Combination of Off-Line and On-Line Signature Verification Systems Based on SVM and DST

Nassim Abbas and Youcef Chibani

Speech Communication and Signal Processing Laboratory,
Faculty of Electronics and Computer Science
University of Science and Technology Houari Boumediene (USTHB),
32, El Alia, Bab Ezzouar, 16111, Algiers, Algeria

nabbas@usthb.dz, ychibani@usthb.dz

Abstract—The objective of this work is to present a signature verification system based on combination of off-line and on-line systems for managing conflict provided by the Support Vector Machine (SVM) classifiers. This system is basically divided into three parts: i) off-line verification stage, ii) on-line verification stage and iii) combination module using Dempster-Shafer theory (DST). The proposed framework allows combining the normalized SVM outputs and uses an estimation technique based on the dissontant model of Appriou to compute the belief assignments. Combination is performed using Dempster-Shafer (DS) rule followed by the likelihood ratio based decision making. Experiments are conducted on the well known NISDCC signature collection using false rejection and false acceptance criteria. The obtained results show that the proposed combination framework using DST yields the best verification accuracy compared to the sum rule even when individual off-line and on-line classifications provide conflicting results.

Keywords-Off-line signature verification; On-line signature verification; Support Vector Machines; Dempster-Shafer theory; belief assignments; conflict.

I. INTRODUCTION

Biometrics is one of the most widely used approaches for person identification and authentication. Hence, several biometric modalities have been proposed in the last decades [1], which are based on physiological and behavioral characteristics depending on their nature.

Usually, the handwritten signature is the legal and social acceptance by many peoples. Hence, an intense research field has been devoted to develop various robust verification systems [2] according the acquisition mode of the signature. Thus, two acquisition modes are used for capturing the signature: off-line mode and on-line mode. The off-line mode allows generating a handwriting static image from a document scanning. In contrast, the on-line mode allows generating from pen tablets or digitizers dynamic information such as velocity and pressure. For both modes, many Handwritten Signature Verification Systems (HSVS) have been developed in the past decade [2]. Indeed, the handwritten signature remains important for many government/legal/financial transactions such as office automation, validation of cheques, credit cards, historical documents, etc [2]. Usually, the on-line HVS provides more reliable comparatively to the off-line HVS since features are more discriminative between users and are harder to imitate [2].

In order to enhance the performances of both handwritten signature verification systems, we propose a combination method based on DST for managing the conflict generated from the two sources (off-line and on-line systems). The DST has already been used for combining various biometric modalities. For instance, Arif and Vincent [3] proposed a fusion methodology for two biometric applications. Nakanishi et al. proposed a parameter combination in Dynamic Time Warping (DTW) domain [4] for on-line signature verification. Motil et al. proposed a combination algorithm of on-line and off-line kernels [5] for signature verification using SVM. Recently, combination of off-line image and dynamic information which are obtained from the same signature [6] has been proposed that exploit global and local information.

In this paper, we propose to associate off-line and on-line signatures in order to improve the performance of single-source biometric systems and ensure greater security. Thus, the combination is performed through a biometric decision combination framework using Dempster-Shafer Theory (DST) [7]. The combination framework allows managing significantly the conflict generated between the outputs of SVM classifiers. The performance of the proposed combination framework is evaluated comparatively to the sum rule used in the probabilistic theory.

The paper is organized as follows. We give in section 2 a principle of DST. In section 3, we present the description of the proposed verification system. Experiments conducted on the NISDCC signature collection are presented in section 4. The last section gives a summary of the proposed combination framework.
II. Principle of Dempster-Shafer Theory

Generally, the signature verification is formulated as a two-class problem where classes are associated to genuine and impostor, respectively. Hence, the combination of the offline and on-line signatures, corresponding to two information sources, are performed through the DST. Therefore, we denote \( S^1 \) and \( S^2 \) two information sources, respectively, while \( \theta_{\text{gen}} \) and \( \theta_{\text{imp}} \) are classes corresponding to genuine and impostor signatures, respectively. For two-class problem, a reference domain also called the frame of discernment is defined as a finite set of exhaustive and mutually exclusive hypotheses: \( \Theta = \{ \theta_{\text{gen}}, \theta_{\text{imp}} \} \). To address the limitations of the sum rule defined in probabilistic framework, a theoretical framework for evidential reasoning with imperfect data has been proposed by Dempster then developed by Shafer [7]. Example of such approaches is the DS rule. The main concept of the DST is to distribute unitary mass of certainty over all the sub-sets of \( \Theta \) instead of making this distribution over the elementary hypothesis only. Therefore, the belief functions, also known as the basic belief assignment (bba), are computed on the power set defined as \( 2^\Theta = \{ \emptyset, \theta_{\text{gen}}, \theta_{\text{imp}}, \theta_{\text{gen}} \cup \theta_{\text{imp}} \} \), such that \( m(\cdot); 2^\Theta \rightarrow [0,1] \) and \( m(\theta_{\text{gen}}) + m(\theta_{\text{imp}}) + m(\theta_{\text{gen}} \cup \theta_{\text{imp}}) = 1 \). \( m(\theta_{\text{gen}} \cup \theta_{\text{imp}}) \) defines the mass of the ignorance, which is attributed when the two sources are not well distinguished.

