Pattern Anal Applic (2014) 17:451–463
DOI 10.1007/s10044-012-0283-9

ORIGINAL ARTICLE

A new approach to signature recognition using the fuzzy method

Przemysław Kudłacik · Piotr Porwik

Received: 2 December 2011 / Accepted: 5 July 2012 / Published online: 15 August 2012

Abstract The paper presents a new fuzzy approach to *off-line* handwritten signature recognition. The solution is based on characteristic feature extraction. After finding signature's center of gravity a number of lines are drawn through it at different angles. Cross points of generated lines and signature sample, which are further grouped and sorted, are treated as the set of features. On the basis of such structures, obtained from a chosen number of learning samples, a fuzzy model is created, called the fuzzy signature. During a verification phase the level of conformity of an input sample and the fuzzy signature is calculated. The extension in feature extraction as well as proposed fuzzy model has never been employed before. It needs to be emphasized that information stored within the verification system cannot be used to recreate the original signatures collected at the enrolment phase. The fact is particularly valuable for large databases and systems where storage safety is crucial. The solution is very flexible and allows the user to extend an intuitive structure of fuzzy sets by employing dynamic features, making the approach an *on-line* method. The results obtained should be still improved, similarly to the case of other known biometric systems related to signature recognition. However, the presented technique can be easily utilized in applications where FAR coefficient should be very low and is more important than FRR ratio.

Keywords Signature recognition · Fuzzy sets · Fuzzy system

P. Kudłacik · P. Porwik (✉)
Institute of Computer Science,
University of Silesia, Katowice, Poland
e-mail: piotr.porwik@us.edu.pl

P. Kudłacik
e-mail: przemyslaw.kudlacik@us.edu.pl

1 Introduction

An analysis of handwritten documents is an important task for business, forensic casework, banking, etc. Obviously, handwriting should be considered individually, because each person has unique style of writing. For this reason professional recognition of a writer is treated as complex and difficult task. The result is credible when performed by highly qualified graphologists only. It should be noted that such investigations are expensive and rarely commissioned—in cases when documents are very important and their authenticity questioned. Moreover, graphological analysis of long documents is very time-consuming.

Some inconveniences can be overcome when only handwritten signature is analysed. Depending on type of an electronic handwriting capture, the source can be processed as a digital image or as a set of dynamic features—when signature is stored using a specialised device such as tablet. The second approach allows the potential system to analyse the source more precisely because in this case other unique properties are available.

The signature features are very often classified as global or local. Global features describe an entire signature and are determined, i.e. by means of both the discrete Wavelet and Hough transform, horizontal and vertical projections and so on. On the contrary, local features describe dynamic properties such as pen motion, slant, pressure, tremor and so on.

The signature recognition methods are also classified as *on-line* and *off-line*, where appropriate dynamic or static features are extracted and analysed. These techniques are well known within the research community [7, 13, 23–25, 34, 41].

There is a number of limitations in the data acquisition phase. The first is signature's length. In case of too long

signatures the data analysis may be difficult for the recognition system to identify the unique data points. In addition, pre-processing and recognition process are time consuming. On the other hand, in case of too short signatures the data set may not be representative enough and false accept rate (FAR) coefficient may be too high (i.e. an impostor can be authorised by the system).

The second limitation is the environment and conditions where a person performs the enrolment and verification phase. For example, two signatures taken from an individual may substantially differ from each other only because the position of a person was different.

After the data acquisition phase the recognition system extracts the unique features; hence signature recognition is classified as behaviour biometric. Given signature is described by means of unique features that identify the signer. Biometric systems should be able to detect whether the signature is genuine or forged. The results of the verification depend on the type of forgery. The first type is a random forgery and can be represented by a signature that belongs to any writer (forger has no information about the signature style and the name of a signer). The second type—simple forgery is a signature characterised by a similar shape as the genuine. The third type is so-called skilled forgery, which is a professional imitation of the genuine.

Off-line verification methods are used to detect the random and simple forgeries. It follows from the fact that in this approach only the shape of the signature is accessible, so only this kind of data can be considered. Unfortunately, the *off-line* method does not register timestamps; hence modelling of the signer's pen motion is impossible or very complex, which makes the recognition task even harder.

On-line method requires a stylus and an electronic tablet connected to a computer to capture dynamic signature information. In this method, nature of signatures can be described more precisely because additional parameters can be measured like velocity, pressure points, strokes, accelerations as well as static characteristics. This technique is preferable because dynamic features are very difficult to imitate. Unfortunately, these systems require user-cooperation and complex hardware.

In case of *off-line* recognition, signature template comes from an imaging device, and hence only static data are obtained. The person does not have to be present at the time of verification. For this reason, *off-line* signature recognition is simpler and convenient in various situations such as document verification, banking transactions, etc.

The paper proposes *off-line* fuzzy approach, which makes recognizing forged and genuine signatures possible. However, the method is flexible and allows the future user to include *on-line* features.

The most important advantage of the fuzzy approach is adjusting uncertainty to the input data. Each feature of the signature has a different soft constraint assigned in a fuzzy set form, relevant to a divergence occurring within learning samples. Therefore, to allow the system a proper adjustment, the signature of each individual must be captured at least several times.

The whole process of proposed recognition is described in the following sections of the paper. First, the pre-processing phase is presented. The process of building a fuzzy structure, called the fuzzy signature, is described next. Subsequent sections present the verification phase and obtained results with conclusion at the end.

2 Related works and critical remarks

Signature recognition methods are extensively studied and developed for many years [24, 34]. Unfortunately, reliable comparison of different approaches is quite difficult, which is caused by inconsistency in presented standards. In practice different databases are used, where different number of original and forged signatures are stored. The datasets of biometric features are frequently composed on the basis of private (hence unavailable) signatures as well as signatures coming from professional, published databases. It is a well-known fact that recognition performance decreases when number of samples in a database of biometric features is increased. It can be noticed even for small number of additional database records [27]. Such important remark is often ignored; therefore, we postulate that presented results should always be normalized and presentation principles should be respected. In presented approach all results were obtained for SVC2004 database, which is fully available [49]. Hence, results obtained and proposed algorithms can be always reliably compared with achievements of other authors.

On the other hand, it can be also observed that results reported in many papers use different coefficients (FAR, FRR, EER) and factors (accuracy, sensitivity, specificity). Unfortunately, only one of these parameters is very often treated as a single quality factor of described biometric systems. It is another obstacle precluding comparison of achieved results.

An influence of mentioned difficulties can be observed in the short review of obtained results in the work [7], where main recent research directions and results have been presented and discussed. Results gathered in that work are presented in Table 1 for *off-line* and Table 2 for *online* methods. The same problem can be noticed for results gathered in earlier extensive survey of the state-of-the-art [24].

