Personal Authentication Using Signature Recognition

Diana Kalenova

Department of Information Technology, Laboratory of Information Processing,
Lappeenranta University of Technology
Diana.Kalenova@lut.fi

Abstract. In this paper, a problem of personal authentication through the use of signature recognition is described. The methods of verification include both on-line (or dynamic) and off-line (static) signature verification algorithms. The dynamic methods covered, are based on the analysis of the shape, speed, stroke, pen pressure and timing information. While the static methods involve general shape recognition techniques. The paper gives a brief historical overview of the existing methods and presents some of the recent research in the field.

Introduction

A problem of personal verification and identification is an actively growing area of research. The methods are numerous, and are based on different personal characteristics. Voice [1], lip movements [2], hand geometry [3, 4], face [5, 6, 7], odor [8, 9], gait [10, 11], iris [12], retina [13], fingerprint [14] are the most commonly used authentication methods. All of these psychological and behavioral characteristics are called biometrics. The biometrics is most commonly defined as measurable psychological or behavioral characteristic of the individual that can be used in personal identification and verification [15]. The driving force of the progress in this field is, above all, the growing role of the Internet and electronic transfers in modern society. Therefore, considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems.

The biometrics have a significant advantage over traditional authentication techniques (namely passwords, PIN numbers, smartcards etc.) due to the fact that biometric characteristics of the individual are not easily transferable, are unique of every person, and cannot be lost, stolen or broken.

The choice of one of the biometric solutions depends on several factors [13]:

- ✓ User acceptance
- ✓ Level of security required
- ✓ Accuracy
- ✓ Cost and implementation time

The method of signature verification, reviewed in this paper, benefits the advantage of being highly accepted by potential customers. The use of the signature has a long history, which goes back to the appearance of the writing itself. Utilization

of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus, the users are more likely to approve this kind of computerized authentication method [16].

Another advantage of the use of signature recognition as an authentication method is that most of the modern portable computers and personal digital assistants (PDAs) use handwritten inputs, thus there is no need in invention of principally new devices for biometric information collection [17].

At the same time there are very few signature recognition solutions that can provide sufficiently high recognition rates at a reasonable level of efficiency. However, this area of research is vastly growing and has a promising future [16].

Signature verification systems can generally be divided into two vast areas: static methods (or sometimes called off-line) that assume no time-relayed information, and dynamic (sometimes called on-line) with time-related information available in the form of p-dimensional function of time, where p represents the number of features of the signature [18].

Both of the methods of signature verification are considered in this paper, with more emphasis given on the on-line methodology.

The Nature of Human Signatures

It is reasonable to start this part with a general definition of what a signature is. According to American Heritage Dictionary [19] signature can be defined as: “the name of a person written with his or her own hand; the act of signing one's name” [19].

Second definition refers to the whole process of signing, and brings us to the assumption that the way the signature is made is a part of this signature [18]. Which further leads to a hypothesis that the characteristics of the process of signing (i.e. velocity, pen pressure, stroke etc.) are unique to every individual. [16] suggests that the signature consists of a series of rapid movements. It is supposed that the features of the process of signing originate from the intrinsic properties of human neuromuscular system, which produces the aforementioned rapid movements. Knowing that this system is constituted by a very large number of neurons and muscle fibers, is possible to declare, based on the central limit theorem, that a rapid and habitual movement velocity profile asymptotically tends toward a delta-lognormal equation [16]. This statement explains stability of the characteristics of the signatures. Thus, the signature can be treated as an output of a system observed in a certain time interval, necessary to make the signature. This system models the person making the signature [18].

On the other hand, looking at the first definition of the signature, it is possible to describe the signature as a static two-dimensional image, which does not contain any time-related information [18].

Both of the definitions of the signature lead to two different approaches of signature verification. First is based on static characteristics of the signature, which

are time invariant. In this sense signature verification becomes a typical pattern recognition task. Knowing that variations in signature patterns are inevitable the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variations [20].

Second approach is based on dynamic characteristics of the process of signing, and is called on-line. The task in this case would be to extract some characteristics from the recorded information of the signing process and further compare them with the characteristics of the reference signature [16]. The question that arises in this case is which kinds of characteristics should be recorded and extracted in order to identify the person in question in the most efficient and accurate way.

Types of forgery

The main task of any signature verification task is to detect whether the signature is genuine or forged. The instruments and the results of the verification depend upon the type of the forgery. Three main types of forgeries are shown in Fig. 1.

