Freehand Forgery Detection
Using Directional Density and Fuzzy Classifier

Han, Soowhan[*], ° Woo, Youngwoon[**]
Dept. of Multimedia Eng.[*], Dept of Computer Eng.[**]
Dongeui University

한수환[*], °우영운[**]
동의대학교 멀티미디어공학과[*]
동의대학교 컴퓨터공학과[**]

Abstract

This paper is concerning off-line signature verification using a density function which is obtained by convolving the signature image with twelve-directional 5x5 gradient masks and the weighted fuzzy mean classifier. The twelve-directional density function based on Nevatia-Babu template gradient is related to the overall shape of a signature image and thus, utilized as a feature set. The weighted fuzzy mean classifier with the reference feature vectors extracted from only genuine signature samples is evaluated for the verification of freehand forgeries. The experimental results show that the proposed system can classify a signature whether genuine or forged with more than 98% overall accuracy even without any knowledge of varied freehand forgeries.

1. Introduction

The verification of handwritten signature is an important research area, which has the numerous applications in banking, crime investigation and other high security environments. Automatic handwritten signature verification systems(AHSVS) are either on-line or off-line, which are differentiated by the data acquisition method [1][2]. In an off-line system, signature images are acquired with scanners or cameras after the complete signatures have been written. The problem of off-line signature verification can be stated simply as: given a signature and knowing the identity of the person whose signature is presented (i.e., by credit card number), verify that the signature belongs to that person or declare it to be a forgery. This task is more difficult than real-time input because the kinematic information of handwriting is lost.

A wide range of techniques have been applied in the past to solve the more difficult off-line signature verification problems[3][4][5][6]. In recent years, a classical back-propagation neural network classifier with the directional probability of the gradient on the signature image[7] and with geometric features[8][9] were introduced for the detection of random forgeries.

One of the important factor on off-line AHSVS is to select an appropriate classifier. In this paper, a triangular fuzzy membership function and a weighted fuzzy mean are utilized as a classifier without any knowledge of forged signatures. This fuzzy classifier has a simple structure and it can easily improve the classification results by a weighted fuzzy mean extracted from analyzing the incoming feature vectors.

Another important factor is to extract feature vectors representing the characteristics of signature images. In this paper, a global feature based on twelve-directional 5x5 gradient masks is presented. The approach taken for the feature extraction is as follows. The first step involves scanning actual signatures. Signatures that are written in a specified area of 0.5" by 2" are scanned and digitized with 256 dots per inch, and stored in a 128 by 512 pixel matrix, according to its gray level representation (quantified into 256 levels). The second step is to extract the signature image from the background after noise reduction. The third step involves the choice of orientation and its gradient amplitude for each pixel on the entire gradient images by using twelve-directional 5x5 Nevatia-Babu gradient masks[10]. After the normalization, this twelve-directional density function which preserves the overall shape information of the signature is used as a feature set. This feature vector is fed into the weighted fuzzy mean classifier to verify a signature whether it belongs to a genuine or forgery.

In this study, only the freehand forgeries which

are written in a forger's own handwriting without knowledge of the appearance of the genuine signature are considered, which means this paper focuss on the definition of the first processing stage of a complete AHSVS.

2. Preprocessing stage and Feature extraction

Preprocessing Stage : The goal of preprocessing stage is to extract the signature image from the noisy background. In this portion of the study, the four step preprocessing operations proposed by Ammar *et al.* are used[9]. The first step is to equalize and reduce the background by using equations (1) and (2) as follows.

$$p'(i,j) = p(i,j) - \frac{1}{m} \sum_{l=1}^{m} p(l,j) \tag{1}$$

$$(1 \le i \le m, 1 \le j \le n)$$

$$p''(i,j) = p'(i,j) \quad \text{if} \quad p'(i,j) > 0, \tag{2}$$
$$otherwise \quad p''(i,j) = 0$$

where $p(i,j)$: the original image, $p'(i,j)$: the equalized image, $p''(i,j)$: the equalized image after clipping, and m by n is the size of the image (128 by 512). Noise reduction is accomplished by the averaging process shown in equation (3) to the entire signature image.

