A Simple and Effective Method for Online Signature Verification

Napa Sae-Bae and Nasir Memon
Computer Science Department, NYU-Poly
Six Metrotech Center, Brooklyn, New York, 11201
nsae-b01@students.poly.edu, memon@poly.edu

Abstract: This paper presents a simple and efficient method for online signature verification. The technique is based on a feature set comprising of several histograms that can be computed efficiently given a raw data sequence of an online signature. The features which are represented by a fixed-length vector can not be used to reconstruct the original signature, thereby providing privacy to the user's biometric trait in case the stored template is compromised. To test the verification performance of the proposed technique, several experiments were conducted on the well known MCYT-100 and SUSIG datasets including both skilled forgeries and random forgeries. Experimental results demonstrate that the performance of the proposed technique is comparable to state-of-art algorithms despite its simplicity and efficiency.

1 Introduction

A handwritten signature is a socially and legally accepted biometric trait for authenticating a human. Typically, there are two types of handwritten signature verification systems: *off-line* and *online* systems. In an off-line system, just an image of the user's signature is acquired without any additional attributes, whereas, in an online system, a sequence of x-y coordinates of the user's signature along with associated attributes like pressure, time, etc., are also acquired. As a result, an online signature verification system usually achieves better accuracy than an off-line system [FJS11].

The increasing number of personal computing devices that come equipped with a touch sensitive interface and the difficulty of entering a password on such devices [FWW11] have led to an increased interest in developing alternative user authentication mechanisms on such devices [SBAIM12]. In this context, an online signature verification system is a plausible candidate given the familiarity users have with the concept of a signature for the purpose of authentication. This paper presents a simple online signature verification system that is suitable for use on personal computing devices. It has high accuracy with low computation, and space complexity as well as it requires a small number of enrollment samples. In addition, the stored template in the proposed system does not reveal the user's signature thereby providing privacy protection to an original biometric trait.

1.1 Previous Work

There have been two approaches proposed in the literature for online signature verification, namely, function-based and feature-based approaches [Pla89]. The former refers to a system where the matching process is done using, directly or indirectly, the original time sequence of the signature. The latter refers to a system where the matching process is done using descriptive features of the signature. Examples of well-known function-based approaches include Dynamic Time Warping Algorithm(DTW) [KY08,FZ07, FW03], and Hidden Markov Model(HMM) [OGFAS$^+$03].

The major advantage of a function-based approach is that it generally yields better verification accuracy than a feature-based system [FOGRGR07]. However, a user's biometric information is not protected, since, during the matching process, a dynamic construction of an original signature is revealed. Furthermore, the system is generally more complex and slower than feature-based systems [FW03]. Even worse, when a template protection approach is applied in order to provide biometric privacy and/or security, then

the verification performance can get significantly degraded. For instance, Maiorana et al [MMDC$^+$08] have proposed a convolution scheme to protect the original signature sequence of the user that can be directly applied to a function based approach in general. The idea is to split the original input sequence into W subsequences. Each subsequence may have a different selected length based on a random parameter. This technique has been applied with HMM and DTW based verification systems as reported in [MCN09, MMDC$^+$08, NMLC10]. They also reported that, with this convolved version of a signature, verification rates were lower when compared to the original version of the signature.

With a feature-based system, a clear template of a user's signature does not have to be stored. This results in increased biometric privacy and security. Further, there are many known algorithms to derive a cryptographic key [LTT12, CZC]from feature sets which are typically fixed length. However, the major difficulty for a feature-based approach for online signature verification is to derive a good set of descriptive features that can be used to effectively and efficiently verify an online signature [Pla89,FZ07,FW03].

There have been many proposals to derive a feature set from an online signature. In 2005, Fierrez-Aguilar et al [FANLP$^+$05] proposed a set of 100-features, such as total duration of signature, number of pen ups, sign changes of (dx/dt) and (dy/dt), etc. to represent an online signature and applied a feature selection method to rank the proposed features. Based on this 100-feature set, Nanni [Nan06] proposed a multi-matcher method to verify an online signature. The system achieved outstanding performance when two factor authentication is applied, namely a signature sample, and a user-specific token. In addition, Guru and Prakash [GP09] derived a symbolic representation of an online signature and introduced the concept of writer independent threshold in order to improve verification accuracy. Regardless of these efforts, however, the system performance has not been promising when only a feature set is used without a second factor.