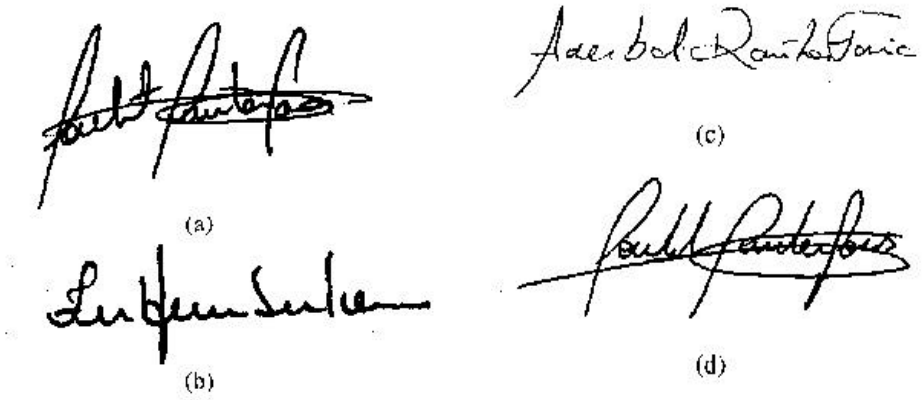

Fig 1. Types of forgery. (a) genuine signature; (b) random forgery; (c) simulated simple forgery; (d) simulated skilled forgery [21]

The first type of a forgery is a random forgery (see Fig. 1(b)), can normally be represented by a signature sample that belongs to a different writer (meaning that the forger has whatsoever no information about the signature style and the name of the person), the second type – simple forgery is a signature with the same shape of the genuine writer's name (see Fig. 1(c)). And the third type of the forgery is a skilled forgery (see Fig. 1(d)), which is a suitable imitation of the genuine signature [21].

Each of the verification approaches (off-line and on-line) deal with different types of forgeries. Off-line methods are normally used with the random and simple forgeries. The reason for that is the fact that this method generally deals with the shape factors of the signatures. However, the off-line verification lacks timing information and is not capable of modeling the handwriting motion, therefore it is harder to recognize the genuine signature using the off-line method [21].

By definition the skilled forgery has the shape practically similar to the genuine signature, and therefore static methods dealing only with the shape, regardless of the timing are not efficient in this case. While on-line methods have shown to be suited for these kinds of tasks [21].

Off-line Signature Verification

Off-line signature verification problem has attracted a great deal of attention in the past years; many results have been obtained [22-38]. However, these results are far from being perfect, and do not give the accuracy required for many security problems.

For many years the problem of signature verification has generally been solved by some authority or clerical employee, however with the invention of computers and scanning devices the trend has been towards automation of the whole process.

During a period of more than 20 years many approaches to the problem of automatic off-line signature verification have been created. The techniques used include: 2D transforms [22], histograms of directional data [23-25], curvature [26], horizontal and vertical projections of the writing trace of the signature [27], structural approaches [28], local measurements made on the writing trace of the signature [29], the position of feature points located on the skeleton of the signature [30]. One of the best results in this area has been reported in [31], where the error rate was less then one percent [32].

One of the pioneering works in this area has been conducted by Ammar [33] in 1980s. The idea has been to use the statistics of high gray-level pixels to identify pseudo-dynamical characteristics of signatures. Meaning that the level of gray-scale intensity is closely connected with pen pressure, which in turn is an individual characteristic of each signature [20, 33]. Several years later Qi and Hunt [30] have suggested algorithms for extracting global geometric and local grid features of signature images. The local measurement in this case is based on a non-uniform grid. The feature vector at each grid position includes the boundary code and the total number of pixels in this grid cell [20]. Then these features are combined in order to form a multi-scale verification function. Results indicate that the multi-scale verification function yields a lower verification error rate and higher reliability than the single-scale verification function using either global geometric or local grid feature representation [30].

Practically the same year Sabourin et al. [31] has published results of the research, where an extended shadow code has been used as a feature vector incorporating both local and global information in the verification decision process. Extended shadow code means in this case a method allowing extraction of general features of the signature at a low resolution and the rest of the features from characteristic areas of the signature at high resolution [20]. Several years later Sabourin [32] has suggested an algorithm that uses local granulometric size distributions. A signature image consisting of 512 * 128 pixels, centered on a grid of rectangular retinas and excited by local portions of the signature has been chosen. Granulometric size distributions have been used for the definition of local shape descriptors in an attempt to characterize the amount of signal activity exciting each retina on the focus of the attention grid. A

pattern spectrum derived through successive application of morphological operators, has been used as a local shape factor [32]. Guo et al. [34] have examined the stroke segments extracted from a set of training signatures. A signature is segmented on the basis of edge information [20]. This model is a stroke-level model, containing both spatial and relative temporal information (function of (x,y) coordinates, pseudo-time and pen-up/pen-down events). Thus a priori on-line tracing is necessary for the model in order to determine the ordering of the strokes information. The verification process includes matching of the signature in question with an a priori received model [34].