$$\bar{p}(i,j) = \frac{1}{9} \sum_{l=i-1}^{i+1} \sum_{k=j-1}^{j+1} p''(l,k) \tag{3}$$

where $\bar{p}(i,j)$ is the averaged image. After this phase, the signature becomes separable from the background by thresholding. The threshold value, *THD*, is automatically selected based on an entropy method proposed by Kapur *et al* [12]. Next, the original density information is restored in the image by using equation (4).

$$\hat{p}(i,j) = p(i,j) \quad \text{if} \quad \bar{p}(i,j) > THD, \tag{4}$$
$$otherwise \quad \hat{p}(i,j) = 0$$

where $\hat{p}(i,j)$: the extracted image and $p(i,j)$: the original image. More details about algorithms and a sample signature before and after the preprocessing stage are found in [8][12].

Feature Extraction: Input to the weighted fuzzy mean classifier for the verification is the twelve-directional density function abstracted from the incoming signature image. It depends on the overall shape of the signature image, and is

assumed to have enough information for the detection of freehand forgeries. In the gradient computation process, the gain normalized 5x5 masks developed by Nevatia and Babu[11] are utilized to detect the orientation and amplitude of the edges.

The twelve-directional gradient masks $M_m(i,j)$ are convolved with each pixel on the entire signature image, which is shown in equation (5).

$$G_m(i,j) = M_m(i,j) \otimes S(i,j), \quad m = 1,2,3,\ldots,12 \tag{5}$$

where $M_m(i,j)$: the mth directional gradient mask, $S(i,j)$: a pixel on the signature image, and $G_m(i,j)$: the mth directional gradient amplitude.

The amplitude and orientation for each pixel are determined by the direction of the largest gradient, which is shown in equation (6) and (7).

$$G(i,j) = \max[|G_1(i,j)|, |G_2(i,j)|, \cdots |G_{12}(i,j)|] \tag{6}$$
$$A(i,j) = m \text{ (the directional index of the}$$
$$\text{largest gradient)} \tag{7}$$

where $G(i,j)$ and $A(i,j)$: gradient amplitude and orientation on signature pixel (i,j). In this paper, the directional intensity of the entire signature pixels is investigated for feature extraction. Thus the twelve-dimensional feature vector is abstracted by equation (8).

$$F(A(i,j)) = \sum_{i=1}^{128} \sum_{j=1}^{512} G^2(i,j) \tag{8}$$

According to equation (8), the feature value, $F(A(i,j)=m)$, is weighted more significantly for the pixels located on the well defined edge of the signature line by square of $G(i,j)$ to preserve the overall shape information. After this stage, $F(m)$ should be normalized for size. Finally, the directional density function of the signature image, $NF(m)$, is found by equation (9).

$$NF(m) = \frac{F(m)}{\sum_{m=1}^{12} F(m)} \quad where \quad m = 1,2,\ldots,12 \tag{9}$$

The directional density function of each incoming signature, $NF(m)$, is utilized as a feature vector to be an input of the fuzzy mean classifier for verification. It has an invariance property with respect to size (scale) and shift (translation), but it is sensitive to rotations. Figure 1 shows some

samples of genuine and forged signatures and their feature vectors, NF(m). The directional density values of two genuine signatures, (a) and (b) shown in figure 1, are very similar together, but different from feature values of freehand forger (c) and (d).

3. Weighted Fuzzy Mean Classifier

In general, a fuzzy classifier depends on the type of fuzzy membership function and the calculation method of mean value for membership grades[13].

