International Journal of Electronics,
Communication & Instrumentation Engineering
Research and Development (IJECIERD)
ISSN 2249-684X
Vol. 3, Issue 1, Mar 2013, 77-86

SIGNATURE VERIFICATION & RECOGNITION – CASE STUDY

MEERA V. KANAWADE[1] & KATARIYA S. S[2]

[1]Electronics Department., AVCOE Sangamner, Ahmednagar, Maharashtra, India

[2]Assitant Professor, Electronics Department., AVCOE Sangamner, Ahmednagar, Maharashtra, India

ABSTRACT

For identification of a particular human being signatures prove to be an important biometric. The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. However human signatures can be handled as an image and recognized using computer vision. With modern computers, there is need to develop fast algorithms for signature recognition. There are various approaches to signature recognition with a lot of scope of research. In this paper, off-line signature recognition & verification is proposed, where the signature is captured and presented to the user in an image format. Signatures are verified cbn based on parameters extracted from the signature using various image processing techniques. This paper presents a case study on signature verification method for verifying offline-signatures .

KEYWORDS: Signature, Authentication, Offline-Signature Recognition & Verification

INTRODUCTION

As available computing power eventually increases and computer algorithms become smarter, tasks that a few years ago seamed completely unfeasible, now come again to focus. This partly explains why a considerable amount of research effort is recently devoted in designing algorithms and techniques associated with the problems like human handwritten signature recognition and verification.

OBJECTIVE

A signature recognition and verification (SRVS) is a system capable of efficiently addressing two individual but strongly related tasks (a)identification of the signature owner, and , (b) decision whether the signature is genuine or forger. Depending on the actual needs of the problem at hand, SRVSs are often categorized in two major classes: on-line SRVSs and offline SRVSs.

While for systems belonging to the former class, only digitized signature images are needed, for systems in the latter classes'. Information about the way the human hand creates the signature such as hand speed and pressure measurements, acquired from special peripheral units, is needed.

PROBLEM STATEMENT

Recognizing signatures ignoring the variations such as:

- Variations due to different pens
- Variations arising out of the fact that "No two signatures of the same person are exactly- same" , and
- Any marks on the paper or any such element.

Overcoming the above variations and establishing the authenticity of a Signature.

Handwritten signature verification has been extensively studied & implemented. Its many applications include banking, credit card validation, security systems etc. In general, handwritten signature verification can be categorized into two kinds' online verification and off–line verification. On–line verification requires a stylus and an electronic tablet connected to a computer to grab dynamic signature information. Offline verification, on the other hand, deals with signature information which is in a static format.

LITERATURE REVIEW

Signature verification systems are different both in their feature selection and their decision making methodologies. The features can be categorized in two types: global and local. Global features are those related to the signature as a whole, including the average signing speed, the signature bounding box, and signing duration. Frequency domain feature studied in this work are also examples of global features. Local features on the other hand are extracted at each point or segment along the trajectory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory and our piecewise AR model.

The decision methodology depends on whether global or local features are used. Even the signatures of the same person may have different signing durations due to the variability in signing speed. The advantage of global features is that there are a fixed number of measurements per signature, regardless of the signature length, making the comparison easier. When local features are used, one needs to use methods which are suitable to compare feature vectors which have different size.

The use of frequency domain system identification method for online signature verification has not been extensively considered as it studies this problem in a quite different perspective, though some relative techniques have been proposed. In the signature is normalized to a fixed length vector of 1024 complex numbers that encodes the x and y coordinates of the points on the signature trajectory. Performing FFT, 15 Fourier descriptors with largest magnitude were chosen to be the feature.

The system is tested using very small signature dataset (8 genuine signatures of the same user and 152 forgeries provided by 19 forgers), achieving 2.5% error rate. In [5], the authors also use the Fourier Transform, and proposed alternatives for the preprocessing, normalization and matching stages. The system is tested on a large database (dataset of around 1500 signatures collected from 94 subjects), and achieved 10% equal error rate for verification. In our project, while Fourier transform is also used, we explored this area more deeply on different types of normalization, feature extraction and decision making method adapted from system identification.Many research works on signature verification have been reported.