Another approach used for the purpose of signature verification is Hidden Markov Model (HMM) of intrapersonal and interpersonal variations of signature models. The model described in [21] uses a grid segmentation scheme in order to collect the features of the signature image. The features used in this research can be divided into static and pseudodynamic. First is the pixel density in each of the grid cells. Then extended shadow code [31]. And a signature skeleton image projected into the grid, in order to determine the predominate stroke slant in each cell (axial slant feature) [21]. Afterwards, a set of codebooks for each feature is generated and based on it a HMM signature model adapted to each writer is generated [21].

Mizukami [35] has proposed a method using an extracted displacement function [20]. The method consists in minimization of a function, defined as a weighted sum of a squared Euclidean distance between two signatures and a penalty term of the smoothness of the displacement function. In order to avoid stopping at local minima the signatures are transformed into coarse images by Gaussian filtering [35]. An example of a displacement function is shown in Fig. 2.

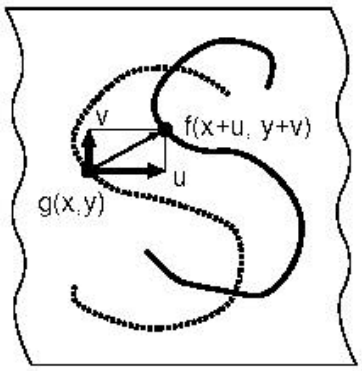

Figure 2. Displacement function of the authentic ***g*** and questionable ***f*** signatures [35]

Another wide category of off-line signature verification systems is the systems that are based on neural network approach [36, 37]. The whole range of this works is out of the scope of this work. Let us stop at two publications concerning this question [36, 37].

First [36] suggests the use of an autoassociator neural network based on the constructive cascade correlation architecture (CASCOR). The performance of the method is compared with multilayer perceptron network (MLP) with

backpropagation. The set of features for the experiment has been chosen through the use of the method of moments and Principal Component Analysis (PCA). The features extracted form the signature images are shown in Fig. 3.

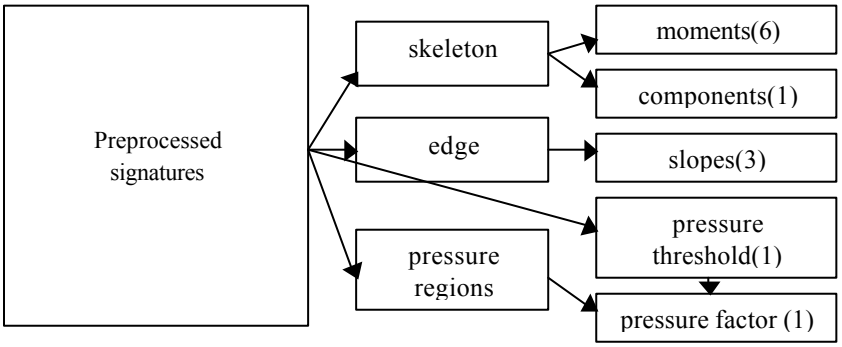

Figure 3. Feature extraction from the database [36]

First three processed images are produced out of the original signature image: skeleton, edge and pressure regions. Then a set of 12 features are extracted from these. Skeleton image produces six monents and the number of signature components, edge images give signature global slopes; and from the pressure regions the pressure threshold and pressure factor are extracted. Whilst using PCA 40 first eigenvalues and eigenvectors have been used as a set of features.

The results of the application of CASCOR and MLP to both the set of features obtained through the method of moments and through PCA, has shown that CASCOR performs significantly better in the task of signature verification tasks both in the case of simple, random and simple forgeries.

Another atempt of application of the Neural Networks is described in [37]. Where a multiple neural network structure is built. The netwok is based on three different sets of features, describing three different aspects of the signature: global features, grid information features, and texture features [37].

Global features are conisidered to be classical in the pattern recognition problems. In this case we are using the following (these are computed after normalization and skeletonization of the signature image) [37]:

- ✓ Signature height
- ✓ Image area
- ✓ Pure width (the width of the image with horizontal black space removed)
- ✓ Pure height
- ✓ Baseline shift, computed as the difference between the vertical centers of gravity of the left and the right part of the image.
- ✓ Vertical center of mass
- ✓ Horizontal center of mass
- ✓ Maximum vertical projection
- ✓ Maximum horizontal projection
- ✓ Vertical projection peaks. The number of local maximums of the vertical projection function.
- ✓ Horizontal projection peaks
- ✓ Global slant angle

- ✓ Local slant angle
- ✓ Number of edge points
- ✓ Number of cross points
- ✓ Number of closed loops

Grid features are calculated in the following way: the image is divided into 96 rectangular regions (12*8) and the area is calculated for each of these regions [37].