The proposed fuzzy classifier in this study uses the triangular fuzzy membership function and the weighted fuzzy mean method(equation (10)) with each variance of the twelve-dimensional reference feature set utilized as the weights, w_i.

$$h_x(\mu_1(x_1), \mu_2(x_2), \cdots, \mu_n(x_n); w_1, w_2, \cdots, w_n)$$
$$= \sum_{i=1}^{n} \mu_i(x_i) \cdot w_i, \quad (\sum_{i=1}^{n} w_i = 1) \tag{10}$$

where μ_i and w_i are a membership grade and a weight for an ith feature value, x_i, respectively, and n is the dimension of incoming feature vector (12 in this paper).

Feature extraction : directional density extracted from each of four signatures
[a] and [b]: genuine signatures
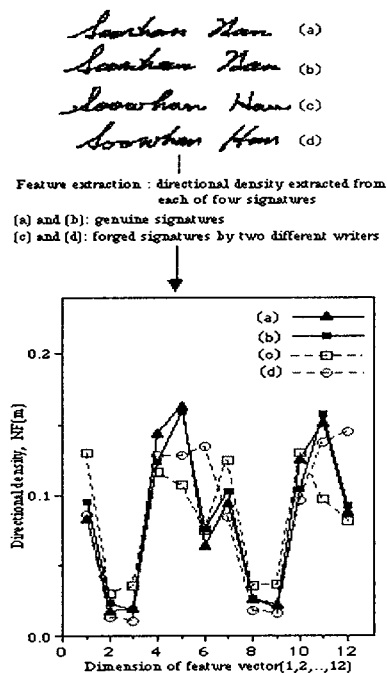[c] and [d]: forged signatures by two different writers

Figure 1. samples of genuine and forged signatures and their twelve-directional density function, NF(m).

The triangular type of fuzzy membership function is easy to apply where the only one reference feature set, which is the arithmetic mean of feature values of reference signature samples, is used as in this paper.

This type of fuzzy classifier does not require a training stage while the neural network structure does. In the experimental process, the membership functions for each of twelve-dimensional feature values are simply constructed by using the reference feature set and utilized for the verification of an incoming signature without any training procedure. The evaluation process is much simpler and easier than that of the conventional neural network classifier.

The construction of triangular membership functions and weights, and the verification process with and without weights are shown and discussed in the experimental section.

4. Experimental procedure and Verification results

The signature samples used in the experimental procedure consist of two data sets. Each of them contains 80 signatures taken from four different writers. One of four different writers was chosen as a target and asked to write his own name twenty times on a white sheet of paper using similar black ink ball point pens, with no constraint on the handwriting process, except for the 0.5" by 2" box where the signatures have to be written. Three of the remaining writers were assigned to be forgers. Each of the forgers was asked to write the targeted name twenty times in his/her own handwriting. The forgers were not allowed to study the samples of the original signature. Thus 20 genuine signatures and 60 freehand forgeries were collected for each data set. The target for the data set 1 is "Soowhan Han", and the other is "Dohong Jeon". Some samples of genuine and forged signatures for data set 1 and 2 are shown in fig. 2 and 3, and their twelve-directional density features in fig. 4 and 5, respectively.

In the experimental procedure, a labeled signature was presented to the fuzzy classifier, and it decided whether the signature was that of the person indicated by the label or was forgery. The construction of a fuzzy classifier and the classification process were done by as follows.
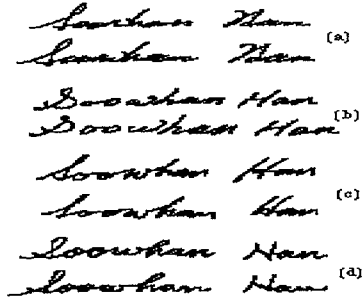
Figure 2. Two sample signatures for each writer in data set 1. ((a): genuine, (b)-(d): freehand forgeries from three other writers)
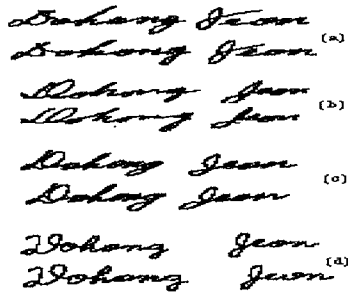