Researchers have applied many technologies, such as neural networks and parallel processing to the problem of signature verification and they are continually introducing new ideas, concepts, and algorithms. Other approaches have been proposed and evaluated in the context of random forgeries, like 2D transforms , histograms of directional data or curvature , horizontal and vertical projections of the writing trace of the signature, structural approaches , local measurements made on the writing trace of the signature and the position of feature points located on the skeleton of the signature. Following Plamondon et al a handwritten signature is the result of a rapid movement.

Hence, the shape of the signature remains relatively the same over time when the signature is written down on a pre-established frame (context) like a bank check.This physical constraint contributes to the relative time-invariance of the signatures, which supports using only static shape information to verify signatures. Some other solutions in the case of random forgeries are mainly based on the use of global shape descriptors as the shadow code, investigated by Sabourin et

al Other approaches using global shape descriptors such as shape envelope projections on the coordinate axes, geometric moments, or even more general global features such as area, height and width, have been widely investigated.

In offline models of signature verification are compared based on HMMs. The approach of employs a three expert system that evaluates the signature three different ways and judges it as genuine, forgery, or rejection by a majority vote of the three experts. In a signature verification system is presented that works with both static and dynamic features. In the authors infer that shape similarity and causality of signature's generation are more important than matching the dynamics of signing. This result indicates that this dynamics is not stable enough to be used for signature verification since the subject is trying to reproduce a shape rather than a temporal pattern. This is why we use, in this paper, only static images to verify signatures.

SIGNATURE RECOGNITION OVERVIEW

Introduction

Signature has been a distinguishing feature for person identification through ages. Signatures for long have been used for automatic clearing of cheques in the banking industry. Despite an increasing number of electronic alternatives to paper cheques, fraud perpetrated at financial institutions in the United States has become a national epidemic.

Since commercial banks pay little attention to verifying signatures on cheques mainly due to the number of cheques that are processed daily a system capable of screening casual forgeries will prove beneficial. Most forged cheques contain forgeries of this type. We in our project have tried developing a robust system that automatically authenticates documents based on the owner's handwritten signature.

Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation.

A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR.)The false rejection rate (FRR) and the false acceptance rate (FAR) are used as quality performance measures.

The FRR is the ratio of the number of genuine test signatures rejected to the total number of genuine test signatures submitted. The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted. When the decision threshold is altered so as to decrease the FRR, the FAR will invariably increase, and vice versa.

Signature is a special case of handwriting that can be considered as an image. There is a growing interest in the area of signature recognition and verification (SRVS) since it is one of the important ways to identify a person. Recognition is finding the identification of the signature owner.

FORGERIES

Automatic examinations of questioned signatures were introduced in the late 1960s with the advent of computers. As computer systems became more powerful and more affordable, designing an automatic forgery detection system became an active research subject.

Most of the work in off-line forgery detection, however, has been on random or simple forgeries and less on skilled or simulated forgeries.

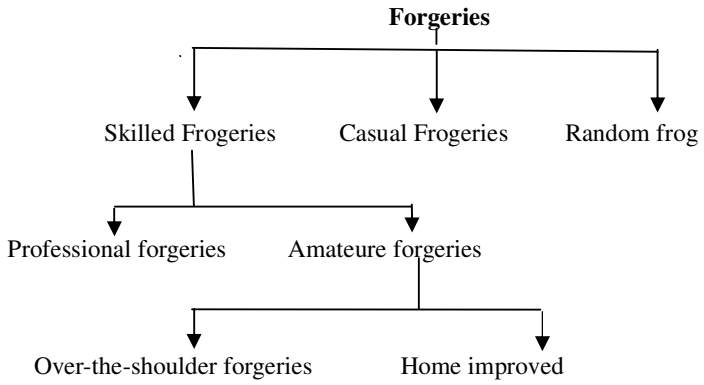
Before looking into the landmark contributions in the area of forgery detection, we first enumerate the types of forgeries .Verification is the decision about whether the signature is genuine or forged.