To obtain the texture features it is necessary to apply cooccurence matrices of the image. For binary images, these are 2*2 matrices describing the transition of black and white pixels for given directions and distances [37].

All of the features are realized in a multiple fixed-size neural newtork. A different classification structure has been applied to the feature categories described above and each class of the signatures (each signer) is classified by a separate network. The structure of the descision process is presented in Fig. 4. First neural network has 16 inputs (global features), second 96 inputs (grid features), and third 48 inputs (texture features). In conjuction with these networks a simple minimum Euclidean distance classifier has been used [37].

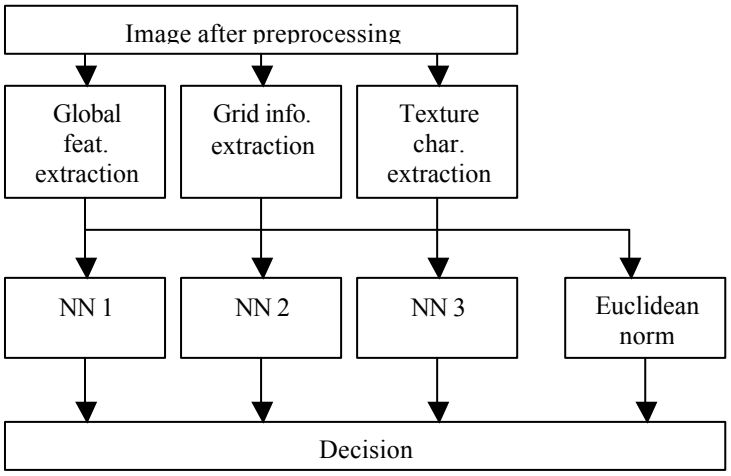

Figure 4. The structure of the classification system [37]

Each of the networks (NN1, NN2, NN3) consists of several one class one networks, specializing at each class of signatures [37].

Many other off-line signature verification solutions exist at the moment, however, none of them provide the efficiency required in most of the security imposed upon most of the biometric solutions. Nevertheless, the use of such metrics is still justified, by a wide acceptance of the solution itself.

An alternative to the off-line solution is provided by dynamic methods of signature verification, which exhibit higher lower error rates and much space for maneuver.

On-line signature verification

On-line signature verification is based on dynamic characteristics of the process of signing. Since time-dependent way of representing the signature contains more information, the accuracy of the recognition is significantly higher. The design and implementation of the on-line signature verification systems involves data acquisition, feature extraction, feature selection, decision-making, and performance evaluation [38]. But, at the same time, dynamic signature verification process requires special equipment to gather the information necessary for the verification process. Most common is a digitizing tablet, which registers not only the trajectory and speed of the process of signing, but also the pressure and pen tip position. These unique characteristics allow verification of the genuine signatures.

Dynamic signature verification methods can generally be divided into two broad groups: functional and parametric. In the first case the feature set, upon which the decision process is built, is constructed of functions, meaning that complete signals (e.g. pressure, velocity, acceleration etc.) are represented by time-dependent functions, whose values constitute the feature set. On the other hand, parameters of the measured signal can be considered as the feature sets [16].

The dynamic or also called on-line methods of human signature verification exhibit a variety of methods applied. Let us look at some of the techniques used in the area.

Probabilistic classifiers

Generally this class of methods performs decision-making based on weighted Euclidean distance between a genuine signature and a forgery. The distance is computed out of a functional feature set, which includes among others: speed, acceleration, curvature etc. However, such methods do not account for the discrimination power, correlation and signer dependence of the features. For such reasons some method of personalized feature selection are necessary. These methods are based on probability distribution of the genuine signature set features and general probability distribution of the whole set of signature features. Generally a distance between these two distributions is determined in order to determine the degree of importance of a certain feature. The larger the distance between the original signature and generalized signature features the more difficult it is to forge [38, 39, 40].

Time warping and dynamic matching

The dynamic time warping systems (DTW) has originated from the field of automatic speech recognition. One of the problems that arise when using the time-dependent features is time variability. By this we mean that non-linear timing differences exist in signature parameters produced by the same person (see Fig. 5). This might be caused by physical or emotional state of the signer [41, 42, 43].

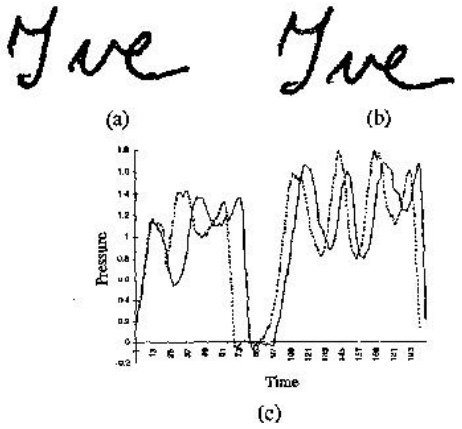

Figure 5. Non-linearities in pressure. (a) is presented by a solid line in (c); (b) by dashed [41]

One of the methods of dealing with the problem is DTW. The goal of the DTW algorithm is to find the most optimal time alignment between the reference signature and the signature in question [41].