Since the beginning of the theory presented by Zadeh [56] fuzzy sets have become a popular and intuitive tool for uncertainty representation. They are widely used in popular

Table 1 Performance comparison with off-line signature secognition systems [7]

Sr.	Approach	FAR	FRR	Accuracy
1	Proposed fuzzy approach	0.61/1.52	22.16/12.16	99.18/98.38
2	Signature recognition using clustering technique [7]	2.5/8.2	6.5/2.96	95.08
3	Contour Method [35]	11.60	13.20	86.90
4	exterior contours and shape features [8]	06.90	06.50	93.80
5	Local granulometric size distributions [47]	07.00	05.00	–
6	Back-propagation neural network prototype [1]	10.00	06.00	–
7	Geometric centers [39]	09.00	14.58	–
8	Two-stage neural network classifier [6]	03.00	09.81	80.81
9	Distance statistics [29]	34.91	28.30	93.33
10	Modified direction feature [4]	–	–	91.12
11	Hidden Markov model and cross-validation [15]	11.70	00.64	–
12	Discrete random transform and a HMM [9]	10.00	20.00	–
13	Kernel principal component selfregression [58]	03.40	08.90	–
14	Parameterized Hough transform [28]	–	–	95.24
15	Smoothness index-based approach [17]	–	–	79.00
16	Geometric based on fixed-point arithmetic [19]	4.9–15.5	5.61–16.39	–
17	HMM and graphometric features [16]	23.00	01.00	–
18	Virtual support vector machine [5]	13.00	16.00	–
19	Wavelet-based verification [12]	10.98	05.60	–
20	Genetic algorithm [55]	01.80	08.51	86.00

Table 2 Performance comparison with on-line signature recognition systems [7]

Sr.	Approach	FAR	FRR	ERR	Accuracy
1	ER2—dynamic time wrapping [36]	–	–	7.20	–
2	On-line SRS—digitizer tablet [26]	7.50–1.10	03.90	–	–
3	Image invariants and dynamic features [2]	–	–	–	83.00
4	On-line SRS model guided segmentation [46]	0.80	–	3.40	–
5	Conjugate gradient neural networks [3]	–	–	–	98.40
6	Consistency functions [42]	01.00	07.00	–	–
7	Variable length segmentation and HMM [48]	04.00	12.00	11.50	–
8	Implementing a DSP kernel [14]	<0.01	–	–	>99.0
9	Dynamic feature of pressure [51]	6.80	10.80	–	–
10	Low cost dynamic SRS [21]	7.00	6.00	–	–

types of intelligent systems handling variations of the input data [40, 43, 50]. Because of the nature of signature verification problems fuzzy approaches are also employed in this kind of research.

Enrolment phase of a general fuzzy approach to signature verification, as well as non-fuzzy methods, usually consists of three stages. The first step considers simple preprocessing of the input data, like normalisation and image filtering. In the second phase signature information is analysed and specific features are extracted. The last phase of fuzzy approaches considers building a fuzzy system (fuzzy model) based on variation of features extracted from learning samples. The verification phase of such systems confronts chosen signature sample (or extracted features) to the fuzzy model and calculates the level of conformity.

Recent research in the field of automatic signature verification employing fuzzy systems are based on different approaches. A significant number of contemporary solutions use different kind of neuro-fuzzy applications [18, 30, 38, 45, 52]. Data for the fuzzy systems come from extraction of various features like position and pressure

[30], angles [38], Zernike moments [18], result of discrete wavelet transform [52] and pseudo-outer product [45]. However, alternative solutions are also developed.

Papers [53, 54] introduce fuzzy snake models. The solution is based on open polygonal line (snake) composed by a variable number of equally spaced control points (piecewise-linear, two-dimensional structure). In this case database stores the exact information about signature's shape, which for some applications could be a disadvantage because of data security reasons.

System based on Bezier curves is presented in paper [57]. The approach allows the user to control the level of uncertainty by adjusting α-cuts, which results in variable ranges of possible position for Bezier nodes. As well as the previous method, this solution also stores the information about signature's shape.

Paper [22] proposes Takagi-Sugeno model with fuzzyfied angle features extracted from box approach.

The authors of [20] introduced a biometric crypto system with a fuzzy key, which is not the issue of this paper. However, the approach employs methods of authorisation with interesting feature extraction based on quantized maxima and minima from upper and lower envelopes of the signature.

The mentioned methods were tested mostly on private and unavailable databases with relatively small number of samples (less than 400). Data tested in paper [38] were obtained from four people and include only 20 forged samples. For that case the final average result is also not defined.

Comparison and assessment of methods introduced in papers [20, 53, 57] is impossible because no test results were presented.

Results obtained by authors of analysed examples are various and strongly depend on the type of database that was used. For example, the paper [18] reports the average error rate obtained at the level of 0.5 %. However, tests of that particular case are based on a database of 200 samples collected from 10 people without any forged samples. In addition, the reported error rate is not precisely defined.

Only the authors of [52, 54] used published databases, where the latter is no longer available at the specified website. The first paper reports EER at the level of 12.5 %. It needs to be emphasized that in this case FRR exceeded 25 % for FAR equal 5 % (based on presented ROC curve). The second paper reports FAR and FRR coefficients generally at the levels exceeding 10 % for a database containing more than 2000 samples.

Non-standard results are also reported in [22], where percentages of accepted and rejected samples are given. The best results were obtained for random forgery tests, where percentage of accepted samples equals 22.5 and 25 %, depending on the used type of method.

Private database employed in tests of online approach [30] (position and pressure) allowed the authors to obtain FAR and FRR coefficients equal 0 and 3.5 % respectively, which is a very good result that unfortunately cannot be verified. The same problem is encountered in another online approach employing a neuro-fuzzy method [45], where the best results were obtained for signatures of Chinese individuals.

The fuzzy approach described in this paper have never been proposed before. The first novelty can be found in the preprocessing phase. The method of feature extraction introduced in [44] was extended, which significantly reflects in results of the system. The second novelty is the original fuzzy model created on the basis of structure obtained in the first phase.

Information stored within database of the verification system cannot be used to recreate original shapes of signatures, which is an advantage from data security point of view. Moreover, the solution is characterised by relatively small computational complexity and in comparison with other methods it is much easier to implement.

Considering a relatively big database (1600 samples in SVC2004 database [49]), results obtained for FAR and FRR coefficients are very promising and encourage to further development of the solution.

3 Signature preparation

The main goal of writer recognition systems is determining whether two handwritten samples were performed by the same person or not. Signatures of the same individual can differ in many parameters such as size, pen pressure, velocity, etc. Therefore, one of the most important aspects of recognition is the unification process (pre-processing), which allows a system to compare signatures more precisely. The approach is based on the idea of characteristic signature preprocessing [44].

A signature can be treated as a set of discrete points (x_j, y_j) laying on the Carthesian X–Y plane, where $j = 1, 2, \ldots, N$, which describes piecewise-linear graphical form. The number N can vary for different signatures. The solution's first step is calculating a signature's center point $(\bar{x}, \bar{y})$ as so-called center of gravity, by the following Eq. [44]

$$\bar{x} = \frac{1}{N}\sum_{j=1}^{N} x_j, \quad \bar{y} = \frac{1}{N}\sum_{j=1}^{N} y_j. \tag{1}$$

In the next step a new set of points (x_k, y_k) is obtained, where $k = 1, 2, \ldots, M$ and $M \ll N$. The new points are calculated from an intersection of a signature and lines generated at different angles and passing through the center

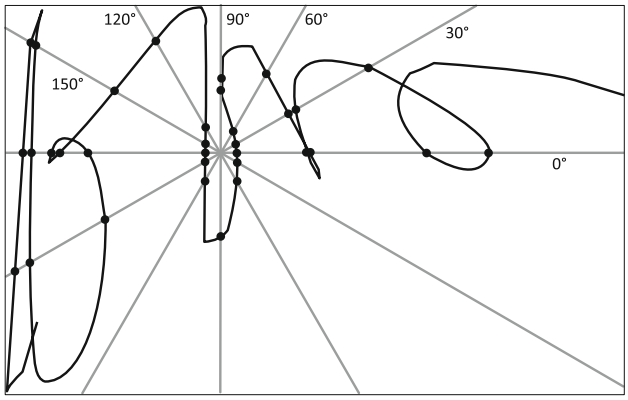

Fig. 1 Points of intersection of a sample signature and lines intersecting a signature's center point

point. The phase is shown at Fig. 1. The number of generated lines depends on an angle step $\Delta\alpha$, which is a parameter of the method. Fig. 1 contains visualization for $\Delta\alpha = 30^\circ$ and for that reason six lines are drawn at 0°, 30°, 60°, 90°, 120° and 150°.