Forged images can be classified into three groups there are three kinds of forgeries –Skilled Random and Casual. Shown below is a self explanatory image of the various kinds of forgeries

Random Images: Are formed without any knowledge of the signer's name or signature shape.

Simple Images: Produce by people knowing the name of the signer's but without any example of the signature.

Skilled Images: Are produce by people looking at the original signature image and try to imitate it as closely as possible.



Various kinds of forgeries are classified into the following types:

Random Forgery

The signer uses the name of the victim in his own style to create a forgery known as the simple forgery or random forgery.

This forgery accounts for the majority of the forgery cases although they are very easy to detect even by the naked eye

Unskilled Forgery

The signer imitates the signature in his own style without any knowledge of the spelling and does not have any prior experience. The imitation is preceded by observing the signature closely for awhile.

Skilled Forgery

Undoubtedly the most difficult of all forgeries is created by professional impostors or persons who have experience in copying the signature. For achieving this one could either trace or imitate the signature by hard way. Figure 4 shows the different types of forgeries and how much they are varies from original signature.

Figure 1: a) Types of Forgery

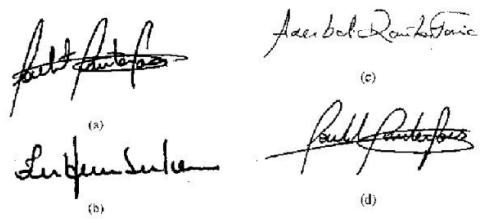


Figure 1: b) Types of forgery
(a) Genuine Signature; (b) Random Forgery; (c) Simulated Simple Forgery; (d) Simulated Skilled Forgery

Initially a set of signatures are obtained from the subject and fed to the system. These signatures and preprocessed Then the preprocessed images are used to extract relevant geometric parameters that can distinguish signatures of different persons. These are used to train the system. The mean value of these features is obtained. In the next step the scanned signature image to be verified is fed to the system. It is preprocessed to be suitable for extracting features. It is fed to the system and various features are extracted from them. These values are then compared with the mean features that were used to train the system. The Euclidian distance is calculated and a suitable threshold per user is chosen. Depending on whether the input signature satisfies the threshold condition the system either accepts or rejects the signature.

Handwritten signature verification is the process of confirming the identity of a user sing the handwritten signature of the user as a form of behavioral biometrics [1][2]. Automatic handwritten signature verification has been studied for decades. Many early research attempts were reviewed in the survey papers [3]. The main advantage that signature verification has over other forms of biometric technologies, such as fingerprints or voice verification, is that handwritten signature is already the most widely accepted biometric for identity verification in society for years. The long history of trust of signature verification means that people are very willing to accept a signature-based biometric authentication system [4].

TYPES OF SIGNATURE VERIFICATION

- Online Signature Verification
- Offline Signature Verification

Online Signature Verification

In On–line approach we can acquire more information about the signature which includes the dynamic properties of signature. We can extract information about the writing speed, pressure points, strokes, acceleration as well as the static characteristics of signatures. This leads to better accuracy because the dynamic characteristics are very difficult to imitate, but the system requires user co-operation and complex hardware. Digitizer tablets or pressure sensitive pads are used to

scan signature dynamically. On-line verification refers to a process that the signer uses a special pen called a stylus to create his or her signature, producing the pen location, speeds and pressures.