Recently, Argones et al [ARMACC12] have proposed a set of HMM model features from a universal background model. The best reported verification performance obtained by their system is promising. However, the system extracts 4800 features from tuning 16 different HMM models, which is a computationally expensive task. Moreover, the universal background model is trained from a pool of 2500 genuine and forged signatures from 50 users on the same device specification, and, in addition, a user-specific classifier is trained from 10 signatures. These make it less feasible to be employed in a mobile device application scenario, where the embedded sensors are different from model to model and only a very few signatures can be taken from a user during enrollment.

1.2 Contributions

This paper presents a method to extract a model-free non-invertible feature set from an online signature. Specifically, the proposed feature set comprises of sets of histograms that capture distributions of attributes generated from several raw signature data sequences and their combinations. Benefits of the proposed method are as follows.

1. The feature set can be computed efficiently, i.e. in linear time proportional to the length of an online signature.
2. The features stored in the system for verification are irreversible. In other words, the original dynamic construction of an online signature is not revealed even when the features are revealed. This is a desirable property from a biometric privacy point of view.
3. Verification performance of the proposed system is superior to several state of the art algorithms on common data sets.
4. There is no large and extensive training set required by the system to train global model parameters. A classifier is derived using only a set of enrolled samples from a specific user. Therefore the verification performance does not depend on the representativeness of the training set which may differ between sensors, native languages of users, and population distributions of training subjects.

5. Features employed in the system are derived from global statistical characteristics of a signature and hence are more robust to fluctuation in local extreme points. This results in competitive verification accuracy even when a small number of samples from a specific user are used to enroll.

The rest of the paper is organized as follows. Section 2 presents a process of deriving a set of histograms from a given online signature, gives details of the proposed online signature verification system, and analyzes its complexity. Experimental results are given in section 3. Section 4 provides conclusions and discussion on future work.

2 The Proposed Online Signature Verification System

This section presents a histogram feature based online signature verification system that comprises of a feature extractor, a template generator and matcher. First, the input online signature is processed by the feature extractor module to extract a set of histograms from which a feature vector is computed. Then, the system constructs a user-specific template from the feature sets derived from multiple enrollment signatures. This template is later used by the matching process to compare against a query signature to verify whether it has been input by the genuine user. The details of each of these components are described in this section.

2.1 Histogram Features

This subsection describes how a set of histograms are computed from an online signature. These histograms are designed to capture essential information of an online signature attributes as well as the relationships between these attributes. Hence they can be used as a succinct representation of an online signature.

Histograms are widely used as feature sets to capture attribute value distribution statistics in many recognition tasks, for instance, in object recognition and off-line signature verification [QLT07]. Using histograms for online signature verification was first suggested by Nelson et al [NTH94]. They have also been used as part of the feature set in [FJS11, FANLP$^+$05]. However, in [FJS11, FANLP$^+$05], they limit the use of histograms only to the angles derived from data points of an online signature. In fact, much more information can be used to construct histograms as a discriminative feature set. These include x-y trajectories, and the corresponding angles, pressure, speed, as well as their derivatives. This paper shows that, when such information is included, the verification performance of the system is significantly improved and it outperforms many of the other state of the art techniques while retaining the inherent simplicity in a histogram based approach.

The feature extraction process of the proposed method begins by decomposing time-series data of a signature to a sequence of cartesian vectors and other attributes as well as deriving their derivatives. Then, each cartesian vector is also converted to a vector in polar coordinate system. Finally, histograms from these vector sequences are derived. Details of the feature extraction process are given below.

Let $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_n\}$, and $P = \{p_1, p_2, \ldots, p_n\}$ be the sequences of position in x-axis and y-axis, and pressure, respectively, of an original online signature time-series with length n sampled at times $T = \{t_1, t_2, \ldots, t_n\}$. For the rest of this paper, it is assumed that the time interval between these samples is constant, and hence the time information is implicit and is ignored. It should be noted that if the time interval is not a constant, a normalization process using information from T can be applied to the sequences X, Y, and P prior to being processed by the system. We leave this investigation for future work. To construct a set of histogram features, first the descriptive feature vectors X^k, Y^k and

