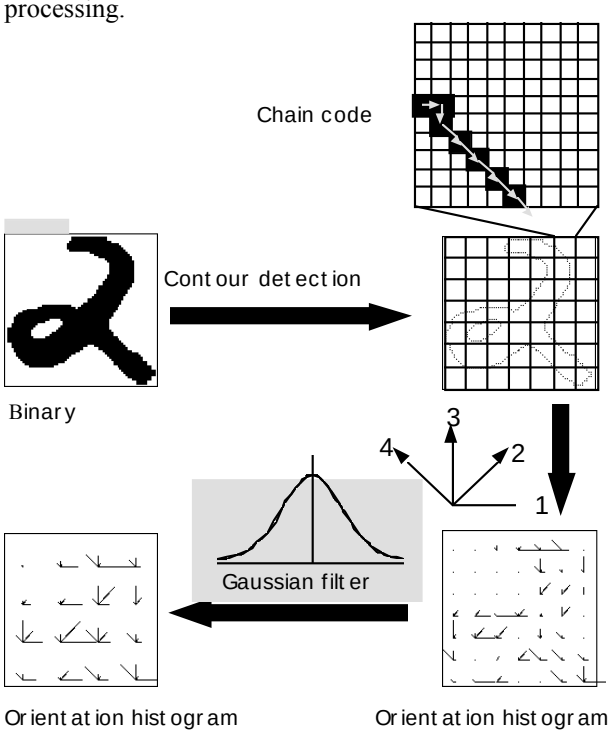

Figure 4 Features derived from contour chain code

For the pixel distribution features dynamic warping was used to derive a cost which was normalized to the range 0 – 1000. For the chain-code features, both Euclidean and weighted distances are computed and normalized to the range of 0 – 1000. The weighted distance is calculated as shown below:

$$g(X) = \sum_{i=1}^{k} \{\Phi_i^T (X - M)\}^2 / \lambda_i$$

The Euclidean distance is defined below:

$$d(X) = |X - M|^2$$

Here X denotes the test feature vector, M denotes the reference feature vector and Φ_i denotes the eigenvectors of the feature covariance matrix, λ_i is the i-th eigen value and k is the number of eigen vectors used. The global features were compared to derive a score in the range of 0 – 1000 as follows:

PixDensity Cost = 2000*abs (PixRef -PixTest)/(PixRef + PixTest)

AspRatio Cost = 2000*abs (AspREf - AspTest)/(AspREf + AspTest)

The slant feature was only used to penalize the final measure of similarity between the test and reference signatures if the relative difference is larger than 15%.

For each feature that is used in this study, a measure of similarity was derived as

Similarity[i] = 100*(1 – Cost[i]/1000), i = 1, 2, 3, and 4

Thus if the two signatures are identical, then we would obtain a similarity measure of 100%. A weighted sum of the similarity scores was computed to obtain the overall similarity measure:

$$Total\_Score = \sum_{i=1}^{4} W[i] * Similarity[i], \qquad \sum_{i=1}^{4} W[i] = 1$$

The weights W[i] were determined empirically based on the effectiveness of each feature used in this study.

2.3. Multi-References ASV Match Function

Now that we have a function *f(x,y)* to match a reference against an unknown signature, we need to formulate how we use all the reference signatures to come up with a final score. For instance we could use the maximum match values between the unknown and all the references but it may be sub-optimal compared to account specific adaptive measures as we present below. Also an important question that we have answered in this paper is whether or not all the reference signatures should be used. Some of the references may be poorly extracted and thus reduce the match value. So some selection criteria had to be devised and now formalized.

Let R_k^a (k=1, 2... K) be a subset of the genuine reference signatures from account *a* (*a*=1,2,…,X). Then let T_j^a (j=1, 2… J) be the test signatures for account *a*. A match value can then be calculated by the average match to the references, i.e.

$$M_j^a = \frac{\sum_{k=1}^{K} f(T_j^a, R_k^a)}{K} \qquad (1)$$

where *f(x,y)* is the signature matching function between *x* and *y* described in 2.2. It returns a match value between 0 (reject) to 100 (excellent).

