ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 6, March 2017

2ND National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-17)

23rd - 24th March 2017

Department of Electrical & Electronics Engineering, College of Engineering Perumon, Kollam, Kerala – 691601, India

Signature Verification Based on Function and Parameter Features

Rini A P [1], Lisha P P[2]

P.G. Student, Department of Computer Engineering, Model Engineering College, Thrikkakara, Kerala, India[1]

Assistant Professor, Department of Computer Engineering, Model Engineering College, Thrikkakara, Kerala, India[2]

ABSTRACT: Signature verification techniques employ various specifications of a signature. Feature extraction and feature selection have an enormous effect on accuracy of signature verification. Feature extraction is a difficult phase of signature verification systems due to different shapes of signatures and different situations of sampling. This paper presents a survey of features used in signature verification.

KEYWORDS:Signature verification, Feature extraction, Feature selection.

I. INTRODUCTION

People Authentication[1], has been known as an intrinsic part of social life. In recent century, biometric technology is used to verify people. Biometric authentication systems have been used in wide range of applications, such as; Banking Con-sumer Verification, Access Control Systems, etc.

The security requirements of the todays society have placed biometrics at the center of a large debate, as it is becoming a key aspect in a multitude of applications. The term biometrics refers to individual recognition based on a persons distinguishing characteristics. While other techniques use the possession of a token (i.e., Badge, ID card, etc.) or the knowledge of something (i.e., A password, key phase, etc.) to perform personal recognition, biometric techniques provides the inherent characteristics of the person to be recognized to perform this task.

A biometric system can either verify or identify. In verification mode, it authenticates the persons identity on the basis of his/her claimed identity. Instead, in identification mode, it establishes the persons identity (among those enrolled in a database) without the subjects having to claim their identity. Depending on the personal traits considered, two types of biometrics can be defined: Physiological or Behavioral.

- Physiological Biometrics: It is based on some physical parts of the human body, such as fingerprint, retina, hand scan recognition, etc.
- Behavioral Biometrics: It is based on measuring some characteristics and behaviors of the human, such as handwritten signature, voice, etc.
-

Handwritten signature recognition is one of the most common techniques to recognize identity of a person.

The objective of signature verification (SV) systems is to differentiate between original and forged signature, which isrelated to intra-personal and inter-personal variability. Intra-personal variation is variation among the signatures of sameperson and inter-personal is the variation between the originals and the forgeries. There will always be slight variations in a humans handwritten signature, the consistency generated by natural motion and practice over time generates a recognizable pattern that makes the handwritten signature suitable for biometric identification.

There are two types of signature verification including Offline (static) and Online (dynamic) verification. In offline setting, the shape of the signature by capturing or scanning them from papers and system must extract features from the picture of the signature. However, for online setting, system uses devices for capturing extra information while the user is signing. Online signatures have extra information for extraction such as time, pressure, pen up and down, azimuth, etc.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 6, March 2017

2ND National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-17)

23rd - 24th March 2017

Department of Electrical & Electronics Engineering, College of Engineering Perumon, Kollam, Kerala – 691601, India

Online signature verification can broadly be divided into two groups.

1. Parametric Approaches: A set of global features derived from the signal, e.g., average speed, pressure, the number of pen ups and pen downs, the number of strokes, etc., represent a signature pattern and consist of the feature vector of a signature. The feature vectors of the test and reference signatures, which have a common length and hence can be dealt with in a more straightforward way, are compared to decide if the test signature is authentic.
2. Functional Approaches: The time sequences describing local properties of an online signature are analyzed. Since the signatures of the same user usually have different lengths, we should use techniques appropriate for evaluating the similarity/dissimilarity between two signals of unequal lengths, among which Dynamic TimeWarping (DTW)[3] and Hidden Markov Model (HMM)[4] are the most commonly used.

A signature verification (SV) system authenticates the identity of any person, based on an analysis of his/her Signature through a set of processes which differentiates a genuine signature from a forgery signature. The precision of signature verification systems can be expressed by two types of error: the percentage of genuine signatures rejected as forgery which is called False Rejection Rate (FRR); and the percentage of forgery signatures accepted as genuine which iscalled False Acceptance Rate (FAR). While dealing with any signature verification system, we take FRR and FAR as its performance estimate parameters.

II. FEATURE EXTRACTION

Two types of features can be extracted from a signature.

- Function-Features: The signature is characterized in terms of a time function whose values constitute the feature set, such as position, velocity, pressure, etc.
- Parameter-Features: The signature is characterized as a vector of elements each representing a value of feature.

When function features are used, the signature is usually characterized in terms of a time function whose values constitute the feature set. When parameter features are used, the signature is characterized as a vector of elements, each one representative of the value of a feature. In general, function features allow better performance than parameters, but they usually require time-consuming procedures for matching.

Furthermore, parameters are generally classified into two main categories: global and local.

- Global features[2] are the features extracted from the whole signature image. Global features include signature area, signature height to width ratio, center of gravity, Maximum horizontal histogram and maximum vertical histogram, Image area, Edge point numbers of the signature, Signature height etc.
- Local features[2] are the features extracted from the small portion of signature image. Local features are so-called because of their relation to each point of the signature, such as height or width ratio of the stroke, stroke orientation, pixel density, etc.

Local parameters can be divided into Component-oriented parameters and Pixel-oriented parameters[2].