III. Description of the System

The proposed combination handwritten signature verification system is composed of an off-line verification system, an on-line verification system and a combination module. \( s_1 \) and \( s_2 \) define the off-line and on-line handwritten signatures provided by two sources of information \( S^1 \) and \( S^2 \), respectively. Both verification systems are generally composed of three modules: pre-processing, feature generation and classification.

A. Pre-processing

According the acquisition mode, each handwritten signature is pre-processed for facilitating the feature generation. Hence, the pre-processing of the off-line signature consists to eliminate the useless information around the binarized image without unifying its size. While, the on-line signature, no specific pre-processing is required.

B. Feature Generation

Features are generated according the acquisition mode, which are based on the uniform grid for off-line signature and dynamic characteristics for on-line signature, respectively.

1) Off-Line Signature: Features are generated using the Uniform Grid (UG) [8]. For our case, we have fixed during all experiments the parameters \( n \) and \( m \) of the grid as \( (n = 5) \) and \( (m = 9) \), respectively. Therefore, the different values of features are finally stored in a vector \( x_1 \) of dimension \( 5 \times 9 \), which characterizes the off-line signature image.

2) On-Line Signature: For the on-line signature verification stage, features are generated using only the dynamic features. Each on-line signature is represented by a vector \( x_2 \) composed of 11 features [8]: signature total duration, average velocity, vertical average velocity, horizontal average velocity, maximal velocity, average acceleration, maximal acceleration, variance of pressure, mean of azimuth angle, variance of azimuth angle, and mean of elevation angle.

C. Classification Based On SVMs

1) Review of SVMs: The classification based on Support Vector Machines (SVMs) has been used widely in many pattern recognition applications as the handwritten signature verification [5]. The SVM is a learning method introduced by Vapnik et al. [9], which tries to find an optimal hyperplane for separating two classes. Its concept is based on the maximization of the distance of two points belonging each one to a class.

Basically, SVMs have been defined for separating linearly two classes. When data are non linearly separable, a kernel function \( K \) is used [9]. Example of such kernels is the Radial Basis Function (RBF) kernel. Then, the decision function \( f: \mathbb{R}^p \rightarrow \{-1,+1\} \), is expressed in terms of kernel expansion as:

\[
    f(x) = \sum_{k=1}^{Sv} \alpha_k y_k K(x,x_k) + b
\]

where \( \alpha_k \) are Lagrange multipliers, \( Sv \) is the number of support vectors \( x_k \) which are training data, such that \( 0 \leq \alpha_k \leq C \), \( C \) is a user-defined parameter that controls the tradeoff between the machine complexity and the number of nonseparable points [9], the bias \( b \) is a scalar computed by using any support vector.

2) Decision Rule: The direct use of SVMs does not allow defining a decision threshold to assign a signature to genuine or forgery classes. Therefore, outputs of SVM are transformed to objective evidences, which express the membership degree (MD) of a signature to both classes (genuine or forgery). In this paper, we use a fuzzy model which has been proposed in [8] to assign MD for SVM output in both genuine and impostor classes. Let \( f(x_d) \) be the output of a SVM obtained for an off-line \((d = 1)\) or on-line \((d = 2)\) signature to be classified. The respective
membership degrees $h_d(\theta_i), i = \{\text{gen, imp}\}$ associated to genuine and impostor classes are defined according to membership models given in [8]. Hence, a decision rule is performed about whether the signature is genuine or forgery as follows:

$$\text{if } \frac{h_d(\theta_{\text{gen}})}{h_d(\theta_{\text{imp}})} \geq t \text{ then } s_d \in \theta_{\text{gen}}$$
$$\text{else } s_d \in \theta_{\text{imp}}$$

where $t$ defines a decision threshold.

D. Classification Based On DST

The proposed combination is conducted into three steps: i) transformation of the normalized SVM outputs into belief assignments using estimation technique based on the dissonant model of Appriou, ii) combination of masses through a combination rule and iii) decision rule.

1) Estimation of Masses: Let the power set of hypotheses $2^\Theta = \{\emptyset, \theta_{\text{gen}}, \theta_{\text{imp}}, \theta_{\text{gen}} \cup \theta_{\text{imp}}\}$. In this paper, the mass functions are estimated using a dissonant model of Appriou, which is defined for two classes as given in [8].