In order for the DTW to be applied to the data the following conditions have to be satisfied [41]:

- ✓ the patterns to be compared should be time-sampled with a common and constant sampling period;
- ✓ there is no a priori knowledge about the relative importance of different parts of the patterns.

Having two signature patterns R (Reference) and T (Test), satisfying the conditions stated above. The warping path (time-alignment) p can be defined as:

$$p = c(0), c(1), c(2)..., c(K) \tag{1}$$

$$p_k = c(k) = (i(k), j(k)) \tag{2}$$

where i and j refer to i^{th}/j^{th} sample of R/T. Assume:

$$d(p_k) = d((i(k), j(k))) = \|R_i - T_i\| \tag{3}$$

$$D(p) = \frac{\sum_{k=1}^{K} w(k) d(p_k)}{\sum_{k=1}^{K} w(k)} \tag{4}$$

Then the algorithm attempts to find the path p, so that is minimizes the value of D(p), thus showing the best time-alignment between the T and R.

For the purpose of the classification of the signature as belonging or not to the set of genuine signature a Mahlanobis distance between the features is computed. As the features the form and motion functions are computed [42].

Neural Networks

At some point of time neural network approach has become a cure-all tool. No wonder that eventually this approach has been applied to the problem of automatic dynamic signature verification. Let us constrict the description of the work done in the area to two most interesting works [44, 45].

[44] constructed a three layer artificial neural network, trained using supervised learning with back propagation. Momentum (η) and learning rate (λ) equal to respectively 0.9 and 0.1. Training was stopped when the maximum error reached the value of 20%. Number of input neurons varied between 28-40, and the network contained one hidden layer of $\log_2 n$ neurons, where n is the number of input neurons. And the output contains one neuron, producing a result of either genuine or forged signature judgment.

The number of input neurons depends on the number of features selected for the training. Among the features are: number of pen lifts, percent of pen contact length between lifts, total pen contact length, average pen stroke angle, pen speed against time with pen lift information removed etc. The results indicate that taking a large enough set the FRR reduces to 7% and FAR to 6% [44].

A number of single output multilayer perceptrons (each for each word in the signature) are created for each user in [45]. Back-propagation with selective updates is chosen to be the learning rule. Decision threshold is set at the level of 0.5. Number of input nodes is equal to the number of features selected for the verification purpose [45].

In this case linear predictor cepstrum coefficients (LPC) are selected to be the features of the signatures. For a time series of samples $\{s(n)\}$, and Nth order linear predictor of sample s(n), denoted as s*(n) can be defined as a linear combination of N previous samples:

$$s^*(n) = \sum_{i=1}^{N} a_i s(n-i) \tag{5}$$

The spectrum of the LPC can be defined as follows:

$$S(e^{jw}) = \frac{s^2}{1 - \sum_{i=1}^{N} a_i e^{-jwi}} \tag{6}$$

The LPC cepstral coefficients $\{c_i\}$ can consequently be defined as:

$$\begin{aligned} c_1 &= a_1, \\ c_i &= a_i + \sum_{m=1}^{i-1} \frac{m}{i} a_m c_{i-m} \end{aligned} \tag{7}$$

where $1<i\leq N$.

x and y coordinates of the signature are first normalized, and then resampled into small frames. Then LPC cepstrum coefficients are obtained through Eq. 7, which in turn, are fed into the MLP [45].

The performance of the system shows that an equal error rate of as low as 4% has been obtained in the experiments.

Hidden Markov Models

Another popular technique is Hidden Markov Models (HMM). These have primarily found application in speech and handwriting recognition. The advantage of this technique for signature recognition task is that it is possible to accept variability and at the same time capture individual features of the signature [47].

The HMM is a doubly stochastic process governed by an underlying Markov chain with a finite number of states and a set of random functions each associated with one state. The model is hidden in the sense that all that can be observed is a sequence of observations [47].

The system in [47] tries to incorporate dynamic normalized directional angle function of the distance along the signature trajectory and model this information by HMMs. A separate HMM is constructed for each signature sample. A Baum-Welch algorithm has been used for training and classification. A probability of a forged signature acceptance by a HMM is computed, and the decision of the authentication of a particular signature is made based on the threshold value. The system produces a 1.75% FRR and 4.44% FAR [47].

Another experiment performed using the same technique [46] yields an equal error rate of approximately 1.2%. What is computed in this case is a log-likelihood of the HMM for a given signature sample. The decision is made on the basis of a predefined threshold [46].