For each point of intersection (x_k, y_k) the distance from the center point d_k is calculated [44]:

$$d_k = \sqrt{(x_k - \overline{x})^2 + (y_k - \overline{y})^2}, \tag{2}$$

and normalized [44]:

$$l_k = \frac{d_k}{d_{\max}}, \quad d_{\max} = \max\{d_1, d_2, \ldots, d_M\}. \tag{3}$$

The normalized l_k values create the Ω_{S_i} set, obtained from S_i signature. The Ω_{S_i} is naturally divided into $\Omega^{\alpha}_{S_i}$ subsets, including only those l_k values obtained for angle α, which can be designated as l_{α_k}. Additionally, the l_{α_k} values of $\Omega^{\alpha}_{S_i}$ subsets are arranged in decreasing order. For all the presented sets the following equations have to be obviously satisfied

$$\#\Omega_{S_i} = \sum_{\alpha} \#\Omega^{\alpha}_{S_i}. \tag{4}$$

It is important to notice that the preprocessing loses information of signature's shape and cannot be used to recreate the original. The Ω_{S_i} set after the described phase is stored as the characteristics of S_i signature.

3.1 Possible extension of the method

Described process is very flexible and easy to extend. In particular, more parameters can be considered such as pressure, velocity or pen's angle. Each parameter corresponds with one additional set of values within each $\Omega^{\alpha}_{S_i}$ set. Considering the mentioned parameters, each element of the Ω_{S_i} set can be described as the following:

$$(l_k, \mathrm{pr}_k, \mathrm{ve}_k, \mathrm{an}_k), \quad k = 1, 2, \ldots, M,$$

where pr_k, ve_k, an_k corresponds with pressure, pen's velocity and angle in (x_k, y_k). Therefore, the generalised element of Ω_{S_i} can be described as the following:

$$(w_{k_1}, w_{k_2}, \ldots, w_{k_G}), \quad k = 1, 2, \ldots, M,$$

where $w_{k_1}, w_{k_2}, \ldots, w_{k_G}$ represent parameters assigned to the (x_k, y_k) point of a given signature and G is a number of parameters.

4 Fuzzy signature

Preprocessing may generate a different number of elements in Ω_{S_i}, even for signatures captured from the same individual. Situation is depicted in Fig. 2 for Ω_{S_i} obtained from three sample signatures $S_i, i = 1, 2, 3$ with $\Delta\alpha = 30^\circ$. Because of page size limit only two groups of sets are shown for α equal 0° and 30°.

The main idea of the method is to construct a fuzzy structure—fuzzy signature *FS*—for each person chosen to be recognized by the system. The structure is formed by a number of fuzzy sets relevant to the input data. Constructed fuzzy sets reflect a diversity existing in the subsequent signatures within a learning set. Let the three samples presented in Fig. 2 represent a learning set. In general, the size of a learning set is not limited.

One can notice that the number of elements for $\Omega^0_{S_1}$, $\Omega^0_{S_2}$ and $\Omega^0_{S_3}$ varies from 2 to 4 and for $\Omega^{30}_{S_1}$, $\Omega^{30}_{S_2}$ and $\Omega^{30}_{S_3}$, from 2 to 3. The next step of preparation levels out the sub sets to the maximum size of $\Omega^{\alpha}_{S_i}$ within the same α. As depicted in Fig. 3, values 0, presented with bold font, are inserted at the end. The figure also contains the original size of $\Omega^{\alpha}_{S_i}$, which is needed for further analysis.

The first reason why 0 is used as a fill up value is simple. As it was mentioned at the end of Sect. 3, each $\Omega^{\alpha}_{S_i}$ is sorted in decreasing order, so the smallest values are located at the end. The value 0 is the shortest distance possible, obtained when the signature's center of gravity (1) is one of the signature's points. Therefore, the smallest value fills up shorter sets, preserving the order. To present the second reason, that mainly explains why to level out the sets, further steps of the method are needed to be introduced.

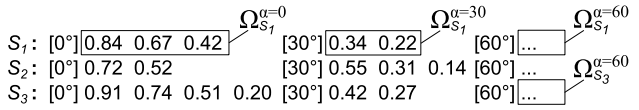

Fig. 2 Points after preprocessing phase for three sample signatures S_1, S_2 and S_3

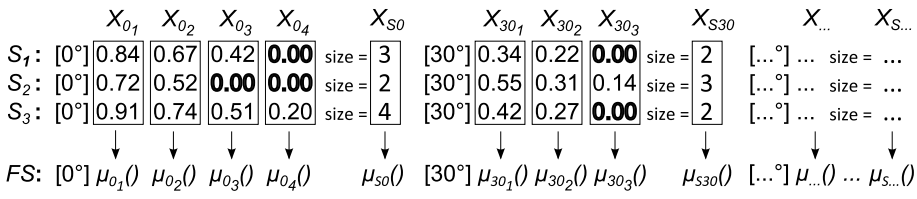

Fig. 3 Scheme of fuzzy signature creation

When sizes of $\Omega^{\alpha}_{S_i}$ are even for each α in all learning samples, they are again divided into groups in order to obtain a membership functions $\mu_{\alpha i}$ and $\mu_{S\alpha}$ describing fuzzy sets. The process is depicted in Fig. 3 by frames and arrows. It is important to notice that $\mu_{\alpha i}$ are created from the content of $\Omega^{\alpha}_{S_i}$ and $\mu_{S\alpha}$ from the size of $\Omega^{\alpha}_{S_i}$. Each frame on the figure represents values of a different universe of discourse X_{α_i} and $X_{S\alpha}$—the domains of $\mu_{\alpha i}$ and $\mu_{S\alpha}$, respectively.

Therefore, a fuzzy signature FS consists of fuzzy sets A_{α_i} and $A_{S\alpha}$ described as follows:

$$A_{\alpha_i} = \{(x, \mu_{\alpha_i}(x)) : x \in X_{\alpha_i}\}, \tag{5}$$

$$A_{S\alpha} = \{(x, \mu_{S\alpha}(x)) : x \in X_{S\alpha}\}. \tag{6}$$

Gaussian-type membership functions were chosen for A_{α_i} sets. However, other functions, like triangular or trapezoidal, can be applied. $A_{S\alpha}$ sets, described with piecewise-linear membership functions, are precisely analysed in subsequent section.

Functions μ_{α_i}, describing A_{α_i} sets, are defined as follows:

$$\mu_{\alpha_i}(x; m_{\alpha i}, \sigma_{\alpha i}) = e^{-\frac{(x-m_{\alpha i})^2}{2\sigma_{\alpha i}{}^2}}, \quad x \in X_{\alpha_i}, \tag{7}$$

where $m_{\alpha i}$ is an arithmetic mean of $\Omega^{\alpha}_{S_i}$ elements from X_{α_i} domain for all learning samples (values in one frame at Fig. 3). The parameter $\sigma_{\alpha i}$ represents the range between elements and is obtained on the basis of the following equation:

$$\sigma_{\alpha i} = \begin{cases} \gamma \dfrac{x_{\alpha i_{\max}} - x_{\alpha i_{\min}}}{2} & \text{for } \sigma_{\alpha i} > \sigma_{\min} \\ \sigma_{\min} & \text{for } \sigma_{\alpha i} \le \sigma_{\min} \end{cases} \tag{8}$$

where $x_{\alpha i_{\max}}$ and $x_{\alpha i_{\min}}$ are, respectively, maximum and minimum of $\Omega^{\alpha}_{S_i}$ elements from X_{α_i} domain for all learning samples. The fuzzyfication ratio γ is a global parameter of the system and allows the user to influence all fuzzy sets by increasing or decreasing their width (for $0 < \gamma < 1$ or $\gamma > 1$ respectively). Additionally, the $\sigma_{\alpha i}$ is limited from below by $\sigma_{\min}$, which is another global parameter of the fuzzy system. This parameter allows the user to set the minimum width, which is applied in case of too small diversity of elements in the $\Omega^{\alpha}_{S_i}$ set.