P^k are computed as follows:

$$X^1 = \{x_i^1 | x_i^1 = x_{i+1} - x_i\}, \tag{1a}$$
$$Y^1 = \{u_i^1 | y_i^1 = y_{i+1} - y_i\}, \tag{1b}$$
$$P^1 = \{p_i\} \quad \text{, where } i = 1, 2, ..., n-1 \tag{1c}$$

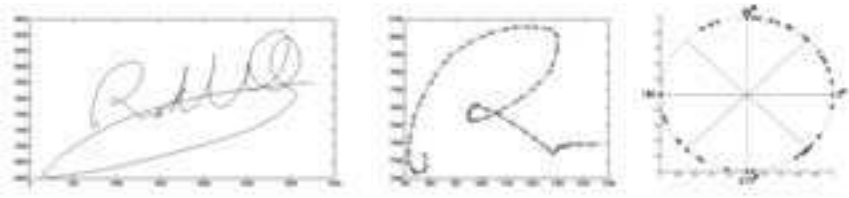
$$\text{and } X^k = \{x_i^k | x_i^k = x_{i+1}^{k-1} - x_i^{k-1}\}, \tag{2a}$$
$$Y^k = \{y_i^k | y_i^k = y_{i+1}^{k-1} - y_i^{k-1}\}, \tag{2b}$$
$$P^k = \{p_i^k | p_i^k = p_{i+1}^{k-1} - p_i^{k-1}\}, \text{ where } k > 1 \text{ and } i = 1, 2, ..., n-k \tag{2c}$$

Noting that, by computing a sequence of differences between each pair of successive points as X^1 and Y^1, the above features serve to eliminate the effect of the first drawing position of a signature (in principle, the system should always accept the signature from the same and honest user regardless of its beginning position.) And by repeating this process of taking differences, X^k and Y^k yields the k^{th} order derivative of the original X and Y sequences respectively.

Then, a sequence of vectors $V = \{v_i^*\}$, is constructed where each of the vector element, $v_i^* = [v_i^1, \ldots, v_i^j]$ is the concatenation of v_i^k which is a five-tuple consisting of the k^{th} order derivative of the cartesian and polar coordinates and pressure attributes as follows:

$$v_i^k = \langle x_i^k, y_i^k, r_i^k, \theta_i^k, p_i^k \rangle \tag{3}$$

$$where \ \theta_i^k = tan^{-1}\left(\frac{y_i^k}{x_i^k}\right)$$
$$r_i^k = \sqrt{\left(x_i^k\right)^2 + \left(y_i^k\right)^2}$$
$$i = 1, 2, ..., n-k$$



(a) Signature (b) Vectorization (c) θ distribution

Figure 1: Illustration of a sample signature a) An original signature b) the sequences of the vector derived from the first 60 points of the signature and c) the distribution of θ derived from the vectors in b)

A set of histograms from the feature vectors above is then computed from their attribute value distribution (figure 1 illustrates the process of deriving θ distribution.) The details of these uniform width histograms are given in Table 1. Specifically, they consist of two types of histograms:

1. One dimensional histograms – these capture the distribution of a single attribute. For example, the histogram Φ^1 captures the angle distribution of an online signature since this can be used to broadly reflects the similarity between two signature shapes. Similarly, Φ^2 is used to capture the

distribution of the angles of the first derivative since it provides more information about how these vectors are aligned, an aspect that is completely ignored in the histogram Φ^1. R^1 is used to capture the speed distribution of an online signature which is one of the distinctive features that is unique among users and is especially useful in combating skilled forgeries.

2. Two dimensional histograms – these capture the distribution of relationship between pairs of attributes, for example, $< \Phi^1, R^1 >_{(1)}$ and $< \Phi^1, R^1 >_{(2)}$ capture the distribution of the dependence between speed and angle of the first and the second halves of an online signature. $< \Phi^1, \Phi^1_{d(1,2)} >$ are used to capture the distribution of the relationship between three consecutive angles of an online signature sequence as well as to provide warping flexibility when comparing two different signatures from the same user.