On-line signature verification schemes extract signature features that characterize spatial and temporal characteristics of a signature. The feature statistics of a training set of a genuine signature are used to build a model or template for validating further test signatures. Selecting a good model is the most important step in designing a signature verification system. Hidden Markov Model is one of the most widely used models for sequence analysis in signature verification. Handwritten signature is a sequence of vectors of values related to each point of signature in its trajectory. Therefore, a well-chosen set of feature vectors for HMM could lead to the design of an efficient signature verification system In all verification systems, the signature to verify is compared to the prototypes of the genuine signature at disposal by means of a similarity measure, often based on Dynamic Time Warping (DTW), or a distance between the signer's model and the signature at hand.

Offline Signature Verification

As compared to on-line signature verification systems, off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case. The verification process has to fully rely on the features that can be extracted from the trace of the static signature image only. Although difficult to design, off-line signature verification is crucial for determining the writer identification as most of the financial transactions in present times are still carried out on paper. Therefore, it becomes all the more essential to verify a signature for its authenticity. The design of any signature verification system generally requires the solution of five sub-problems: data acquisition, pre-processing, feature extraction, comparison process and performance evaluation. Off-line verification just deals with signature images acquired by a scanner or a digital camera. In an off-line signature verification system, a signature is acquired as an image. This image represents a personal style of human handwriting, extensively described by the graphometry.

In such a system the objective is to detect different types of forgeries, which are related to intra and inter-personal variability. The system applied should be able to overlook inter-personal variability and mark these as original and should be able to detect intra-personal variability and mark them as forgeries .In off–line signature recognition we are having the signature template coming from an imaging device, hence we have only static characteristic of the signatures. The person need not be present at the time of verification. Hence off-line signature verification is convenient in various situations like document verification, banking transactions etc. As we have a limited set of features for verification purpose, off-line signature recognition systems need to be designed very carefully to achieve the desired accuracy. The difference between the off-line and on-line lies in how data are obtained. In the on-line SRVS data are obtained using special peripheral device, while in the off-line SRVS images on the signature written on a paper are obtained using scanner or a camera [2].

In this research, an approach for off-line signature recognition and verification is proposed. The designed system consist of three stages: the first stage is pre-processing stage which applied some operations and filters to improve and enhance signature image. The purpose of the preprocessing stage is to determine the best signature image for the next stage which is feature extraction stage, choosing the right feature is an art more than a science. Three powerful features are used: global feature, texture feature and grid information feature [3]. The three features are calculated for each signature image and enter to the last stage which is neural network stage. Neural network consist of two-stage classifiers: the first classifier stage contain three back propagation (BP) neural networks, each one of the three BP takes its input from one of the three features and trained individually of each other. Each BP have two outputs that enter as an input to the second stage

classifier. The second stage classifier consists of two radial basis function (RBF) neural networks. It is the task of the second classifier (RBF) to combine the result of the first classifier (BP) to make the final decision of the system [4]. Off-line verification is concerned with the verification of a signature made by a normal pen. Various different approaches to both classes have been proposed.

SCHEME OF IMPLEMENTATION

Block Diagram

To perform verification or identification of a signature, several steps must be performed. After preprocessing all signatures from the database, then by enhancing the image various features will be extracted. Verification experiments are performed with neural-based classifiers. The present work has to be carried out in two steps. Initially a set of signatures are obtained from the subject and fed to the system. These signatures and preprocessed then the preprocessed images are used to extract relevant features like Extent, Solidity, Number of objects, Major axis length, Equivdiameter, Area, Convex area, Orientation and Euler number that can distinguish signatures of different persons. These are used to train the system.