Figure 3. Two sample signatures for each writer in data set 2. ((a): genuine, (b)-(d): freehand forgeries from three other writers)
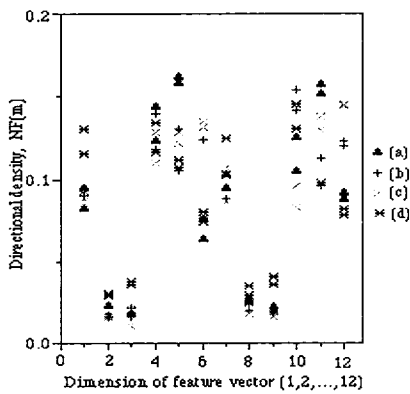

Figure 4. Twelve-dimensional feature values extracted from signature samples shown in figure 2.
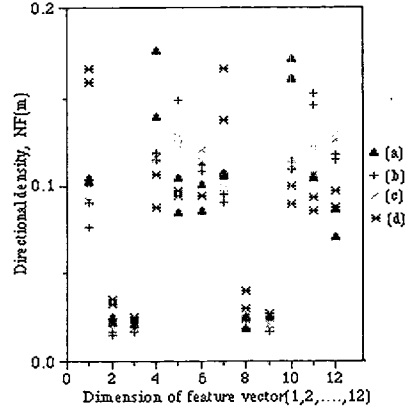

Figure 5. Twelve-dimensional feature values extracted from signature samples shown in figure 3.

Signature Verification : In neural network approach to signature verification problems, the variety of forged signatures is usually needed to train the neural classifier for the high performance [12]. However, under the real world environment, only a few forged signature samples are available. In this study, a fuzzy mean classifier without any knowledge of forged signatures is presented to decide an incoming signature whether it belongs to a genuine or forged signature.

Under this verification scenario, the reference feature set is constructed only for the genuine signatures and the weights for each of twelve-dimensional feature values are derived by equation (11).

$$w_i = 1 - \frac{vr_i - \min(vr_i)}{\max(vr_i) - \min(vr_i)} \tag{11}$$

where w_i is a weight for the ith feature value; vr_i is a variance of ith feature values in reference feature set only for genuine signature samples; $\min(vr_i)$ and $\max(vr_i)$ are an minimum and an maximum in vr_i : i=1,2,...,12, respectively.

By the equation (11), the ith dimension of feature values which has the minimum variance among twelve-dimension of reference feature set has a larger weight, and it means the ith feature values which are not significantly changed between genuine signature samples are more weighted. It has a benefit on verification process because the reference feature set is constructed with only genuine signature samples. The verification results with weights and without weights are compared in table 1 and 2.

In the verification process, the membership grades of the feature values for an incoming signature image are derived by equations (12)-(14).

$$\mu_i(x_i) = \frac{2.5(x_i - f_i)}{f_i} + 1 \quad \text{if} \quad x_i < f_i \quad (12)$$

$$\mu_i(x_i) = -\frac{2.5(x_i - f_i)}{f_i} + 1 \quad \text{if} \quad x_i \geq f_i \quad (13)$$

$$\mu_i(x_i) = \begin{array}{ll} \mu_i(x_i) & \text{if} \quad \mu_i(x_i) \geq 0 \\ 0 & \text{if} \quad \mu_i(x_i) < 0 \end{array} \quad (14)$$

where x_i is an ith feature value of input signature image, f_i is an ith feature value of reference feature set, and $\mu_i(x_i)$ is a membership grade for x_i.