Table 1: Descriptions of histograms that are used in the proposed technique

Histogram	Input Attributes	Min	Max	Number of bins	Output Attributes
Φ^1	$\{\theta^1_1, \ldots, \theta^1_n\}$	$-\pi$	π	24	Relative frequency
Φ^2	$\{\theta^2_1, \ldots, \theta^2_n\}$	$-\pi$	π	24	Relative frequency
$< \Phi^1, \Phi^1_{d(1,2)} >$	$\{\theta^1_1, \ldots, \theta^1_{n-1}, \theta^1_1, \ldots, \theta^1_{n-2}\}$,	$-\pi$	π	8	Actual frequency
	$\{\theta^1_2, \ldots, \theta^1_n, \theta^1_3, \ldots, \theta^1_n\}$	$-\pi$	π	8	
R^1	$\{r^1_1, \ldots, r^1_n\}$	0	$\mu + 3\sigma$	16	Actual frequency
R^2	$\{r^2_1, \ldots, r^2_n\}$	0	$\mu + 3\sigma$	16	Actual frequency
X^1	$\{x^1_1, \ldots, x^1_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	8	Relative frequency
Y^1	$\{y^1_1, \ldots, y^1_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	8	Relative frequency
X^2	$\{x^2_1, \ldots, x^2_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	8	Relative frequency
Y^2	$\{y^2_1, \ldots, y^2_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	8	Relative frequency
$< X^1, X^2 >$	$\{x^1_1, \ldots, x^1_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	6	Relative frequency
	$\{x^2_1, \ldots, x^2_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	4	
$< Y^1, Y^2 >$	$\{y^1_1, \ldots, y^1_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	6	Relative frequency
	$\{y^2_1, \ldots, y^2_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	4	
$< \Phi^1, R^1 >_{(1)}$	$\{\theta^1_1, \ldots, \theta^1_{\lfloor n/2 \rfloor}\}$,	$-\pi$	π	8	Relative frequency
	$\{r^1_1, \ldots, r^1_{\lfloor n/2 \rfloor}\}$	0	$\mu + 3\sigma$	4	
$< \Phi^1, R^1 >_{(2)}$	$\{\theta^1_{\lfloor n/2 \rfloor}, \ldots, \theta^1_n\}$,	$-\pi$	π	8	Relative frequency
	$\{r^1_{\lfloor n/2 \rfloor}, \ldots, r^1_n\}$	0	$\mu + 3\sigma$	4	
$< \Phi^2, R^2 >_{(1)}$	$\{\theta^2_1, \ldots, \theta^2_{\lfloor n/2 \rfloor}\}$,	$-\pi$	π	8	Relative frequency
	$\{r^2_1, \ldots, r^2_{\lfloor n/2 \rfloor}\}$	0	$\mu + 3\sigma$	4	
$< \Phi^2, R^2 >_{(2)}$	$\{\theta^2_{\lfloor n/2 \rfloor}, \ldots, \theta^2_n\}$,	$-\pi$	π	8	Relative frequency
	$\{r^2_{\lfloor n/2 \rfloor}, \ldots, r^2_n\}$	0	$\mu + 3\sigma$	4	
$< \Phi^1, R^2 >_{(1)}$	$\{\theta^1_1, \ldots, \theta^1_{\lfloor n/2 \rfloor}\}$,	$-\pi$	π	8	Relative frequency
	$\{r^2_1, \ldots, r^2_{\lfloor n/2 \rfloor}\}$	0	$\mu + 3\sigma$	4	
$< \Phi^1, R^2 >_{(2)}$	$\{\theta^1_{\lfloor n/2 \rfloor}, \ldots, \theta^1_n\}$,	$-\pi$	π	8	Relative frequency
	$\{r^2_{\lfloor n/2 \rfloor}, \ldots, r^2_n\}$	0	$\mu + 3\sigma$	4	
$P^1_{(1)}$	$\{p^1_1, \ldots, p^1_{\lfloor n/2 \rfloor}\}$	0	$\mu + 3\sigma$	8	Actual frequency
$P^1_{(2)}$	$\{p^1_{\lfloor n/2 \rfloor}, \ldots, p^1_n\}$	0	$\mu + 3\sigma$	8	Actual frequency
$P^2_{(1)}$	$\{p^2_1, \ldots, p^2_{\lfloor n/2 \rfloor}\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	8	Relative frequency
$P^2_{(2)}$	$\{p^2_{\lfloor n/2 \rfloor}, \ldots, p^2_n\}$	$\mu - 3\sigma$	$\mu + 3\sigma$	8	Relative frequency