Since we have up to K=20 possible reference signatures per account we can calibrate the match value and renormalize the match based on the average match and standard deviation for that account. In other words we apply equation (1) on the reference values, i.e.,

$$N_j^a = \frac{\sum_{k=1,k\neq j}^{K-1} f(R_j^a, R_k^a)}{K-1} \qquad (2)$$

We can then compute the average and standard deviation of the N_j^a values.

$$\overline{G}^a = \frac{\sum_{j=1}^{K} N_j^a}{K} \quad \text{and} \quad \sigma_{G^a} = \frac{\sum_{j=1}^{K} (N_j^a - \overline{G})^2}{K} \qquad (3)$$

With the *a priori* knowledge of the average and standard deviation of the reference match values we can normalize the distribution as:

$$\widetilde{M}^a = \frac{(M^a - \overline{G}^a)}{\sigma_{G^a}}$$

We then have a distribution with average 0 and standard deviation of 1. To remap this value to a value between 0 and 100 we applied a linear mapping so that 2 (i.e., average match + 2 times the standard deviation) is 90 and -5 (i.e., average match – 5 times the standard deviation) is 0.

$$M^x = 64.28 + 12.85 \bullet \widetilde{M}^x \qquad (4)$$

Clearly this value may be less than 0 for very bad match and above 100 for extremely good match. The match value was truncated to be between 0 an 100.

Finally it is important to mention that the number of references (i.e., K) is a parameter that varies from 2 to 20. The selection criterion used to pick the next reference is the most centered (based on Euclidean distance) of the remaining references.

3. Results

A total of 85 accounts (50 of which contained real fraudulent signatures) were used in this test. For each account, at least 20 genuine signatures were available for the reference set and 5 to 30 signature images were available for testing. Ideally a genuine match should get a match value computed from equation (4) closer or above 100 and a fraudulent signature should be closer or below 0. One of the interesting finding depicted in figure 5 is that above 12 references the performance degraded.

In all there were 1778 genuine signatures and 151 confirmed fraudulent signatures. The genuine signatures had an average match and standard deviation of 66.25 and 22.6, respectively. The fraudulent signatures had an average match and standard deviation of 15.96 and 20.0, respectively.

Even though 20 or more reference signatures were available from the TRAINING set, we wanted to determine the impact on verification accuracy as we increased the number of references used in matching. We set the false negative rate at 10% (no more than 10% of the actual fraud items accepted as legitimate) and then measured the false positive rate (rejection of genuine cases) as we increased the number of reference signatures.

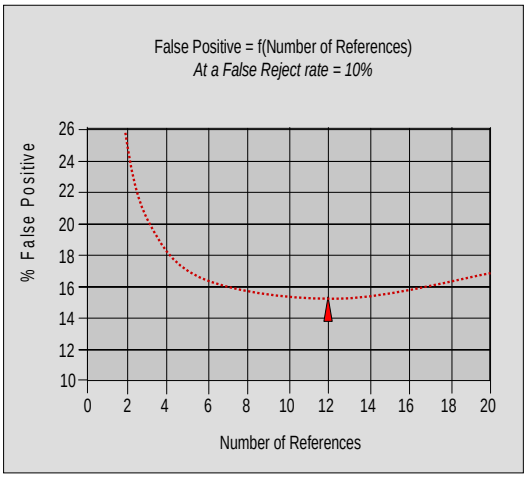

Figure 5: False Positive as a function of number of references

Figure 5 clearly shows that using more than 12 references doesn't help in reducing the false positive percent. In fact the false positive rate increases when using more references.

This may appear abnormal but after further analysis of the 20 possible references some available candidates may be of such poor quality that they may allow bad input signatures to be accepted.

Once the optimal number of references has been determined, we then measured the performance as a function of the reference threshold. Accordingly, Figure 6 shows the cumulative distributions for genuine and fraudulent signatures when using 12 references.

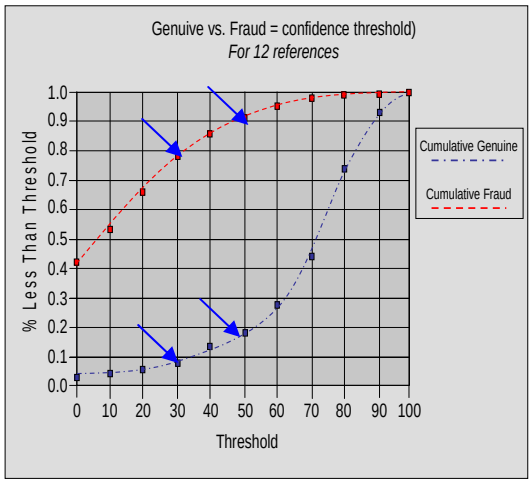

Figure 6: Cumulative Distributions for Genuine and Fraud Sign

For example at a threshold of about 30, almost 80% of the actual fraudulent signatures are identified while only about 10% of the genuine signatures are identified as forgery suspects (false positive rate). At a threshold of 48, almost 90% of the fraudulent signatures are identified while the number of genuine signatures identified as forgery suspects increases to 16% of the total genuine signatures. Additional strategies that are outside the scope of this paper are available to further improve the detection of forgeries and reduce the rejection of genuine documents identified for review.