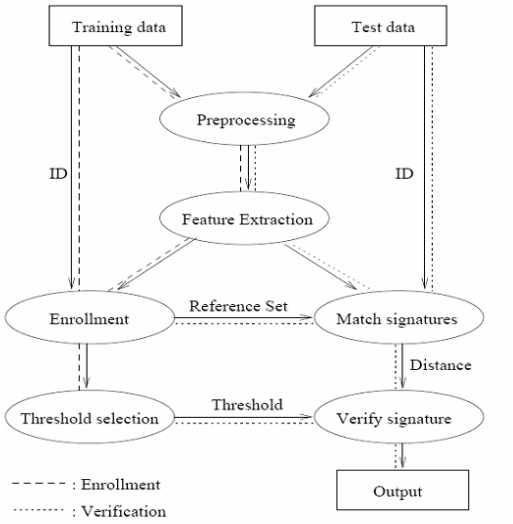


Figure 2.1: Flowchart of the Approach

The procedure for classification of signature image is as follows:

- Acquire the Signature images.
- Enhance image to remove noise and blurring.
- Extract the various features.
- Use these features to train the system using Feed Forward neural network.
- Employ unknown Signature image to extract its features.
- Perform the pattern matching with data set.
- Do the classification
- Take decision as originals or forgeries.

For implementation of signature verification a database of about 15-20 individuals actual signatures and also there forged signatures are required. The below figure describes the work flow of signature verification process. For

correctness of this first the signature is taken and care should be taken that is it should be free from noise & other ambiguities. Then matching process is used and depending on the results of the matched process final results are obtained that is whether the signature is original or forged one.

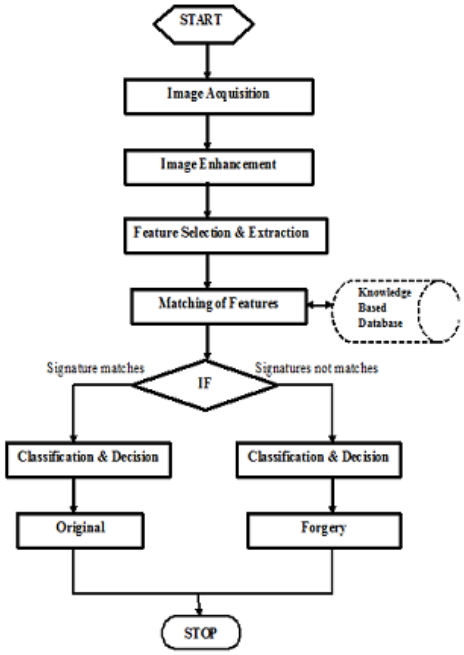


Figure 2.2: Workflow of Signature Verification System

The overall architecture of signature recognition system follows:

- Signature acquisition,
- Preprocessing,
- Feature extraction, and
- Classification.

In pre-processing stage, the RGB image of the signature is converted into grayscale and then to binary image.

Thinning is applied to make the signature lines as single thickness lines and any noise present in scanned images are removed thus making the signature image ready to extract features. Features available to extract in offline signatures can be either global features or texture feature i.e. features extracted from whole images. In this system, the features extracted are Aspect ratio, Signature Area, Maximum horizontal and maximum vertical histogram, End point number of the signature, texture Homogeneity, Texture contrast, Entropy. These extracted features Form the basis to compare and there by classify Signatures either genuine or forge. The features extracted from database are compared with the features extracted from test signatures and based on the classification criteria the signatures are classified either genuine or forged.

Signature Acquisition

Offline signatures are the signatures made on papers. This requires specifying the resolution, image type and format to be used in scanning each image. To this effect, a number of existing offline signature databases was studied. So in any offline signature verification system, the first step is to extract these signatures from papers using scanners. The sheet on which signature is made is provided to scanner which gives scanned image of the signature.

Preprocessing

After an image is acquired, it goes through different levels of processing before it is ready for the next step of feature extraction. The following are the reasons why image preprocessing is important:

- It creates a level of similarity in the general features of an image, like the size aspect. This enhances the comparison between images.
- Signatures vary according to the tool that was used in writing; the type of pen/pencil, the ink, the pressure of the hand of the person making the signature, and so on. In off-line signature recognition, these facts are not important, and have to be eliminated and the matching should be based on more important offline features.
- Noise reduction, defects removal and image enhancement.
- Improves the quality of image information.
- It eases the process of feature extraction, on which the matching depends mainly.
- Image pre-processing differs according to the genre that the image belongs to. The techniques used in this process may vary. There are 4 techniques that are used for signature recognition including; reading, displaying and resizing of the image, segmentation, binarization, fast Fourier transform (FFT), enhancement and thinning