Trapezoidal and triangular membership functions can be defined, respectively, by the following equations:

$$\mu_{\alpha_i}(x; m_{\alpha i}, \sigma_{\alpha i}) = \begin{cases} 0 & \text{for } x < (m_{\alpha i} - \sigma_{\alpha i}) \\ \frac{2x-(m_{\alpha i}-\sigma_{\alpha i})}{\sigma_{\alpha i}} & \text{for } (m_{\alpha i} - \sigma_{\alpha i}) \le x < (m_{\alpha i} - \frac{\sigma_{\alpha i}}{2}) \\ 1 & \text{for } (m_{\alpha i} - \frac{\sigma_{\alpha i}}{2}) \le x < (m_{\alpha i} + \frac{\sigma_{\alpha i}}{2}) \\ \frac{-2x-(m_{\alpha i}+\sigma_{\alpha i})}{\sigma_{\alpha i}} & \text{for } (m_{\alpha i} + \frac{\sigma_{\alpha i}}{2}) \le x < (m_{\alpha i} + \sigma_{\alpha i}) \\ 0 & \text{for } (m_{\alpha i} + \sigma_{\alpha i}) \le x \end{cases}, \tag{9}$$

$$\mu_{\alpha_i}(x; m_{\alpha i}, \sigma_{\alpha i}) = \begin{cases} 0 & \text{for } x < (m_{\alpha i} - \sigma_{\alpha i}) \\ \frac{x-(m_{\alpha i}-\sigma_{\alpha i})}{\sigma_{\alpha i}} & \text{for } (m_{\alpha i} - \sigma_{\alpha i}) \le x < m_{\alpha i} \\ \frac{-x+(m_{\alpha i}+\sigma_{\alpha i})}{\sigma_{\alpha i}} & \text{for } m_{\alpha i} \le x < (m_{\alpha i} + \sigma_{\alpha i}) \\ 0 & \text{for } (m_{\alpha i} + \sigma_{\alpha i}) \le x \end{cases}, \tag{10}$$

where parameters $m_{\alpha i}$ and $\sigma_{\alpha i}$ have the same meaning as in (7).

Therefore, the fuzzy signature FS contains a number of fuzzy sets adjusted to learning samples. The placement of peaks and width of membership functions' shapes are based on the mean of relevant values and their range, respectively. One can notice that the step of sets levelling, by adding 0 values, lowers the influence of other values in calculation of the mean. It informs there was no value in that domain for this sample, which appropriately reflects in produced soft constraint—a fuzzy set.

4.1 Fuzzy size of $\Omega^{\alpha}_{S_i}$

The previous section distinguishes two different types of fuzzy sets. The first, as depicted in Fig. 3, is created from the values of $\Omega^{\alpha}_{S_i}$. The second type, designated as $A_{S\alpha}$ with $\mu_{S\alpha}$ membership function, represents the fuzzy size of $\Omega^{\alpha}_{S_i}$. The sets and creation of their membership functions are precisely analysed in this section.

In general the size of $\Omega^{\alpha}_{S_i}$ sets is a very important information for the recognition system. It is the crucial parameter for the presented method, because similar

signatures should produce similar sizes of the $\Omega^{\alpha}_{S_i}$ sets. Obviously, the $X_{S\alpha}$ domains of $\mu_{S\alpha}$ functions are discrete, containing sizes, which are natural numbers. The fact can be noted by the following expression:

$$\#\Omega^{\alpha}_{S_i} \in X_{S\alpha} \in \mathbb{N}. \tag{11}$$

Therefore, similarly to the first type of fuzzy sets, obtaining $\mu_{S\alpha}$ membership functions is based on appropriate processing of values from $X_{S\alpha}$ domains for all learning samples. In this case no predefined function is chosen. The solution simply assumes that multiple occurrence of the same size should be promoted by assigning a higher membership level. In addition, lower membership levels are appropriately assigned to the sizes that do not occur within the learning samples, but are sufficiently close (within β range), which forms a soft constraint. The general idea is depicted in Fig. 4, where two membership functions are presented for analysed example.

Considering Fig. 3 presented in previous section, it can be noticed that membership levels of μ_{S0} and μ_{S30} are relevant to the number of occurrence of $\Omega^{\alpha}_{S_i}$ size within learning samples. For $\Omega^{\alpha=0}_{S_i}$ three sizes occur once: 3, 2 and 4. That is why to each of those values the same membership level is assigned (circles with black fill). While for $\Omega^{\alpha=30}_{S_i}$ size 3 occurs once, but 2 occurs twice. Therefore, the size 2 is described with a higher membership level.

At this point, considering parameter $\beta = 0$, the membership function $\mu_{S\alpha}$ can be defined as follows:

$$\mu_{S\alpha}(x_i) = \begin{cases} \frac{O_{x_i}}{N_{\mathrm{L}}} & \text{for } \frac{O_{x_i}}{N_{\mathrm{L}}} > \frac{1}{2} \\ \frac{1}{2} & \text{for } 0 < \frac{O_{x_i}}{N_{\mathrm{L}}} \leq \frac{1}{2} \end{cases}, \quad x_i \in \mathbb{N}, \tag{12}$$

where x_i represents the analysed size, O_{x_i} represents the number of its occurrence and N_L represents the number of learning samples.

The presented solution promotes multiple occurrence of $\Omega^{\alpha}_{S_i}$ sizes; however, the minimum level is set to 0.5 (only in case of $\frac{O_{x_i}}{N_{\mathrm{L}}}$ greater than zero and less than 0.5). The minimum is set to avoid too small membership levels and to increase their influence in recognition algorithm, which is precisely described in the following sections.

Nevertheless, Fig. 4 depicts a number of extra points with nonzero membership level, inserted additionally to create a soft constraint (circles with white fill). The membership levels in this case are obtained from a linear function created according to the chosen β range—near $x_{S\alpha_{\min}}$ as a raising edge and $x_{S\alpha_{\max}}$ as a falling edge ($x_{S\alpha_{\min}}, x_{S\alpha_{\max}}$ represent minimum and maximum of $\#\Omega^{\alpha}_{S_i} \in X_{S\alpha}$ for all learning samples).

The β range for the analysed example is set to 2.5; hence two additional points are inserted at each edge. Considering the short analysis and the influence of the β parameter, the $\mu_{S\alpha}$ membership function can be fully defined by the following equation:

$$\mu_{S\alpha}(x_i) = \begin{cases} \frac{O_{x_i}}{N_{\mathrm{L}}} & \text{for } \frac{O_{x_i}}{N_{\mathrm{L}}} > \frac{1}{2} \\ \frac{1}{2} & \text{for } 0 < \frac{O_{x_i}}{N_{\mathrm{L}}} \leq \frac{1}{2} \\ f_{\mathrm{up}}(x_i) & \text{for } x_{S\alpha_{\min}} - \beta < x_i < x_{S\alpha_{\min}} \\ f_{\mathrm{down}}(x_i) & \text{for } x_{S\alpha_{\max}} < x_i < x_{S\alpha_{\max}} + \beta \end{cases}, \tag{13}$$

where x_i, O_{x_i}, N_{L} have the same meaning like in (12) and $f_{\mathrm{up}}, f_{\mathrm{down}}$ represent linear functions defined as follows:

$$f_{\mathrm{up}}(x_i) = \frac{\mu_{s\alpha}(x_{S\alpha_{\min}})}{\beta}(x_i - (x_{S\alpha_{\min}} - \beta)), \tag{14}$$

$$f_{\mathrm{down}}(x_i) = -\frac{\mu_{s\alpha}(x_{S\alpha_{\max}})}{\beta}(x_i - (x_{S\alpha_{\max}} + \beta)). \tag{15}$$

It is important to emphasize that the formula (13) produces fuzzy sets with valuable information about the input data. Properties of the membership function, like the maximum value or the range between $x_{S\alpha_{\min}}$ and $x_{S\alpha_{\max}}$, can be used to assess the quality of the input data only through an analysis of the $A_{S\alpha}$ fuzzy sets. This kind of information can be used by an adaptive method of learning, choosing only the informative $\Omega^{\alpha}_{S_i}$ sets in the process.