Next, the fuzzy mean value with the weights is extracted by equation (15) and the signature is verified by equation (16). In case of without weights, h shown in equation (15) is simply a sum of membership grades of the twelve-dimensional feature values.

$$h(\mu_1(x_1), \mu_2(x_2), \ldots\ldots, \mu_{12}(x_{12}); w_1, w_2, \ldots\ldots, w_{12})$$
$$= \sum_{i=1}^{12} \mu_i(x_i) \cdot w_i \quad (15)$$

where h is a weighted fuzzy mean value for an incoming signature image, μ_i is a membership grade of the ith feature value, and w_i is a weight shown in equation (11).

$$h \geq THD \quad \text{accepted a genuine signature}$$
$$\quad (16)$$
$$h < THD \quad \text{rejected a forged signature}$$

where THD is a threshold value.

In the experiments, two different thresholds are selected. One is 85% of the weighted fuzzy mean value for randomly selected one of reference signature samples (a high THD), and the other is 65% of it (a low THD). Each of two data sets which has 20 genuine signatures and 60 freehand forgeries was evaluated with both of two different thresholds, and also tested with weights and without weights. Five independent simulations were performed with a different choice of signature

Table 1. Averaged verification results for data set 1 (Soowhan Han).

reference feature set / verification results(%)		1	2	3	4
RCA	without weight	90.00 (64.00)	96.00 (96.00)	96.00 (96.00)	99.00 (96.00)
	with weights	—	95.00 (97.00)	100.00 (98.00)	99.00 (100.00)
RCR	without weights	95.33 (99.67)	95.67 (96.33)	96.00 (97.33)	94.00 (96.67)
	with weights	—	99.00 (99.33)	98.33 (99.33)	99.67 (100.00)
SR	without weights	94.00 (90.75)	95.75 (96.25)	96.00 (97.00)	95.25 (96.50)
	with weights	—	98.00 (98.75)	98.75 (99.00)	99.50 (100.00)

* reference feature set 1 is the feature values extracted from randomly selected one genuine signature image.
* reference feature set 2,3 and 4 are the averaged feature values extracted from randomly selected three, five and ten genuine signature images, respectively. ( ) : verification results with a high THD

Table 2. Averaged verification results for data set 2 (Dohong Jeon).

reference feature set / verification results(%)		1	2	3	4
RCA	without weight	80.00 (68.00)	99.00 (98.00)	100.00(100.00)	100.00(100.00)
	with weights	—	99.00 (99.00)	100.00(100.00)	100.00(100.00)
RCR	without weights	99.00 (100.00)	96.00 (98.00)	96.00 (98.00)	93.67 (97.33)
	with weights	—	97.67 (99.33)	97.33 (100.00)	99.00 (100.00)
SR	without weights	94.25 (92.00)	96.75 (98.00)	97.00 (98.50)	96.25 (98.00)
	with weights	—	98.00 (99.50)	98.00 (100.00)	99.25 (100.00)

* reference feature set 1 is the feature values extracted from randomly selected one genuine signature image.
* reference feature set 2,3 and 4 are the averaged feature values extracted from randomly selected three, five and ten genuine signature images, respectively. ( ) : verification results with a high THD

samples for reference feature set, and the verification results were calculated by using the expressions shown in eqs. (17)-(18) and averaged. They are summarized in table 1 for data set 1 and table 2 for data set 2.

Ratio of Correct Acceptance(RCA) =
$$\frac{num.\ of\ correctly\ accepted\ genuine\ signatures}{total\ num.\ of\ tested\ genuine\ signatures} \times 100 \quad (17)$$

Ratio of Correct Rejection (RCR) =
$$\frac{num.\ of\ correctly\ rejected\ forgeries}{total\ num.\ of\ tested\ forgeries} \times 100 \quad (18)$$

System Reliability (SR) =
$$\frac{\substack{num.\ of\ correctly\ accepted\ genuine\ signatures \\ +\ num.\ of\ correctly\ rejected\ forgeries}}{total\ num.\ of\ tested\ signatures} \times 100 \quad (19)$$