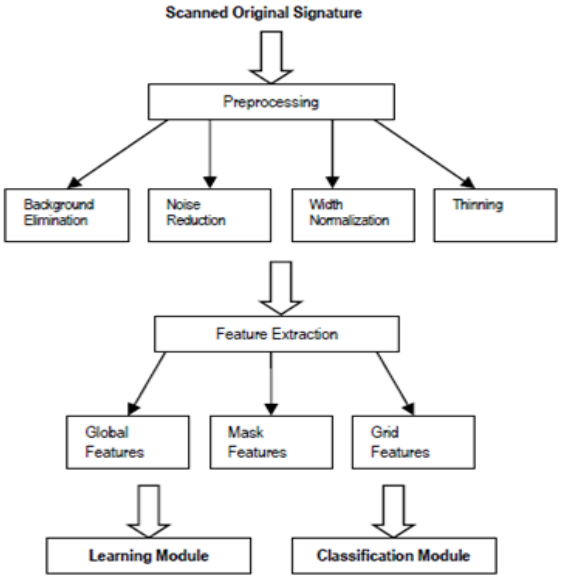


Figure 2.3: Block Diagram of Signature Verification System

Signatures are scanned in gray. The purpose in this phase is to make signatures standard and ready for feature extraction. The preprocessing stage includes following steps:

- Image binarization
- Background elimination,
- Noise reduction,
- Width normalization and
- Thinning.

The preprocessing steps of an example signature are shown in Fig.

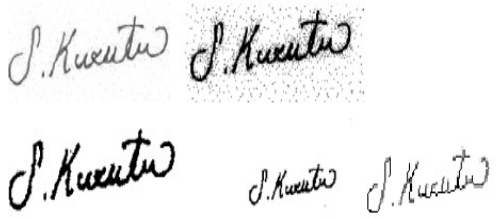


Figure 2.4: Preprocessing Steps: (a) Scanning, (b) Background Elimination, (c) Noise Reduction, (d) Width Normalization, (e) Thinning Applied Signatures

CONCLUSIONS

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

REFERENCES

1. OFF-LINE SIGNATURE VERIFICATION AND RECOGNITION BY SUPPORT VECTOR MACHINE

   Emre Özgündüz,Tülin Şentürk and M. Elif Karslıg Computer Engineering Department, Yıldız Technical University Yıldız , Istanbul, Turkey, phone: + (90) 212 3273673, fax: + (90) 212 3273673, email: emre_ozgunduz@yahoo.com, tulinsenturk@hotmail.com, elif@ce.yildiz.edu.tr

2. J. F. Vélez, Á. Sánchez , and A. B. Moreno, "Robust Off-Line Signature Verification Using Compression Networks And Positional Cuttings", Proc. 2003 IEEE Workshop on Neural Networks for Signal Processing, vol. 1, pp. 627-636, 2003

3. Sansone and Vento, "Signature Verification: Increasing Performance by a Multi-Stage System", Pattern Analysis & Applications, vol. 3, pp. 169–181, 2000.

4. E. J. R. Justino, F. Bortolozzi and R. Sabourin, "Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries", ICDAR 2001, International Conference on Document Analysis and Recognition, vol. 1, pp. 105--110. 2001

5. B. Zhang, M. Fu and H. Yan, "Handwritten Signature Verification based on Neural 'Gas' Based Vector Quantization", IEEE International Joint Conference on Neural Net-works, pp. 1862-1864, May 1998.

6. M. Arif and N. Vincent, "Comparison of Three Data Fu-sion Methods For An Off-Line Signature Verification Prob-lem", Laboratoire d'Informatique, Université de François Rabelais, 2003