Many other approaches exist: signal correlation [49], Euclidean and other distances [50], hierarchical approaches combining several different methods [48], Baum-Welch training etc. We have restricted the scope of this paper to most promising and explored methods of dynamic signature verification.

Conclusions

In this paper we have considered a problem of personal authentication through the use of signature recognition. Both on-line and off-line methods have been described. The method of signature verification, reviewed in this paper, benefits the advantage of being highly acceptable by potential customers as compared to the rest of biometric solutions. The driving force of the progress in this field is, above all, the growing role of the Internet and electronic transfers in modern society. Therefore, considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems.

Among off-line methods the following techniques have been used: 2D transforms [22], histograms of directional data [23-25], curvature [26], horizontal and vertical projections of the writing trace of the signature [27], structural approaches [28], local measurements made on the writing trace of the signature [29], the position of feature points located on the skeleton of the signature [30]. One of the best results in this area has been reported in [31], where the error rate was less then one percent [24].

The dynamic (on-line) methods include probabilistic classifiers [38, 39, 40], time warping or dynamic warping [41, 42, 43], neural networks [44, 45], HMM [46, 47], signal correlation [49], hierarchical approach [48], Euclidean and other distances [50]

etc. The best of the results are given by HMM [46] approach, with an equal error rate of as low as 1%.

According to the requirements set by Association for Payment Clearing Services (APACS) the FRR should be equal 0.001% and FAR 5%. However, none of the commercially available systems meet the requirements nowadays [12].

A list of companies involved in signature verification systems production is given in Appendix 1, along with a short description of the products available. Israeli company WonderNet in its solution "Penflow" provides one of the most secure commercially available solutions at the moment.

Although signature verification is not one of the safest biometric solutions, the use of it in business practices is still justified. Primarily due to the fact that the signature is a de facto mean of confirming the identity of the person, and therefore will provide a far less disruptive migration to an advanced technology than any other biometric can. Thus, signature verification has a very promising future.

References

1. J. P. Campbell, "Speaker Recognition: A Tutorial", Proc. IEEE, vol. 85, pp. 1437-`462, 1997.
2. A.W.C.; Leung, S.H.; Lau, W.H. Liew, Lip contour extraction using a deformable model, Image Processing, 2000. Proceedings. 2000 International Conference on , Volume: 2 , 10-13 Sept. 2000 Page(s): 255 -258 vol.2
3. Ashbourn, J., Practical implementation of biometrics based on hand geometry Image Processing for Biometric Measurement, IEE Colloquium on , 20 Apr 1994 Page(s): 5/1 - 5/6.
4. Sanchez-Reillo, R., Hand geometry pattern recognition through Gaussian mixture modelling, Pattern Recognition, 2000. Proceedings. 15th International Conference on , Volume: 2 , 3-7 Sept 2000 Page(s): 937 -940 vol.2.
5. R. Chellappa, C. Wilson, and S. Sirohey, "Human and Machine Recognition of Faces: a Survey", Proc. IEEE, vol. 83. No. 5, pp. 705-740, 1995.
6. P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The Feret Evaluation Methodology for Face-Recognition Algorithms", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 10, pp. 1090-1104, Oct. 2000.
7. S. A. Rizvi, P. J. Phillips, and H. Moon, "The Feret Verification Testing Protocol for Face Recognition Algorithms", Proc. Intl. Conf. Automatic Face- and Gesture-Recognition, pp. 48-53, 1997.
8. Nakamoto, T.; Ishida, H.; Moriizumi, T., Active odor sensing system, Industrial Electronics, 1997. ISIE '97., Proceedings of the IEEE International Symposium on , Volume: 1 , 7-11 July 1997 Page(s): SS128 -SS133 vol.1.
9. Moriizumi, T.; Nakamoto, T., Odor sensing system using neural network pattern recognition, Industrial Electronics, Control, Instrumentation, and Automation, 1992. 'Power Electronics and Motion Control'., Proceedings of the 1992 International Conference on , 9-13 Nov. 1992 Page(s): 1645 -1649 vol.3.
10. Huang, P.S.; Harris, C.J.; Nixon, M.S., Human gait recognition in canonical space using temporal templates, Vision, Image and Signal Processing, IEEE Proceedings- , Volume: 146 Issue: 2 , April 1999 Page(s): 93 -100
11. Nixon, M.S.; Carter, J.N.; Nash, J.M.; Huang, P.S.; Cunado, D.; Stevenage, S.V., Automatic gait recognition, Motion Analysis and Tracking (Ref. No. 1999/103), IEEE Colloquium on , 10 May 1999 Page(s): 3/1 -3/6.