The reference feature set 1 is constructed with only one genuine signature sample. Thus the weights derived by the variance of each dimensional feature value of reference signature samples cannot be applied to the verification process. The RCA with reference feature set 1 is relatively low when a high THD was used, which means the fuzzy classifier with a high THD made a lot of false rejections. However a THD does not significantly affect the verification results where more signature samples are available for the reference feature set. It is shown in SR with reference feature set 3 and 4. And the fuzzy classifier with the reference feature set constructed with more signature samples shows the better verification ratios. From table 1 and 2, it is clear that the verification results can be easily improved by using the weights, and the system reliability with reference feature set 4, SR, is reached over 99% for both of two data sets.

5. Conclusion

From the high verification results in the experimental process, it is known that the weighted fuzzy mean classifier with the twelve-directional density features obtained by convolving the signature image with 5x5 Nevatia-Babu gradient masks performs well to verify an incoming signature whether it is a genuine or forged signature. In the verification process, only the genuine signature samples are utilized for the reference feature set because a few forged signature samples are available under the real world environment. The further research area in a near future should involve an investigation of feature extractions from a signature image which contain more detailed shape information characterizing the genuine signature while still maintaining relatively small dimensionality for inputs to the fuzzy classifier.

References

[1] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification-the state of the art," *Pattern Recognition*, Vol. 22, No. 2, pp. 107-131, 1989.

[2] G.Pirlo, *Alogorithms for signature verification, Fundamentals in Handwriting Recognition*, S, Impedovo, ed., pp.435-452, Springer, Berlin, 1994.

[3] F. Nouboud, *Handwritten signature verification: a global approach, Fundamentals in Handwriting Recognition*, S, Impedovo, ed., pp.455-459, Springer, Berlin, 1994.

[4] R. Sabourin, M. Cheriet and G. Genest, " An extended shadow-code based approach for off-line signature verification", *Proc. ICDAR'93: Int. Conf. on Document Analysis and Recognition*, Tsukuba Science City, Japan, pp.1-5, IEEE Computer Society Press, 1993.

[5] S.N. Nam, J.Y. Park, and S.B. Rhee, "A Study on Signature Identification using the Distribution of Space Spectrum", *Journal of the Korea Institute of Telematics and Electronics*, Vol. 30,No.9, pp. 638-644, August, 1993, Korea.

[6] R .N. Nagel and A. Rosenfeld, "Computer detection of freehand forgeries," *IEEE Trans. Computers*, Vol. C-26, No. 9, pp. 895-905, 1977.

[7] R. Sabourin and J. P. Drouhard, "Off-line signature verification using directional PDF and neural networks," *Proc. of 11th IAPR International conference on Pattern Recognition*, Vol. 2, pp. 321-325, 1992.

[8] H. Kai and H. Yan, "Off-Line Signature Verification Based on Geometric Feature-Extraction and Neural Network Classification", *Pattern Recognition Letters*, Vol.30, No.1, pp.9-17, 1997.

[9] R. Bajaj and S. Chaudhury, "Signature Verification Using Multiple Neural Classifier", *Pattern Recognition Letters*, Vol.30, No.1, pp.1-7, 1997.

[10] R. Nevatia and K. R. Babu,"Linear Feature Extraction and Description", *Computer Graphics and Image Processing*, Vol.13, No.3, pp.257-269, July, 1980.

[11] J. N. Kapur, P .K. Sahoo, and A. K. C. Wong, "A new method for grey-level picture threshold using the entropy of the histogram," *Computer Vision, Graphics, and Image Processing*, Vol. 29, pp. 273-285, 1985.

[12] Soowhan Han, "A new approach for off-line signature verification using fuzzy ARTMAP", *Journal of Fuzzy Logic and Intelligent Systems in Korea* , Vol. 5, No. 4, pp. 33-40, Dec., 1995.

[13] H. J. Zimmermann, *Fuzzy Set Theory and Its Applications*, pp. 217-239, Kluwer Academic Publishers, 1996.