The histograms above are computed by splitting the range of the feature (specified by Min and Max columns in Table 1), into a number of equal width bin intervals (also given in Table 1), and counting the number of elements that fall into each particular bin. For an angle attribute and its derivative, the range of its histogram is defined as $[-\pi, \pi]$. For an input attribute which has no explicit boundary, an outlier process with cutoff at three standard deviations from its mean is applied prior to computing the mean and standard deviation of the attribute in order to derive its implicit range described in Table 1. For example, histogram Φ^1 is derived from a sequence $\{\theta^i_1; i = 1, ..., n\}$ by forming a 24 bin histogram with equal

width bin intervals beginning from $-\pi$ to π and counting the number of elements, $\{\theta_i^1\}$, that fall into each of the 24 bins. It then results in a vector of 24 bin frequencies.

It should be noted that histogram's frequencies are divided into two types: absolute frequency – the actual count of elements that fall into a particular bin, and relative frequency – frequencies that are normalized by the total number of elements in the histogram which is essentially the factor of a signature's length, n. Using absolute frequency results in more implicit importance given to the length of the signature whereas using relative frequency ignore the length of the signature. In this paper, we choose to use relative frequency counts more often than absolute frequency counts. Out of the 21 histograms listed in Table 1, only 5 are absolute frequencies. These are the speed and its first derivative histograms, the pressure histograms of the first and second half of a signature, and the $< \Phi^1, \Phi^1_{d(1,2)} >$ histogram as they are derived from the lowest order derivative of considered sequences, which are the most consistent ones in our empirical experiment. In future work, the effect of this choice will be investigated in more detail.

Once, all the histogram vectors are computed, they are concatenated and used as an online signature's feature vector as follows. Let B_i be a vector of bin frequencies of i^{th} histogram. An online signature's feature vector F is defined as $F = \{B_1 \| B_2 \| ... \| B_j\}$, where j is the total number of histograms, and $\|$ is the concatenation operator. Once the feature vector F is constructed, each of the elements is used independently as a feature component of an online signature. So for the rest of the paper we treat F as a feature vector and do not distinguish which histogram each feature belongs to. Hence we say we have a feature vector $F = \{f_i; i = 1, ..., M\}$ where M is the total number of histogram bins from all j histograms.

2.2 User Template Formation and Verification

This subsection describes the proposed verification system. Generally, an online signature verification system comprises of two stages:

1. Enrollment stage – where a user enrolls in the system by giving multiple online signatures which will later be used to verify a user,
2. Verification stage – where a user claims an identity by inputting a signature on the system's sensor and the system accepts the signature if the distance between the enrolled template corresponding to that identity and the newly input one is less than a pre-defined threshold.

In the proposed system, an online signature is represented by the set of features derived by the feature extraction module described in the previous sub-section. During the enrollment process, multiple signatures are acquired from a user and features are computed for each sample. The set of feature vectors are then used to identify feature variations of each feature component for the specific user. A user-specific uniform quantizer is constructed for each feature component and the resulting user specific vector of quantization step sizes, Q^u, which we call that quantization step size vector is created. Q^u helps recover a reliable quantized feature vector from noisy biometric data during the verification process. Each feature vector from the enrollment samples is then quantized according to Q^u and a feature vector template $\dot{F}^u$ for the user is obtained by averaging the quantized feature vectors.

In the verification stage, the claimed user is asked to produce a single signature which is again represented by the set of features derived by the feature extraction module. The system then derives a signature's quantized feature vector from a given signature using the stored feature quantization step size vector and compares it against the stored user-specific quantized feature vector template. The signature is accepted if the Manhattan distance between these two quantized vectors is less than a predefined threshold, otherwise it is rejected. A summary of the system is shown in Figure 2. The details on how to derive the quantization step size vector Q^u and the template feature vector are given below.

Let S be the total number of enrolled samples, and let $F^s = \{f_i^s | i = 1, .., M\}$ be the feature vector of the enrolled sample s of the user u where $1 \leq s \leq S$, and M is the total number of online signature features.