12. J. G. Daugman, "High Confidence Visual Recognition of Persons by a Test of a Statistical Independence", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148-1161, Nov. 1993.
13. Biometrics: Personal Identification in Networked Society, A. Jain, R. Bolle, and S. Pankarti, eds., Kluwer Academic, 1999.
14. A. K. Jain, L. Hong, S. Pankanti, and E. Bolle, "An Idenity-Authentication System Using Fingerprints", Proc. IEEE, vol. 85, no. 9, pp. 1365-1388, 1997.
15. D. Sakamoto, M. Kondo, H. Morita, D. Muramatsu, M. Sasaki, T. Matsumoto, Dynamic Biometric Person Authentication Using Pen Signature Trajectories, Proc. 9th Intl. Conf. Neural Information Processing, vol. 4, 2002, pp. 2078-2082.
16. R. Plamondon, "The Handwritten Signature as a Biometric Identifier: Psycophysical Model and System Design", Proc. European Convention on Security and Detection, pp. 23-27, 1995.
17. M. E. Munich, P. Perona, "Visual Identification by Signature Tracking", IEEE Trans Pattern Analysis and Machine Intelligence, vol. 25, no. 2, Feb. 2003.
18. A. Pacut, A Czajka, "Recognition of Human Signatures", pp. 1560-1564, 2001.
19. Amercian Heritage Dictionary, Third Ed., ver. 3.6a, SoftKey Intl. Inc., 1994.
20. B. Fang, C. H. Leung, Y.Y. Tang, K. W. Tse, P. C. K. Kwok, Y. K. Wong, "Off-line Signature Verification by the Tracking of Feature and Stroke Positions", Pattern Recognition 36 (2003), pp. 91-101.
21. E. J. R. Justino, F. Bortolozzi, R. Sabourin, "Off-line signature verification using HMM for random simple and skilled forgeries", Proc. 6th Intl. Conf. On Document Analysis and Recognition, 2001, pp. 450-453.
22. W. F. Nemcek, W.C. Lin, "Experimental Investigation of Automatic Signature Verification", IEEE Trans. Systems, Man and Cybernetics, pp. 121-126, 1974.
23. J. P. Drouhard, R. Sabourin, M. Godbout, "Evaluation of a training method and of Various Rejection criteria for a neural network classifier used for off-line signature verification", IEEE Intl. Conf. Neural Networks, Orlando Fla., June 26-July 2, pp. 4294-4299, 1994.
24. J. P. Drouhard, R. Sabourin, M. Godbout, "A neural approach to off-line signature verification using directional PDF", Pattern Recognition, vol. 29, no. 3, pp. 415-424, Mar. 1996.
25. T. S. Wilkinson, J. W. Goodman, "Slope histogram detection of forged handwritten signatures", Proc SPIE, pp. 293-304, Boston, 1990.
26. E. R. Brocklehurst, "Computer methods of signature verification", J. Forensic Science Society, pp. 445-457, 1985.
27. M. Ammar, Y. Yoshida, T. Fukumura, "Off-line preprocessing and verification of signatures", Intl. J. Pattern Recognition and Artificial Intelligence, vol. 2, no. 4, pp. 589-602, 1988.
28. R. Sabourin, R. Plamondon, L. Beaumier, "Structural interpretation of handwritten signature images", Intl. J. Pattern Recognition and Artificial Intelligence, Special Issue on Automatic Signature Verification, pp. 709-748, 1994.
29. R. N. Nagel, A. Rosenfeld, "Computer detection of freehand forgeries", IEEE Trans. Computers, vol. 26, no. 9, pp. 895-905, 1977.
30. Y. Qi, B. R. Hunt, "Signature verification using global and grid features", Pattern Recogn. 27 (12) (1994), pp. 1621-1629.
31. R. Sabourin, G. Genest, "An extended-shadow-code-based approach for off-line signature verification: Part I. Evaluation of the bar mask definition", Proc. Of 12th ICPR, Jerusalem, Israel, 1994, pp. 450-453.
32. R. Sabourin, G. Genest, F. J. Preteux, "Off-Line Signature Verification by Local Granulometric Size Distributions", IEEE Trans. Pattern Anal. Mach. Intell. 19 (9) (1997), pp. 976-988.