- Component-oriented parameters[2], which are extracted at the level of each component (i.e., height to width ratio of the stroke, relative positions of the strokes, stroke orientation, etc.).
- Pixel-oriented parameters[2], which are extracted at pixel level (i.e., grid-based information, pixel density, gray-level intensity, texture, etc.).

A. FUNCTION FEATURES

It is worth noting that some parameters, which are generally considered to be global features, can also be applied locally, and vice versa. For instance, contour-based features can be extracted at global level (i.e., envelopes extracted at the level of the whole signature) or at local level (i.e., at the level of each connected component).

Position, velocity, and acceleration functions are widely used for online signature verification. Position function is conveyed directly by the acquisition device where as velocity and acceleration functions can be provided by both the acquisition device and numerically derived from position. In recent years, pressure and force functions have been used frequently and specific devices have been developed to capture these functions directly during the signing process. In

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 6, March 2017

2ND National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-17)

23rd - 24th March 2017

Department of Electrical & Electronics Engineering, College of Engineering Perumon, Kollam, Kerala – 691601, India

particular, pressure information, which can be registered with respect to various velocity bands, has been exploited for signature verification in order to take advantage of interfeature dependencies. Furthermore, direction of pen movement and pen inclination have also been successfully considered to improve the performance in online signature verification, where as pen trajectory functions have been extracted from static signatures, in order to exploit the potential of dynamic information for offline signature verification as well.

In general, position, velocity, and pen inclination functions are considered among the most consistent features in online signature verification, when a distance-based consistency model is applied. This model starts from the consideration that the characteristics of a feature must also be estimated by using the distance measure associated to the feature itself.

B. PARAMETER FEATURES

some parameter features[2] that have been widely considered for automatic signature verification. Some parameters are specifically devoted to dynamic signature verification. This is the case of some global parameters that describe the signature apposition process, as the total signature time duration,the pen-down time ratio, and the number of pen lifts (pen-down, pen-up). Other parameters are numerically derived from time functions representative of a signature, like, for instance, the average (AVE), the root mean square (rms), and the maximum (MAX) and minimum (MIN) values of position, displacement, speed, and acceleration. In other cases, the parameters - that have been used for both dynamic and static signature verification - are determined as coefficients obtained from mathematical tools as Fourier, Hadamard, cosine, wavelet, Radom, and fractal transforms.

When grid-based parameters[2] are used, the signature image is divided into rectangular regions and well-defined image characteristics, such as ink-distribution or normalized vector angle, are evaluated in each region. Grid features and global geometric features are used to build multiscale verification functions. Texture features have also beenextracted, based on the co-occurrence matrices of the signature image, shape matrices, and gray-level intensity features that provide useful pressure information. The extended shadow code has been considered as a feature vector to incorporate both local and global information into the verification decision.

Whatever feature set is considered, the evidence that an individual's signature is unique has led many researchers to devote specific attention to the selection of the most suitable features for a signer. Indeed, signatures from different writers generally contain very few common characteristics, and thus, the use of a universally applied feature set is not effective. Feature selection in the domain of signature verification is also required because system efficiency, processing cost, and memory requirement are strictly dependent on the cardinality of the feature set. Therefore, the smaller the feature vector, the greater the number of individuals that can be enrolled in the system and the faster speeds that can be achieved in the verification process. In recent years, several techniques have been proposed for feature selection based on principal component analysis (PCA) and self-organizing feature maps, Sequential Forward Search/Sequential Backward Search (SFS/SBS), inter–intra class distance radios (ICDRs), and analysis of feature variability. Forgery based feature analysis has also been proposed to select feature sets well suited for random and skilled forgery, respectively. This approach has been motivated by evidence that some features are best suited for distinguishing skilled forgeries from genuine signatures whereas other features are better at distinguishing random forgeries.

Other approaches use the same features set for each person and face the problem of personalized feature selection by assigning a different weight to each feature. Neural networks (NNs) and genetic algorithms (GAs) have been widely used for determining genetically optimized weighted parameters, as well as for selecting optimal functions, personalized parameters, or signature strokes to be used for verification.

III. CONCLUSION

There are mainly two approaches to online signature verification: parametric approaches and functional approaches.Generally speaking, functional approaches provides better performance than parametric approaches, but require more time and more space.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 6, March 2017

2ND National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-17)

23rd - 24th March 2017

Department of Electrical & Electronics Engineering, College of Engineering Perumon, Kollam, Kerala – 691601, India

we extract some features of signature image. Here different algorithms can be used to extract these features which will be used as input for training and verification. The features can be classified as global and local features. Global features like width, height, aspect ratio are obtained from entire signature image. Local features are obtained from specific parts of the signature image. The set of features are selected for verification based on the requirement of the application.

REFERENCES

[1] Mohsen Fayyaz, Mohammad HajizadehSaffar, Mohammad Sabokrou and Mahmood Fathy "Feature Representation for Online Signature Verification", The International Symposium on AISP, pp. 211- 216, 2015.
[2] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 38, no. 5, pp. 609–635, Sep. 2008.
[3] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," Pattern Recognition, vol. 40, pp. 981-992, 3// 2007.
[4] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, HMM-based on-line signature verification: Feature extraction and signature modeling, Pattern Recognit. Lett., vol. 28, pp. 2325-2334, Dec. 2007.