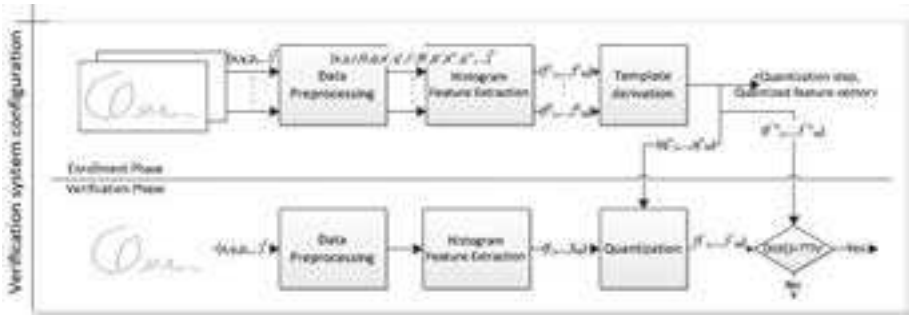


Figure 2: The proposed verification system

The quantization step size vector of the user u, $Q^u = \{q_i^u | i = 1, .., M\}$, is obtained by computing the standard deviations over all the enrolled samples for each feature and using a multiple of this as the quantization step size. That is,

$$q_i^u = \beta \sqrt{\frac{1}{S} \sum_{s=1}^{S} \left(f_i^s - \mu_{f_i^{(u)}} \right)^2}, i = 1, \ldots, M \tag{4}$$

where $\mu_{f_i^{(u)}} = \frac{1}{S} \sum_{s=1}^{S} f_i^s$, β is experimentally fixed at 1.5. Then, a quantized feature vector, $\hat{F}^{(s|u)} = \{\hat{f}_i^s | i = 1, .., M\}$ is derived from each sample s using the quantization step sizes q_i^u in Q^u (adding a small ϵ to prevent division by zero) as follows:

$$\hat{f}_i^{(s|u)} = \left\lfloor \frac{f_i^s}{q_i^u + \epsilon} \right\rfloor , i = 1, \ldots, M \tag{5}$$

where ϵ is at 0.002 and 0.8 for histograms with absolute and relative frequencies, respectively. Lastly, the user-specific feature vector template, $\ddot{F}^u = \{\ddot{f}_i^u | i = 1, .., M\}$, is derived by averaging the quantized feature vectors of all the enrolled online signature samples from the user u.

$$\ddot{f}_i^u = \left\lfloor \frac{\sum_{s=1}^{S} \hat{f}_i^{(s|u)}}{S} \right\rfloor , i = 1, \ldots, M \tag{6}$$

A pair $\left(Q^u, \ddot{F}^u\right)$ comprising of the quantization step size vector and its associated feature vector template is then stored as the user u's template and used to verify a claimed signature of the user u.

During the verification, given that t is claimed to be a sample from user u, $\hat{F}^{(t|u)}$ is calculated using Q^u. Then the system derives a dissimilarity score using manhattan distance between $\ddot{F}^u$ and $\hat{F}^{(t|u)}$ as,

$$Score = \sum_{i=1}^{M} |\hat{f}_i^{(t|u)} - \ddot{f}_i^u| \tag{7}$$

The system then accepts the sample t if the dissimilarity score is less than a predefined threshold, otherwise it rejects.

2.3 Complexity

Given n as the length of an online signature's sequence, X^k, Y^k, R^k, Φ^k, and P^k can be computed in time $O(n)$. Then, they are used to derive h histograms which yields $O(h * n)$ or $O(n)$ time complexity in deriving a feature vector as h is a constant. For the classification process, a feature vector is first quantized and then used to construct or to compare against the feature vector template. Since the number of features is a constant, the time complexity is $O(1)$. The space required to store a template is clearly a constant as it consists of two fixed-length vectors. As a result, the proposed method requires constant space to store a user's template and achieves linear time complexity for enrolling and verifying a signature.

3 Experiments

In this section we provide experimental results for the proposed technique and compare its performance to others published in the literature.

Experiments were performed with the well known MCYT dataset [OGFAS$^+$03], which consists of signatures from 100 individuals with 25 genuine samples and 25 skilled forgery samples, and the SUSIG dataset [KY08], which consists of signatures from 94 individuals with 20 genuine samples from two separate sessions and 10 skilled forgery samples. Additional details of these two datasets can be found in [OGFAS$^+$03, KY08].