33. M. Ammar, Y. Yoshida, T. Fulumura, "A new effective approach for off-line verification of signatures by using pressure features", Proc. 8th ICPR, Washington DC, USA, 1986, pp. 566-569.
34. J.K. Guo, D. Doermann, A. Rosenfeld, "Local correspondence for detecting random forgeries", Proc. 4th IAPR Conf. On Doc. Analysis and Recognition, Ulm, Germany, 1997, pp. 319-323.
35. Y. Mizukami, H. Miike, M. Yoshimura, I. Yoshimura, "An off-line signature verification system using an extracted displacement function", Proc. Of the ICDAR 99 5th Intl. Conf. Document Analysis and Recognition, 1999, pp. 757-760.
36. J. N. de Gouvea Ribeiro, G. C. Vasconcelos, "Off-line signature verification using an auto-associator cascade architecture", Proc. IJCNN'99 Intl. Joint Conf. Neural Networks, Vol. 4, 1999, pp. 2882-2886.
37. N. Papamarkos, H. Baltzakis, "Off-line signature verification using multiple neural network classification structures", Proc. of DSP 97, 13th Intl. Conf. On Digital Signal Processing, Vol. 2, 1997, pp. 727-730.
38. L. L. Lee, T. Berger, E. Aviczer, "Reliable on-line human signature verification systems", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 18, No. 6, June 1996.
39. S. H. Kim, M. S. Park, J. Kim, "Applying personalized weights to a feature set for on-line signature verification", Proc. 3rd Intl. Conf. Document Analysis and Recognition, pp. 882-885, Montreal, Aug 1995.
40. F. Bauer, B. Writz, "Parameter reduction and personalized parameter selection for automatic signature verification", Proc. 3rd Intl. Conf. Document Analysis and Recognition, pp. 183-186, Montreal, Aug 1995.
41. R. Martens, L. Claesen, "Dynamic programming optimisation for on-line signature verification", Proc. 4th Intl. Conf Document Analysis and recognition, pp. 653-656, Ulm, Germany, Aug. 1997.
42. R. Martens, L. Claesen, "On-line signature verification by dynamic time warping", Proc. 13th Intl. Conf. Pattern recognition, pp. 38-42, Vienna, 1996.
43. B. Wirtz, "Stroke-based time warping for signature verification", Proc. 3rd Intl. Conf. Document Analysis and Recognition, pp. 179-182, Montreal, Aug 1995.
44. D. J. Hamilton, J. Whelan, A. McLaren, I. Macintyre, and A. Tizzard, "Low cost dynamic signature verification system", IEEE Conf. Publications, n. 408, pp. 202-206, 1995.
45. Q.-Z. Wu, S.-Y. Lee, and L.-C. Jou, "On-Line Signature Verification Using LPC Cepstrum and Neural Networks", IEEE Trans. Systems, Man, and Cybernetics, vol. 27, n. 1, part B, pp. 148-153, 1997.
46. J.G.A. Dolfing, E.H.L. Aarts, J.J.G.M van Oosterhout, "On-line signature verification with Hidden Markov Models", Proc. 14th. Intl. Conf. Pattern Recognition, pp 1309-1312, Brisbane, Australia, Aug. 1998.
47. L. Yang, B. K. Widjaja, R. Prasad, "Application of hidden markov models for signature verification", Pattern Recognition, vol.28, no. 2, pp. 161-170, 1995.
48. X. H. Xiao, R.W. Dai, "A hierarchical on-line chinese signature verification system", Proc. 3rd Intl. Conf. Document Analysis and Recognition, pp. 202-205, Montreal, Aug 1995.
49. V. S. Nalwa, "Automatic on-line signature verification", Proc. IEEE, vol. 85, no.2, pp. 215-240, 1997.
50. T. Matsuura, S. Yamamoto, "On-line signature verification by IIR System", Proc. 5th Intl. Workshop Frontiers in Handwriting Recognition, pp. 537-545, Taejon, Korea, 1996.

Appendix 1. Providers of Signature Verification Solutions

1. Communication Intelligence Corporation
   - ✓ Sign-it – Windows server for Word, Adobe, AutoCad
   - ✓ Sign-On – Login security for Palm and Windows CE
   - ✓ InkTools – SDK for Palm OS and Windows
   - ✓ ISign – SDK for Internet applications

Official website: www.cic.com

2. Cyber-SIGN Japan Inc.
   - ✓ Cyber-SIGN – Acrobat, Lotus Notes and Word
   - ✓ Cyber-SIGN Enetrprise & Smart Card
   - ✓ Cyber-Sign Personal – client-server applications
   - ✓ Log-on-Lock – Pocket PC and Windows CE

Official website: www.cybersign.com

3. DATAVISION corporation
   - ✓ PCVision
   - ✓ RXVision

Official website: www.datavisionimage.com

4. Hesy
   - ✓ HESY

Official website: www.hesy.de

5. SOFTPRO
   - ✓ SignPlus Solution

Official website: www.softrpro.de

6. Security Biometrics, Inc.
   - ✓ "Signature Secure" powered by PenFlow (TM)

Official website: www.signio.com

7. WonderNet
   - ✓ Penflow

Official website: www.wondernet.co.il

8. Valyd, Inc.
   - ✓ eSign Desktop
   - ✓ eSign Eenterprise
   - ✓ eSign Logon
   - ✓ eSign SDK

Official website: www.valyd.com