4.2 Extension of the method and the fuzzy signature

The Sect. 3.1 introduced an extension in preprocessing phase, where more parameters of a signature can be considered (i.e. pen's angle, velocity, pressure etc.). Creating the fuzzy signature FS in this case is not much more

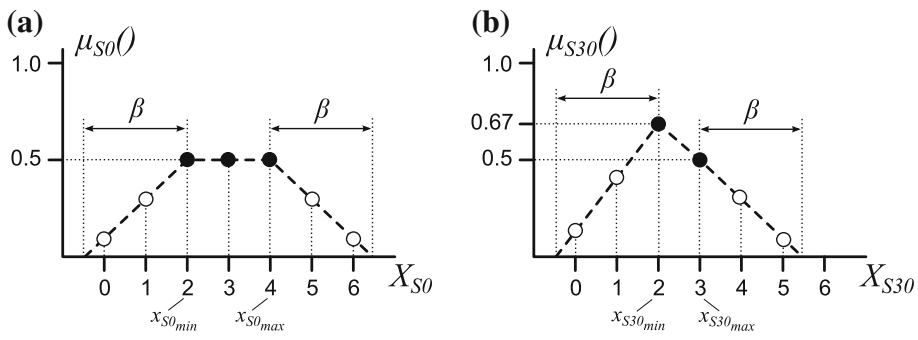

Fig. 4 Membership functions of fuzzy sizes for sample signatures: **a** $\mu_{S0}()$ for $\alpha = 0°$, **b** $\mu_{S30}()$ for $\alpha = 30°$

complicated. The only difference lies in the content of $\Omega^{\alpha}_{S_i}$ which elements are extended, containing more information for each point of a signature. Obviously, the $\#\Omega^{\alpha}_{S_i}$ does not change; therefore, fuzzy size $A_{S\alpha}$ can be obtained as described in the previous section. However, other stored parameters need to be processed, which will extend the fuzzy signature FS by additional fuzzy sets.

Membership functions of additional fuzzy sets can be obtained analogically to μ_{α_i} of A_{α_i}, which are precisely described in Sect. 4.

Let $A_{\alpha_{ki}}$ designates the generalised version of A_{α_i}, where $k = 1, 2, \ldots, G$ describes the G number of additional parameters. In that case the Gaussian membership function $\mu_{\alpha_{ki}}$ describing the fuzzy set, is defined as follows:

$$\mu_{\alpha_k i}(x; m_{\alpha ki}, \sigma_{\alpha ki}) = e^{-\frac{(x-m_{\alpha kj})^2}{2\sigma_{\alpha ki}{}^2}}, \quad x \in X_{\alpha_{ki}} \tag{16}$$

where $m_{\alpha ki}$, $\sigma_{\alpha ki}$ and $X_{\alpha_{ki}}$ domain represent parameter k and are analogical to $m_{\alpha i}$, $\sigma_{\alpha i}$ and X_{α_i} from (7), which has been described in Sect. 4.

The generalized versions of trapezoidal and triangular membership function $\mu_{\alpha_{ki}}$ can be obtained the same way.

5 Signature recognition

The fuzzy signature FS is created and stored in the system's database for each person that needs to be recognised. The process of recognition is based on obtaining the levels of conformity of a given signature with fuzzy structures from the database. If the level of conformity meets configured requirements, the signature can be considered as recognised. In general, the task can be accomplished by different means. However, the first phase of calculation is common for different approaches; that is why it will be described next.

Let S_{in} represent an input signature after preprocessing and FS is a fuzzy signature chosen from the database. If the preprocessing parameter $\Delta\alpha$ was the same for learning samples creating the FS and given S_{in}, the structures can be directly compared, because of the same number of $\Omega^{\alpha}_{S_i}$ sets. If this condition is not satisfied, the structures cannot be compared and are treated as different (the level of conformity equals 0). The scheme of the phase is depicted in Fig. 5 where subsets for the two sample α parameter: 0° and 30°, are presented.

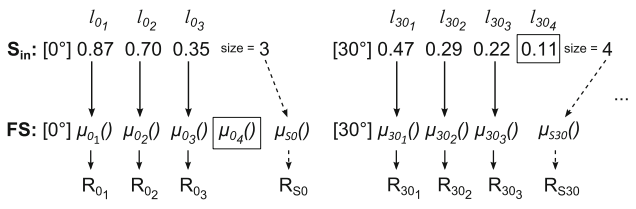

Fig. 5 Scheme of a signature verification

The values of $\Omega^{\alpha}_{S_{\text{in}}}$ and their sizes are taken as an input of the relevant membership functions of the FS. It is important to emphasize that in case of different number of l_{α_i} and μ_{α_i}, which is a normal situation, elements that cannot be paired are simply omitted in the process. The problem occurs for the example on Fig. 5 for l_{30_4} and μ_{0_4} depicted in frames. Therefore, the results $R_{\alpha_i} \in [0, 1]$ and $R_{S\alpha} \in [0, 1]$ are obtained, respectively, by the following equations:

$$R_{\alpha_i} = \mu_{\alpha_i}(l_{\alpha_i}), \quad i = 1, 2, \ldots, n_\alpha \tag{17}$$

$$R_{S\alpha} = \mu_{S\alpha}(\#\Omega^{\alpha}_{S_{\text{in}}}), \tag{18}$$

where $l_{\alpha_i} \in \Omega^{\alpha}_{S_{\text{in}}}$ and assuming μ_{α_k} for $k = 1, 2, \ldots, K_\alpha$, the value $n_\alpha = \min(K_\alpha, \#\Omega^{\alpha}_{S_{\text{in}}})$.

Calculated results are basis for further processing within different verification methods that produce one final result $R \in [0, 1]$, representing the output level of conformity. In general, this kind of tasks are performed by operators of aggregation.

Let $\oplus$ represent operator of aggregation as a mapping $\oplus : [0, 1]^I \to [0, 1]$ of I values $x_1, x_2, \ldots, x_I \in [0, 1]$ to one $x \in [0, 1]$, that is [10]:

$$x = \bigoplus_{i=1}^{I} x_i = \oplus(x_1, x_2, \ldots, x_I). \tag{19}$$

Therefore, the general method of signature verification can be described by the following equation:

$$R = \bigoplus_{\alpha=0}^{\alpha_{\max}} \left\{ R_{S\alpha} \bigstar_T \bigoplus_{i=0}^{n_\alpha} R_{\alpha_i} \right\}, \tag{20}$$

where $\alpha_{\max}$ represents the maximum α for S_{in} and FS, n_α is a number of R_{α_i} results for particular α and $\bigstar_T$ represents any T-norm [10, 11, 37].

The main idea of the approach is that the influence of the local results—aggregated R_{α_i}—is controlled by the $R_{S\alpha}$, because the fuzzy size $A_{S\alpha}$ is the most important element in the structure of FS. It can be described as higher in the hierarchy. For a better result, the sizes of $\Omega^{\alpha}_{S_{\text{in}}}$ have to be matched first to increase the influence of the lower structure. Various methods of verification can be obtained from (20) by applying different $\oplus$ operators.

