Mathematical Problems of Computer Science 36, 115–120, 2012

Off-Line Signature Verification and Recognition

Vahe Khachaturyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: vahe@7smarts.com

Abstract:

In this paper we propose a technique that can be used for signature recognition. This technique is a contour based technique. Here we propose a simple and effective approach that can be easily implemented in a programming language.

The paper deals with the recognition of the signature, as human operator generally makes the work of signature recognition. Hence the algorithm simulates human behavior, to achieve perfection and skill through AI. The logic that decides the extent of validity of the signature must implement Artificial Intelligence Pattern recognition is the science that concerns the description or classification of measurements, usually based on underlying model. Since most pattern recognition tasks are first done by humans and automated later, the most fruitful source of features has been to ask the people who classify the objects how they tell them a part. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. This technique gives acceptable results in a simple and fast way.

Key words: Pattern Recognition, Signature Recognition, Image Morphology

1. Introduction

Signature of a person is an Important Biometric Attribute of a human being and is used for authorization purpose for decades. With a lot of computing power available with modern computers there is a vast scope to develop fast algorithms for signature recognition. There is a lot of research work being conducted in this field.

Various approaches are possible for signature recognition with a lot of scope of research. In this paper we deal with an Off-line signature recognition technique, where the signature is captured and presented to the user in the format of image only. We use various image processing techniques to extract the parameters of signatures and verify the signature based on these parameters.

Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. [1], [2].

2. Off-Line Signature Verification

Literature Overview Automatic off-line signature verification is a very old pattern classification problem, involving the discrimination of genuine and forgery signatures, written on a piece of paper. Unlike on-line systems, off-line systems have only the image of a signature as input; in other words, dynamic information is not available for the off-line signature verification. Other difficulties such as variation within genuine signatures, noise introduced by the scanning device or a difference in pen width make off-line signature verification a challenging problem. It is worth to notice that, even professional forensic examiners perform at about 70% of correct classification rate (genuine or forgery). The difficulty of the classification can be appreciated by looking at the Figure which depicts four genuine and test signatures. Although the test signature seems to be authentic, it is actually a forgery. [3], [4], [5] [6] et al.

3. Contour Generation

The scanned signature is first pre-processed to get a normalized binary image. We follow a series of operations like noise removal using filtering, Scaling, Smoothening, Intensity normalization, Thinning. This gives us a binary signature template. This is shown in following figures[7].

PREPROCESSING

The preprocessing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signatures standard and ready for feature extraction. The preprocessing stage includes four steps: Background elimination, noise reduction, width normalization and skeletonization. The preprocessing steps of an example signature are shown in Fig. 1.

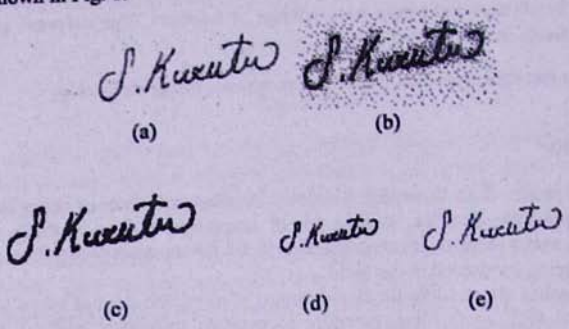

Fig 1. Preprocessing steps: (a) scanning, (b) background elimination, (c) noise reduction, (d) width normalization, (e) thinning applied signatures.

3.1 Background Elimination

Data area cropping must be done for extracting features. P-tile thresholding was chosen to capture signature from the background. After the thresholding the pixels of the signature would be "1" and the other pixels which belong to the background would be "0".

3.2 Noise Reduction

A noise reduction filter is applied to the binary image for eliminating single black pixels on white background. 8-neighbors of a chosen pixel are examined. If the number of black pixels is greater than the number of white pixels, the chosen pixel will be black otherwise it will be white.

3.3 Width Normalization

Signature dimensions may have intrapersonal and interpersonal differences. So the image width is adjusted to a default value and the height will change without any change on height-to-width ratio. At the end of width normalization the width dimension is adjusted to 100.

3.4 Thinning

The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick. In this system Hilditch's Algorithm is used.

We use the normalized template for further processing. The signature has intra-class variations i.e. signatures of a same user have variations, but these variations are limited. Forged signatures (Simple forgeries) and different user's signatures have vast variations (Inter – Class variations). We try to detect these variations in signature segments.

We generate a contour of signature; this contour is actually the external boundary of the signature. The Dilation algorithm is used for this and various levels of dilations are used. This is achieved in programming environment by drawing circles of various radii on the templates and filling them with appropriate color; the circles are drawn with radii r1, r2, r3, r4. Where r4 > r3 > r2 >r1. This operation gives a structure with bands of varying thickness. These bands of colors will represent the variation extent of each pixel and hence the signature segments. This structure is shown in Fig 2.

Fig 2. Contour Generated for signature

The four bands in the testing program were generated with r1=3 Pixel, r2=6 Pixel, r3=10 Pixel and r4=16 Pixel radius and filled with Black, Red, Green, Blue colors respectively. The colors are represented in (R,G,B) format where Red=(255,0,0), Green=(0,255,0), Blue=(0,0,255) and white=(255,255,255), Black=(0, 0, 0). We call this bands pattern as a "Check pattern". In the next section we discuss the detection process.