The overall measure is computed for a given matching threshold T below which the signature is rejected. For those above or equal to T we can calculate the false positive rate FP = flagged-fraud / flagged. It is noteworthy to observe that 12 feature references fits in less than 2 kilobytes.

It is interesting to observe that 40% of the fraudulent signatures are identified at the threshold setting of zero. Due to the normalization that is performed (see equation 4), thresholds would have to be set to negative values to falsely accept forged signatures. It was also observed that 1.2% of the genuine signatures are also falsely rejected at the threshold setting of zero.

4. Conclusions

In this paper we have presented an Automatic Signature Verification system based on features extracted from signature images. The main advantages of the proposed technique are summarized below.

- The proposed ASV matches against multiple signature references, which increases accuracy.
- It is only necessary to store pre-computed features for each account.
- Because features for the reference images are pre-computed, a significant reduction in CPU utilization for much faster processing is realized.
- Binary signature images captured at 240 dpi can be processed at a rate exceeding 70 images per second.
- Furthermore the amount of storage required to store features from a large number of reference signatures is about the same as that required for storing a single reference image.
- The feature references contain no visual representation of potential use to fraud perpetrators thereby reducing exposure to fraud losses should would-be fraud perpetrators find ways to access this data.
- The proposed technique to select references from previous transactions provides financial institutions with a cost-effective solution to creating signature databases to replace or complement signature cards.

With enhanced features further improvements in false rejection and false acceptance can be achieved. The authors are also testing a second feature-based ASV engine to further increase accuracy.

Acknowledgment

The authors gratefully acknowledge Jim Mason (president of Kappa Image LLC) and Johan Berkhuysen (director of DIA Europe BV) for their valuable comments and suggestions.

References

[1] Edson J. R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, "An Off-Line Signature Verification System Using HMM and Graphometric Features", DAS 2000.

[2] Robert Sabourin: Off-Line Signature Verification: Recent Advances and Perspectives. 84-98, Brazilian Symposium on Document Image Analysis (BSDIA 1997)

[3] F. Bauer, and B. Wirtz, “Parameter Reduction and Personalized Parameter Selection for Automatic Signature Verification”, ICDAR-1995 183-186 pp

[4] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification - The State of the Art", *Pattern Recognition*, Vol. 22, No. 2, pp. 107-131, 1989.

[5] F. Leclerc and R. Plamondon, "Automatic Signature Verification: The State of the Art - 1989-1993", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 8, No. 3, pp. 643-660, 1994.

[6] R. Plamondon and S. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey", IEEE Transactions on PAMI, Vol. 22, No. 1, pp. 63-84, 2000.

[7] J-J. Brault and R. Plamondon, "Segmenting Handwritten Signatures at Their Perceptually Important Points", IEEE Transactions on PAMI, Vol. 15, No. 9, pp. 953-957, 1993.

[8] A. Zimmer and L. L. Ling, "Preprocessing: Segmenting by Stroke Complexity", Proceedings of the VI Iber-American Symposium on Pattern Recognition, pp. 89-94,.Florianópolis, Brazil, 2001.

[9] W. Guerfali and R. Plamondon, "The Delta LogNormal Theory for the Generation and Modeling of Cursive Characters", Proceedings of the ICDAR, Vol. 2, pp. 495-498, 1995.

[10] L. O’Gorman, "Curvilinear Feature Detection from Curvature Estimation" , Proceedings of the 9th International Conference on Pattern Recognition, pp. 1116-1119, 1988.

[11] R. Sabourin. and G. Genest, “An extended Shadow-Code Based Approach for Off-Line Signature Verification: Part I – Evaluation of the Bar mask Definition”, Proceedings of the IAPR, pp. 450-455, Jerusalem, Israel, 1994.

[12] K. V. Mardia, “Statistics of Directional Data”, Academic Press, 1972.

[13] J. P. Drouhard, R. Sabourin and M. Godbout, "Neural network approach to off-line signature verification using directional PDF", Pattern Recognition, Vol. 29, No. 3, pp. 415-42, 1996

[14] Jinhong K. Guo, David Doermann, Azriel Rosenfeld, "Off-Line Skilled Forgery Detection Using Stroke and Sub-Stroke Properties," *icpr*, p. 2355, 15th International Conference on Pattern Recognition (ICPR'00) - Volume 2, 2000.