The most restrictive solution is obtained when aggregation operator is a T-norm. In that case the Eq. (20) takes the following form:

$$R = \bigstar_{\text{T}}^{\alpha=0}{}^{\alpha_{\max}} \left\{ R_{S\alpha} \bigstar_T \bigstar_{\text{T}}^{i=0}{}^{n_\alpha} R_{\alpha_i} \right\}, \tag{21}$$

where $\bigstar_{\text{T}}$, as $\bigstar_T$, represents any T-norm. Therefore, the lowest partial result has the most influence on the output result like for the classic approach of Mamdani and Assilan [40]. The method is named "hard", because it absolutely

disqualifies signatures with partial match. On the other hand, the least restrictive solution is obtained for a mean as the aggregation operator. In this case the Eq. (20) takes the following form:

$$R = \biguplus_{\alpha=0}^{\alpha_{\max}} \left\{ R_{S\alpha} \bigstar_T \biguplus_{i=0}^{n_\alpha} R_{\alpha_i} \right\}, \tag{22}$$

where $\uplus$ represents any mean operator. Contrary to previous one, this method is named "soft", because it allows the system to obtain results greater than zero in case of partial matches.

Additional methods are created as a hybrid solution of the presented above. First, called "hard-soft", assumes a T-norm as the first aggregation operator and a mean as the second. Hence, the Eq. (20) takes the following form:

$$R = \bigstar_{\mathrm{T}\,\alpha=0}^{\alpha_{\max}} \left\{ R_{S\alpha} \bigstar_T \biguplus_{i=0}^{n_\alpha} R_{\alpha_i} \right\}. \tag{23}$$

The equation for the method called "soft-hard" is obtained analogically and defined as follows:

$$R = \biguplus_{\alpha=0}^{\alpha_{\max}} \left\{ R_{S\alpha} \bigstar_T \bigstar_{\mathrm{T}\,i=0}^{n_\alpha} R_{\alpha_i} \right\}. \tag{24}$$

5.1 Assessment of an input signature

After obtaining the final result R, which is the level of conformity, an assessment needs to be performed in order to classify the input signature S_{in} as genuine/matched or forged/not matched. In general, two solutions are possible. The most simple way is to assume one fixed level $R_{\min_{\mathrm{in}}}$ for the whole recognition system. Unfortunately, as it is easy to apply, it makes the system insensitive to diversity between different cases.

The second approach considers each fuzzy signature separately. In this case every fuzzy signature stored in the database has a decision level $R_{\min_i}$ assigned, where $i = 1, 2, \ldots, P$ and P is the number of stored fuzzy signatures FS. The $R_{\min_i}$ value works as a trigger. When $R \geq R_{\min_i}$ for the S_{in} sample, it is classified as genuine/matched for signature number i or forged/not matched if $R < R_{\min_i}$.

In the presented approach the second form of assessment is applied. The trigger level $R_{\min_i}$ is calculated immediately after obtaining the fuzzy signature FS and again involves the learning samples in the process. The idea is to calculate the level of conformity of the FS with the learning samples and to adjust the $R_{\min_i}$ to the worst result. It can be described by the following equation:

$$R_{\min_i} = \min(R_1, R_2, \ldots, R_L)(1 - \Delta r), \tag{25}$$

where $R_1, R_2, \ldots, R_L$ represent the levels of conformity obtained for L learning samples. An additional parameter $\Delta r \in [0, 1]$ is used to allow the system user to define an extra range where signatures are also classified as genuine/matched.

6 Results obtained

The described method was implemented in Java programming language using the FUZZLIB library [31–33] as the set of tools for fuzzy systems development. The designed application allows the system user to configure many different properties and parameters, which are presented in Table 3.

Tests were performed for different configuration of parameters to find the suite of values and properties giving the best results of FAR and FRR error levels. As the source of signatures the SVC2004 database was used [49]. It contains 1,600 signatures of 40 people, where 40 signatures are assigned to each person (20 genuine and 20 professionally forged). Unfortunately, performing tests covering all possible combinations, even for several values of each

Table 3 Configurable properties and parameters of the fuzzy system

Property/parameter	Description
Verification method	A type of verification method used to obtain the output level of conformity ("hard", "soft", "hard-soft" and "soft-hard")
T-norm	A type of triangular norm used in computation (considered types implemented in FUZZLIB library: minimum, product, nilpotent, Hamacher product and Łukasiewicz t-norm)
$\Delta\alpha$	The angle step of the preprocessing phase—Fig. 1
γ	The fuzzyfication ratio (8)—influences the width of μ_{α_i} membership functions
$\sigma_{\min}$	The minimum width of the μ_{α_i} membership functions—Eqs. (8), (7)
β	The range defining the width of edges for the $\mu_{S\alpha}$ membership functions—Fig. 4 and Eq. (13)
Δr	The range of classification (25)
L	the number of learning samples

parameter, is extremely time-consuming because of an exponential complexity of the problem. That is why in assessment of the most important parameters of the system test were executed starting with arbitrarily chosen values which were modified during the process. In many cases this kind of method reveals a general influence of one changing parameter on the obtained results.

Before the tests the problem of the learning samples number (parameter L) had to be analysed. In general, if more signature samples of an individual are involved in the learning process, then the recognition level for signatures of that person is higher. On the other hand, in case of the analysed approach, too much samples can generate large widths of created fuzzy sets making the system too "fuzzy", having a negative impact on the FRR error. It is caused by the differences between signatures of one person. Secondly, adjusting the system with too big number of learning signatures is uncomfortable for the user and the person responsible for the process. Even if it is done only once, in case of many potential users it could be considered as a disadvantage of the verification system. That is why the size of a learning set have to be chosen reasonably by finding a compromise.

During tests of the presented system it was assumed that the number of learning signatures should not exceed 5 samples. The decision was based mainly on the small number of genuine signatures for each individual in SVC2004 database (20 signatures). In that case, for at least 15 remaining samples, the obtained FRR coefficient can be considered as representative. That is why the tests were performed for two values: the highest $L = 5$, which were expected to give better results and smaller $L = 3$ to analyse the influence of a decreased number of learning samples. The results presented at Fig. 6 confirm the expectations.

The verification method and the type of T-norm were analysed next. The best results were obtained for the "soft-hard" approach and the minimum T-norm. The "hard" and "hard-soft" solutions were rejected at the beginning. The methods practically adjust the system only to the learning samples and reject most of the other genuine samples, which results in a very big FRR and disqualifies the approaches. The "soft" and hybrid "soft-hard" methods gave the best results, making the system much more responsive to adjustment of the parameters. However, only with the "soft-hard" method the system was able to obtain a very low FAR for FRR below 25 %. In case of T-norm analysis, the Lukasiewicz and the nilpotent T-norms occurred to be too restrictive. These functions assign zero to lower values of their parameters, which is undesirable particularly for the "hard" verification method and partial matching in general. For the product and the Hamacher product the system produces very low values of conformity levels, which causes a difficulty in adjustment of Δr. The problem can be partially solved by increasing γ—the fuzzyfication ratio, which obviously reflects on the FAR error. This fact causes that the system is less responsive to changes of the parameters in comparison to the minimum T-norm.

One of the most important parameters is the $\Delta\alpha$. Therefore, the second group of tests were performed with fixed configuration of other parameters (γ, $\sigma_{\min}$, β, Δr) to analyse the influence of different $\Delta\alpha$ values. Results obtained for $\Delta\alpha = 1, 2, 3, 5, 10, 15, 20, 30, 35, 40$ and 45 are shown in a chart form at Fig. 6.