2) Combination of Masses: In order to manage the conflict generated from the two sources (i.e. off-line and on-line SVM classifications), the combined masses are computed in two steps. First, the estimated belief assignments ($m_{id}(\cdot), i = \{\text{gen, imp}\}$) are combined for generating the belief assignments for each source as follows:

$$m_1 = m_{\text{gen}1} \oplus m_{\text{imp}1} \quad (2)$$
$$m_2 = m_{\text{gen}2} \oplus m_{\text{imp}2} \quad (3)$$

Finally, the belief assignments for the combined sources ($m_d(\cdot), d = 1, 2$) are then computed as:

$$m_c = m_1 \oplus m_2 \quad (4)$$

where $\oplus$ represents the basic sum rule combination (case of probabilistic framework), or DS rule combination (case of DST framework).

3) Decision Rule: A decision for accepting or rejecting a signature is made using the statistical classification technique. First, the combined beliefs are converted into probability measure using a probabilistic transformation, called pignistic probability (BetP), that maps a belief measure to a subjective probability measure [10].

Therefore, the decision rule is defined as:

$$\text{if } \frac{\text{BetP}(\theta_{\text{gen}})}{\text{BetP}(\theta_{\text{imp}})} \geq t \text{ then } s \in \theta_{\text{gen}}$$
$$\text{else } s \in \theta_{\text{imp}}$$

where $s = \{s_1, s_2\}$ is the $j$-th signature represented by both off-line and on-line modalities and $t$ is the decision threshold.

IV. EXPERIMENTAL RESULTS

A. Data Description and Performance Criteria

The Norwegian Information Security laboratory and Donders Centre for Cognition (NISDCC) signature collection contains simultaneously acquired on-line and off-line samples. The off-line dataset is called “NISDCC-offline” and contains only static information while the on-line dataset which is called “NISDCC-online” also contains dynamic information, which refers to the recorded temporal movement of handwriting process. Thus, the acquired on-line signature is available under form of a subsequent sampled trajectory points. Each point is acquired at 200 Hz on tablet and contains five recorded pen-tip coordinates: x-position, y-position, pen pressure, azimuth and elevation angles of the pen. Interested readers are directed to reference [11] for more details on these datasets. For evaluating the performances of the signature verification system, three different kinds of error have been considered: False Accepted Rate (FAR); False Rejected Rate (FRR) and finally the Half Total Error Rate (HTER). Thus, Equal Error Rate is a special case of HTER when $FRR = FAR$.

Signature data are split into training and testing sets for evaluating the performances of the proposed system.

B. SVM model

The SVM model is produced for each individual system according the uniform grid features and dynamic information, respectively. The NISDCC-offline dataset is composed of 1920 images from 12 authentic writers (5 authentic signatures per writer) and 31 forging writers (5 forgeries per authentic signature). For each writer and both datasets, 2/3 and 1/3 samples are used for training and testing, respectively. In our system, the RBF kernel is selected for the experiments. The optimal parameters ($C, \sigma$) for both SVM classifiers (off-line and on-line) are tuned experimentally, which are fixed as ($C = 9.1, \sigma = 9.4$) and ($C = 13.1, \sigma = 2.2$), respectively.

C. Verification Results and Discussion

The task of the proposed combination module is to manage the conflicts generated from both sources for each signature using the combination algorithms. For that, we compute the
verification errors of both SVM classifiers and the proposed combination frameworks with sum rule and DS rule. Fig 1.a and 1.b show the FRR and FAR computed for different values of decision threshold using the SVM classifier on both off-line and on-line data sets, respectively.

For better comparison, figure 2 shows the HTER computed for different values of decision threshold from the SVM classifiers and combination algorithms (sum rule and DS rule). Therefore, results corresponding to the optimal values of threshold are determined for each algorithm.

![Figure 1](image1.png)

(a) (b)

Figure 1. Performance Evaluation in SVM Framework: (a) Off-line signature verification, (b) On-line signature verification

![Figure 2](image2.png)

Figure 2. HTER Curves of Off-line, On-line and Combined Systems for Signature Verification

The off-line verification system based on SVM classifier yields a HTER of 12.47% corresponding to the optimal value of threshold \( t = 0.012 \) while the on-line verification system based on SVM classifier yields a HTER of 0.49% with an optimal value of threshold \( t = 0.195 \). The proposed combination framework with DS combination rule reduces the HTER to 0.16% (for an optimal value of the threshold \( t = 0.218 \)) corresponding to an improvement greater than 0.30%. While basic sum rule combination decreases the HTER to 50%. This is because the estimation model of masses which assigns the same confidence to the combined sources in probabilistic framework. Hence, the sum rule couldn’t handle managing correctly the conflict generated from the two sources.

V. CONCLUSION

We proposed and presented a new system for the signature verification by associating static image and dynamic information in order to improve simultaneously the performance of off-line and on-line verification systems to ensure a greater security. The combination framework is performed through the DS rule using the estimation technique based on the dissonant model of Appriou. Experimental results show that the proposed combination framework with DS rule yields the best verification accuracy compared to the sum rule even when the individual off-line and on-line classifications provide conflicting outputs.

REFERENCES