4. Detection Methodology

For training purpose we take three standard signatures from a user and generate the same band structure for them. For detection purpose we use two templates at a time, one is the test signature and the other is from the standard templates.

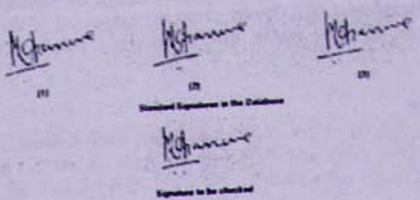

Fig 3.Standard Signatures and the test signature.

Similar check pattern is generated for the test signature. To find the matching between two templates we then perform an EX-OR operation on the two templates.

This EX-OR operation will be performed on the (R, G, B) color triplet of each pixel because of this in the test(x, y) template various colors are generated by the EX-ORing of R G B bands R(255,0,0) Ex-Or G(0,255,0) will yield (255,255,0) If the same color is there it will generate (0, 0, 0) Black (0, 0, 0) Ex-Ored with Any of the R, G, B bands will give the same color only i.e. R, G, B only. The R G B bands in sign template are actually the allowed variations for the pixel and if the pixel is in the allowed variations it will generate Either of the pure R, G, B or otherwise any combination of R, G, B. Pure Black pixels are un-deviated pixels (Black (0, 0, 0) Ex-Or Black (0, 0, 0) Will give (0, 0, 0) i.e. Black only). The color codes used are as follows.

TABLE I

COLOUR CODES USED IN SOFTWARE PROGRAM

0. Black	0	0	0
1. Red	255	0	0
2. Green	0	255	0
3. Blue	0	0	255
4. Background color	0	100	96
5. White	255	255	255
6. Color1	0	252	255
7. Color2	255	8	255
8. Color3	255	252	0
9. Test result background	255	156	168

The check pattern after Ex-Or operation is shown in Fig. 4

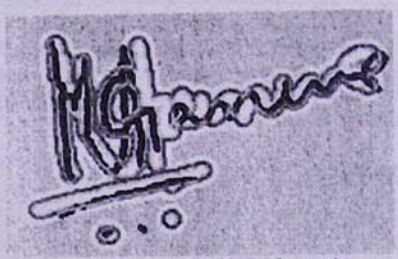

Fig 4. Check Pattern generated after EX-ORing of two signature templates.

The next stem of the operation is to scan this check pattern and count the number of pixels of each color, Red (NR), Green (NG), Blue (NB), Black (NBK) and White (NW) respectively.

We give these parameters as inputs to a neuro-fuzzy classifier. The fuzzy logic detector has four participation sets Perfect, Good, Okay and Rejected, for which the output of neural network is given.

5. Conclusion

We have implemented a simple contour based signature recognition technique. Along with various parameters like the number of pixels, Angle of rotation, width, height we are using check pattern generated by dilation. We use EX-Oring of the bands in check pattern to find out variation in signature pixels.

While implementing the recognition process, we have use quite simpler way. At this stage we are getting accuracy up to about 80% to 90%. The accuracy can be achieved up to 100% by implementing very tight preferences, but in practical situations tradeoffs can be achieved by user's discretion. After checking several signatures, we found that the irrelevant signatures are surely rejected by the software but it is possible that the signature that one thinks to be passed will be rejected. This can be achieved through providing more number of training signatures.

This technique is simple to apply in a program coding and further performance can be improved by using better classification algorithm.

6. References

[1] M. Sonka, V. Hlavac and R. Boyle, "Image processing analysis, and machine vision", *Thomson Learning, Singapore*, pp. 563-64, 573, 583, 593, 2002.

[2] S. Loncaric, A. Dhawan," A morphological signature transform for Shape Description." *Pattern Recognition*, 6: pp. 1029-1037. 1993.

[3] Evett and R. N. Totty, "Study of the variation in the dimensions of genuine signatures", *Journal of the Forensic Science Society*, vol. 25, pp. 207-215, 1985

[4] 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*, vol. 36, pp. 91-101, 2003.

[5] Y. Mizukami, H. Miike, M. Yoshimura, and I. Yoshimura, "An Off-Line signature verification system using an extracted displacement function", *In Proceedings of ICDAR*, pp. 757-760, 1999.

[6] W. F. Nemcek and W. C. Lin, "Experimental investigation of automatic signature verification" *IEEE Transactions on Systems, Man and Cybernetics*, vol. 4 , pp. 121-126, 1974.

[7] T. Joachims, "Text categorization with support vector machines: Learning with many relevant features". *Proceedings of the Tenth European Conference on Machine Learning*. Berlin: Springer, pp. 137 -142, 1998.

<<Օֆլայն>> ստորագրության ճանաչում

Վ. Խաչատուրյան

Ամփոփում

Աշխատանքում առաջարկվում է <<Օֆլայն>> ստորագրության ճանաչման եղանակ՝ հիմնված եզրագծային ներկման վրա, կախված տարբեր պարամետրերից՝ փիքսելների քանակ, շեղման անկյուն, լայնություն, բարձրություն: Մենք օգտագործումենք EX- Oring ստորագրության իսկությունն ստուգելու համար: Բերվում է ստորագրության ճանաչման օրինակ:

Опознание “Офлайн” подписи

В. Хачатурян

Аннотация

В работе предлагается метод опазнания „Офлайн” подписи основанный на контурное окрашивание в зависимости от многих параметров: количество пикселеи, угол наклона, широта, высота. Мы используем EX-Oring для проверки подлинности подписи. Приводится пример опазнания подписи.