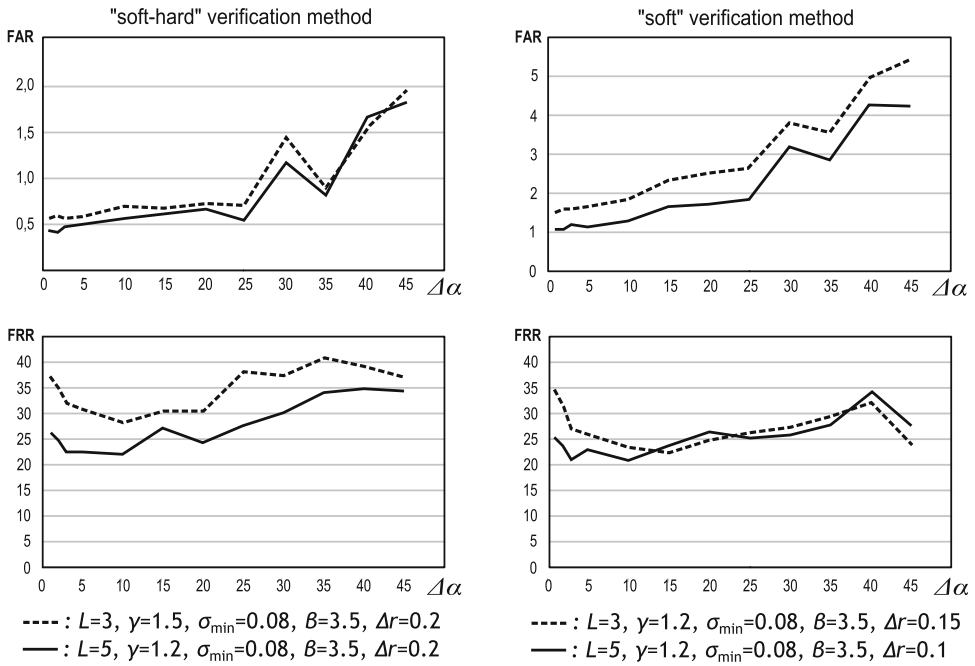

Fig. 6 FAR and FRR errors depending on the $\Delta\alpha$ parameter. Charts obtained for the "soft-hard" and "soft" methods

Table 4 Test results

$\Delta\alpha$	γ	$\sigma_{\min}$	β	Δr	L	FAR	FRR	Accuracy
10	1.09	0.09	3.5	0.2	5	0.61	22.16	0.9919
25	1.19	0.08	3.5	0.2	5	0.61	27.83	0.9914
10	1.35	0.09	3.5	0.2	5	1.52	12.16	0.9838
25	1.35	0.09	3.5	0.2	5	1.52	17.16	0.9833

Taking into account both FAR and FRR coefficients it can be noticed that the highest recognition levels (especially FAR) were obtained for $\Delta\alpha \leq 25^\circ$. Larger values of the parameter cause a noticeable growth of the FAR coefficient in particular. Results of FAR for the "soft-hard" approach in the described range are very similar. However, in case of $\Delta\alpha = 25^\circ$ there is much smaller number of analysed angles, which gives a much shorter time of computation (i.e. around 25 times less data to analyse in comparison to $\Delta\alpha = 1^\circ$). That is why two values from the range were chosen for a detailed analysis: $\Delta\alpha = 10^\circ$ because of the lowest FRR levels and $\Delta\alpha = 25^\circ$ because of the computation time. For the two chosen angles, the "soft-hard" verification method and the minimum T-norm, the remaining parameters of the system were adjusted: fuzzyfication ratio γ, minimum width $\sigma_{\min}$, the range β and the range Δr. The number of learning samples L was set to 5, because it gave better results in the previous test. Table 4 contains two groups of the best results obtained for FAR near 0.6 and 1.5 %.

6.1 Computational complexity

The process of creation of the fuzzy signature FS is characterized by a linear time complexity ($O(n)$), according to the $\Delta\alpha$ parameter. During tests the 2core 2.2 GHz Intel processor machine was used. The average time of computation of one fuzzy signature was equal 1.7 ms for $\Delta\alpha = 10^\circ$, and 0.77 ms for $\Delta\alpha = 25^\circ$. Each FS was created from five learning samples. An average time of verification for one signature (S_{in}) was equal 0.59 and 0.27 ms, respectively.

It is important to emphasize that all numerical tests were implemented in the Java language and executed within the Java Virtual Environment. Considering the fact of possible implementation at non-virtual platform it gives hope for much shorter times of computation.

7 Conclusions

As it was mentioned in the introduction, one goal of the paper was to define an automated process of signature analysis for biometric classifiers, where machine learning methods can be used. The present paper formulates the appropriate structure of such method and describes all the phases needed to build a fuzzy system dedicated for signature verification. The proposed method can be applied in the environment, where input signatures, even of the same person, are characterised by a large differences and for this reason cannot be accurately recognized using other methods. The high FRR ratio causes that the technique is destined for important security systems, where FAR errors should be very low. It must be emphasised that a very good result of FAR obtained for the presented solution stands against the common opinion that the *off-line* methods are easy to forge.

Another advantage of the approach, certainly very important for security systems, is the characteristic preprocessing phase, which greatly increases the safety level of information stored in the database. In case of a data theft the intruder has an access to a processed form of signatures, which cannot be used to recreate the original. In addition, small time complexity of the algorithm gives hope for a further development of the method, which can be applied in various domains.

References

1. Abbas R (2003) Back propagation neural network prototype for off line signature verification. Thesis submitted to RMIT, Melbourne
2. Al-Shoshan AI (2006) Handwritten signature verification using image invariants and dynamic features. In: Proceedings International Conference on computer graphics, Imaging and visualization (CGIV'06), pp 173–176
3. Ammar M, Yoshida Y, Fukumura T (1986) A new effective approach for off-line verification of signatures by using pressure features. In: Proceedings international conference on pattern recognition, pp 566–569
4. Armand S, Blumenstein M, Muthukkumarasamy V (2004) Off-line signature verification based on the modified direction feature. In: Proceedings 18th International Conference on pattern recognition (ICPR '06), vol. 04, pp 509–512
5. Audet S, Bansal P, Baskaran S (2006) Off-line signature verification using virtual support vector machines. In: ECSE 526—Artificial Intelligence, pp 1–8
6. Baltzakis H, Papamarkos N (2001) A new signature verification technique based on a two-stage neural network classifier. Eng Appl Artif Intell 14:95–103

