Offline Verification for Handwritten Signatures Using Chain Code

Anis Ismail
Lebanese University, Lebanon

Aziz M. Barbar
American University of Science & Technology, Lebanon

INTRODUCTION

Signatures are used every day to authorize the transfer of funds of millions of people. Bank checks, credit cards, and legal documents all require signatures. Forgeries in such transactions cost millions of dollars each year. Handwritten Signature Verification (HSV) is the process of confirming the identity of a user using the corresponding handwritten signature as a form of behavioural biometrics for authentication and authorization.

Computer based signature verification can be divided into two main approaches, the online (or dynamic) and the offline (or static) approaches. In online signature recognition, the whole process of signing is done using a special pen called a stylus. The pen location, speed, velocity, and acceleration are captured using some acquisition devices (stylus, digital tablet, etc.), then analyzed and used to take a decision. The aim of offline signature verification is to decide whether a signature had originated from a given signer; a decision merely based on the scanned image of the signature and a few images of the original signatures of the signer. Unlike online signature verification, which requires special acquisition hardware and setup, offline signature verification can be performed independently from the normal signing process, and is thereby less intrusive and more user friendly.

Usually three kinds of forgery can happen in signature verification: a) random forgery is taking the genuine signature of others for that of the current user, b) skilled forgery is produced with close imitations – can be differentiated from the genuine one by shape variations, c) simple forgery is produced with the knowledge of content but without close imitations.

Several research papers have discussed signature recognition. Most published work uses the concept of feature recognition (Martínez & López, 2002), while some papers use the concept of Neural Networks (Sansone & Ven, 2000) and Hidden Markov Models (Muramatsu & Matsumoto, 2003). Automatic extraction of identity from personal traits (e.g. signature, fingerprint, speech, and face image) has given raise to a particular branch of pattern recognition, biometrics, where the goal is to infer identity of people from biometric data (Jain et al., 2004).

This article provides an easy to use application that detects digital signatures. It provides efficient algorithms that were implemented to recognize signatures on a one processor machine or on two processors. The algorithms are based on the digital image foundations where several algorithms are created and manipulated to provide a certain result. Our solution helps to detect, with minimum processing time, whether the input digital signature exists in a database that holds a huge set of records of different people's signatures.

BACKGROUND

Many systems have been implemented for signature verification. Ahmed et al. (Abdelrahman et al., 2013) presented an offline signature verification system using support vector machine technique. Global features are extracted from the signatures using radon transform. For each registered user in the database system, several reference signatures are enrolled and aligned for statistical information extraction about his/her signature. Dynamic time warping algorithm is used to align two signatures. During support vector machine

DOI: 10.4018/978-1-4666-5888-2.ch139

classifier training, many genuine and forged signatures are chosen. A signature's verification is established by first aligning it with each reference signature for the claimed user. The signature is then classified as genuine or forgery, according to the alignment scores which are normalized by reference statistics, using standard pattern classification techniques. Using a database of 2250 signatures (genuine signatures and skilled forgeries) from 75 writers in the proposed signature verification system, a performance of approximately 82% is achieved.

Authorizing handwritten signature has always been a challenge to prevent illegal transactions, especially when the forged and the original signatures are very "similar-looking" in nature. Tirtharaj et al. (Dash et al., 2012) aimed to automate forged signature verification process, offline, using Adaptive Resonance Theory type-2 (ART-2), which has been implemented in "C" language using both sequential and parallel programming. The said network has been trained with the original signature and tested with twelve very similar-looking but forged signatures. The mismatch threshold is set as 5%; however, it is set flexible as per the requirement from case-to-case. In order to obtain the desired result, the vigilance parameter (ρ) and the cluster size (m) have been tuned by carefully conducted parametric studies. The accuracy of the ART-2 was almost 100% with $\rho = 0.97$ and $m = 20$.

Recognizing handwritten signatures is important due to several legal issues. Manual verification is often difficult when very much 'similar-looking' but forged signature is produced. Tirtharaj et al. (Dash et al., 2013) tried to automate such kind of signature verification process offline using Adaptive Resonance Theory type-1 (ART-1). It is implemented using both serial and parallel processing, the performance of which are then compared. The said network has been trained with the original signature and tested with two forged signatures. The grade of similarity has been computed by introducing the term 'Similarity Index' (SI). Performance analysis reveals that after a careful tuning of vigilance parameter (ρ), both serial and parallel processing are able to learn the exemplary patterns with 100% accuracy. While testing, it is noted that parallel processing performs better than the serial processing in terms of speed as well as identifying the forged signatures by computing the mismatch.

A number of biometric techniques have been proposed for personal identification in the past. Among the vision-based ones are face recognition, fingerprint recognition, iris scanning, and retina scanning. Voice recognition or signature verification are the most widely known among the non-vision based ones. As signatures continue to play an important role in financial, commercial, and legal transactions, secured authentication becomes more and more crucial. A signature by an authorized person is considered to be the "seal of approval" and remains the most preferred means of authentication. The method presented in Ashwini et al. (Pansare & Bhatia, 2012) consists of image prepossessing, geometric feature extraction, and neural network training with extracted features and verification. A verification stage includes applying the extracted features of test signature to a trained neural network which will classify it as a genuine or forged.

Automating business transactions over the Internet relies on digital signatures, a replacement of conventional handwritten signatures in paper-based processes. Although they guarantee data integrity and authenticity, digital signatures are not as convenient to users as the manuscript ones. Eskander et al.(Eskander, et al., 2013) proposed to produce digital signatures using offline handwritten signatures. This methodology facilitates the automation of business processes, where users continually employ their handwritten signatures for authentication. Users are isolated from the details related to the generation of digital signatures, yet benefit from enhanced security. First, signature templates from a user are captured and employed to lock his/her private key in a fuzzy vault. Then, when the user signs a document by hand, his/her handwritten signature image is employed to unlock his private key. The unlocked key produces a digital signature that is attached to the digitized document. The verification of the digital signature by a recipient implies authenticity of the manuscript signature and integrity of the signed document. An experimental result on the Brazilian offline signature database (that includes various forgeries) confirms the viability of the proposed approach.

Darwish (Darwish, 2013) proposed an offline digital signature verification technique that depends on extracting several features from the signatures to be used during simulation. Some signatures were used for training and others were used for testing only. Different methods such as, vectors manipulation, ensemble classification using boosted trees, and bagged trees were used.