7. Bharadi VA, Kekre HB (2010) Off-line signature recognition systems. Int J Comput Appl 1(27):48–56
8. Chen S, Shrihari S (2005) Use of exterior contours and shape features in off-line signature verification. In: Proceedings of eight International Conference on document analysis and recognition (ICDAR'05), pp 1280–1284
9. Coetzer J, Herbst BM, du Preez JA (2004) Offline signature verification using the discrete radom transform and a Hidden Markov model. EURASIP J Appl Signal Process 4:559–571
10. Czogala E, Leski J (2000) Fuzzy and neuro-fuzzy intelligent systems. Springer, Berlin
11. Czogala E, Leski J (2001) On equivalence of approximate reasoning results using different interpretations of if–then rules. Fuzzy Sets Syst 117:279–296
12. Deng P, Yuan H, Liao M, Tyan H (1996) Wavelet based off-line signature recognition system. In: Proceedings of 5th Conference on optical character recognition and document Analysis
13. Doroz R, Porwik P, Para T, Wrobel K (2008) Dynamic signature recognition based on velocity changes of some features. Int J Biometrics 1(1):47–62
14. Dullink H, van Daalen B, Nijhuis J, Spaanenburg L, Zuidhof H (1995) Implementing a DSP kernel for online dynamic handwritten signature verification using the TMS320 DSP Family, EFRIE SPRA304
15. Edson J, Justino R, Bortolozzi F, Sabourin R (2002) The interpersonal and intrapersonal variability influences on off-line signature verification using HMM. In: Proceedings of XV Brazilian Symposium computer graphics and image processing, pp 197–202
16. Edson J, Justino R, Yacoubi AE, Bortolozzi F, Sabourin R (2000) An off-line signature verification system using HMM and graphometric features. DAS 2000:211–222
17. Fang B, Wang Y Y (1999) A Smoothness Index Based Approach for Off-line Signature Verification, Proceedings of fifth International conference on document analysis and recognition (ICDAR '99), pp 785–787
18. Fasihfar Z, Haddadnia J, (2010) Designing a fuzzy RBF neural network with optimal number of neuron in hidden layer and effect of signature shape for persian signature recognition by Zernike moments and PCA. In: International Conference on web information systems and mining, pp. 188–192
19. Ferrer MA, Alonso JB, Travieso CM (2005) Offline geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Trans Pattern Anal Mach Intell 27(6):993–997
20. Freire M, Fierrez J, Martinez-Diaz M, Ortega-Garcia J (2007) On the applicability of off-line signatures to the fuzzy vault construction. In: International Conference document analysis and recognition, pp 1173–1177
21. Hamilton D, Whelan J, McLaren A (1995) Low cost dynamic signature verification system. In: Proceeding of IEEE CNF European convention on security and detection, pp 202–206
22. Hanmandlu M, Hafizuddin MY, Madasu VK (2005) Off-line signature verification and forgery detection using fuzzy modeling. Pattern Recogn 38:341–356
23. Huang K, Yan H (1997) Off-line signature verification based on geometric feature extraction and neural network classification. Pattern Recogn 30(1):9–17
24. Impedovo D, Pirlo G (2008) Automatic signature verification: the state of the art. IEEE Trans Syst Man Cybern C Appl Rev 38(5):609–635
25. Jain AK, Flynn P, Ross AA (2007) Handbook of biometrics. Springer, New York
26. Jain AK, Ross A, Prabhakar S (2002) On Line Signature Verification. Pattern Recogn 35(12):2963–2972
27. Johnson AY, Sun J, Bobick A F (2003) Using similarity scores from a small gallery to estimate recognition performance for larger galleries. In: IEEE International Workshop on analysis and modeling of faces and gestures (AMFG2003), pp 100–103
28. Kaewkongka T, Chamnongthai K, Thipakom B (1999) Off-line signature recognition using parameterized Hough transform. In: Proceedings of fifth International Symposium on signal processing and its applications (ISSPA '99), vol. 1, pp 451–454
29. Kalera MK, Shrihari S (2004) Offline signature verification and identification using distance statistics. Int J Pattern Recogn Artif Intell 18(7):1339–1360
30. Khalid M, Mokayed H, Yusof R, Ono O (2009) Online signature verification with neural networks classifier and fuzzy inference. In: Proc Third Asia International Conference on modelling, simulation, pp 236–241
31. Kudlacik P (2008) Operations on fuzzy sets with piecewise-linear membership function (Polish). Studia Informatica 29 3A(78):91–111
32. Kudlacik P (2010) Structure of a knowledge base in the FUZZ-LIB library (Polish). Studia Informatica 31 2A(89):469–478
33. Kudlacik P (2010) Advantages of an approximate reasoning based on a fuzzy truth value. J Med Inf Technol 15:57–61
34. Leclerc F, Plamondon R (1994) Automatic signature verification: the state of the art. Int J Pattern Recogn Artif Intell 8(3):643–660
35. Lee S, Pan JC (1992) Off-line tracing and representation of signatures IEEE Trans Syst Man Cybern 22(4):755–771
36. Lei H, Palla S, Govindraju V (2004) ER2: an intuitive similarity measure for on-line signature verification. In: Ninth International Workshop on frontiers in handwriting recognition (IWFHR-9 2004), pp 191–195
37. Łukasiewicz J (1920) O logice trojwartosciowej (in Polish). Ruch filozoficzny5:170–171 (English translation: On three-valued logic. In: Borkowski L (ed.) Selected works by Jan lukasiewicz. North-Holland, Amsterdam, pp 87–88 (1970))
38. Madasu VK, Hanmandlu M, Madasu S (2003) Neuro-fuzzy approaches to signature verification. In: 2nd National Conference on document analysis and recognition (NCDAR-2003)
39. Majhi B, Reddy Y, Babu D (2006) Novel features for off-line signature verification. Int J Comput Commun control 1(1):17–24
40. Mamdani EH, Assilan S (1975) An experiment in linguistic synthesis with a fuzzy logic controller. Int J Man Mach Stud 20:1–13
41. Muramatsu D, Matsumoto T (2007) Effectiveness of pen pressure, azimuth, and altitude features for online signature verification. Lect Notes Comput Sci Adv Biometrics 4642:503–512
42. Nalwa V (1997) Automatic on-line signature verification. Proc IEEE Trans Biometrics 85(2):215–239
43. Nassery P, Faez K(1998) Signature pattern recognition using moments invariants and a new fuzzy LVQ model. IEICE Trans Inf Syst E81-D(12):1483–1493
44. Porwik P, Wrobel K (2008) Signature preprocessing based on Walsh coefficients. J Med Inf Technol 12:57–61
45. Quek C, Zhou RW (2002) Antiforgery: a novel pseudo-outer product based fuzzy neural network driven signature verification system. Pattern Recogn Lett 23(14):1795–1816
46. Rhee T, Cho S (2001) On line signature recognition using model guided segmentation and discriminative feature selection for skilled forgeries. In: Proceedings of Sixth International Conference on document analysis and recognition, pp 645–649
47. Sabourin R, Genest G, Preteux FJ (1997) Off-line signature verification local granulometric size distributions. IEEE Trans Pattern Anal Mach Intell 19(9):976–988
48. Shafiei M, Rabiee HR (2003) A new on-line signature verification algorithm using variable length segmentation and Hidden Markov models. In: Proceedings of seventh International Conference on document analysis and recognition (ICDAR 2003), vol 1, pp 443–446
49. SVC2004 signature database http://www.cse.ust.hk/svc2004/

50. Takagi T, Sugeno M (1985) Fuzzy identification of systems and its applications to modelling and control. IEEE Trans Syst Man Cybern 15(1):116–132
51. Tanabe K, Yoshihara M, Kameya H, Mori S, Omata S, Ito T (2001) Automatic signature verification based on the dynamic feature of pressure. In: Proceedings of sixth international conference on document analysis and recognition (ICDAR 2001), pp 1045–1049
52. Tian W, Qiao Y, Ma Z (2007) A New scheme for off-line signature verification using DWT and fuzzy net. In: 8th ACIS International Conference on software engineering, artificial intelligence, networking, and parallel/distributed computing, pp 30–35
53. Velez JF, Sanchez A, Moreno AB, Esteban JL (2007) Introducing fuzziness on snake models for off-line signature verification: a comparative study. In: International Conference on intelligent systems design and applications, pp 843–848
54. Velez JF, Sanchez A, Moreno AB, Esteban JL (2009) Fuzzy shape-memory snakes for the automatic off-line signature verification problem. Fuzzy Sets Syst 160:182–197
55. Xuhua Y, Takashi F, Obata K, Uchikawa Y (1995) Constructing a high performance signature verification system using a GA method. in: IEEE Conference ANNES, pp 170–173
56. Zadeh LA (1965) Fuzzy sets. Inf Control 8:338–353
57. Zakaria R, Wahab AF, Ali JM (2010) Confidence fuzzy interval in verification of offline handwriting signature. Eur J Sci Res 47(3):455–463
58. Zhang B (2006) Off-line signature recognition and verification by kernel principal component selfregression. In: Proceedings of 5th International Conference on machine learning and applications (ICMLA'06), pp 28–33