In terms of training samples, there have been two approaches taken in the literature. Some papers [GP09, YK09] randomly select k samples as the training set and then they average over multiple such random selections to arrive at the final performance result. The reasoning is that such a strategy better captures within-user variation. Other papers [MCN09, ARMACC12, KY08, OGFAS$^+$03, MMDC$^+$08, MCN09] choose the first k samples, according to the original order in which the data was acquired, as the training set. For online signature verification most papers have chosen this second approach to perform experiments since it provides a more realistic result in the sense of mimicking what an application will actually do. In any application, at first enrollment samples will be acquired which would then be repeatedly used to test against query samples. The results from such an approach also captures the timing effect [YK09, FOGRGR07], which is, in fact, one of the major causes for degradation of verification performance called the template aging problem [FOGRGR07, YK09, URJ04] which a system designer often needs to take into consideration.

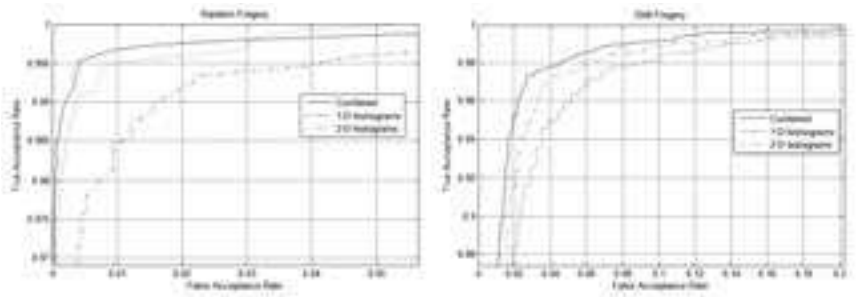
In our experiments, the first k samples of the set from a specific user were used to enroll a template, and the rest were used to evaluate the False Rejection Rate (FRR) at different threshold levels. In the random forgery scenario or zero knowledge attack, i.e., an attacker simply attacks the system using his own signature, all samples from all other individuals were used to evaluate the False Acceptance Rate, namely FAR-RF. On the other hand, for the skilled forgery scenario, 25 skilled forgery samples from MCYT dataset and 10 skilled forgery samples from SUSIG dataset for each user were used to evaluate the False Acceptance Rate, namely FAR-SF. The Equal Error Rate (EER), the rate at which FAR and FRR are equal, was also used to compare the verification performance of different approaches.

Noting that, in this work, first and second derivative sequences of vectors $v^* = [v_i^1, v_i^2]$, as described in Section 2.1, were derived from an online signature. Then a set of 448 features, which consisted of the histograms described in Table 1 were extracted.

3.1 Effectiveness of 1-D versus 2-D histogram features through verification performance

As mentioned in the previous section, the proposed histogram features are derived from two types of histograms namely, one dimensional histograms and two dimensional histograms. These histograms capture the distributions of a single attribute and relationship between pairs of attributes, respectively. The former is commonly used in many feature based systems [NTH94, FANLP$^+$05, Nan06] whereas the latter one, to the best of our knowledge, has never been explored in the research literature. In this subsection, we investigate the effectiveness of using these two types of histograms by evaluating their verification performance against both skilled and random forgery. The plot of the receiver operator characteristic (ROC) curve obtained from MCYT-100 dataset when each of these histograms is used as well as when they are combined, using 10 enrollment samples, is depicted in Figure 3.

The results show that 2-D histograms are indeed a more effective feature set in terms of discrimination power against both skilled and random forgeries compared to 1-D histograms provided that they are employed with larger bin widths. They also appear to work well with less information since pressure information was not included in the 2-D histograms we computed. The results also demonstrate that 1-D histogram features provide complementary information since the best result is observed when the two sets are combined.



(a) ROC of random forgery (b) ROC of skill forgery

Figure 3: ROC of skill and random forgery obtained from MCYT-100 dataset when 1-D histogram, 2-D histogram, and both sets are applied

3.2 Verification performance of the proposed system

The performance of the proposed verification system for different number of training samples per user derived from MCYT-100 dataset is reported in Table 2. The results demonstrate that the proposed system can effectively verify a user's online signature even if only three signatures are supplied by a user during enrollment. However, verification performance at every operating point slightly improves as the number of training samples grows. Using the same dataset, the plot of receiver operator characteristic (ROC) when 5 and 10 training samples are supplied are shown in Figure 4. In Figure 5, we show the the distributions of dissimilarity scores for a pool of 1,500 genuine samples, 2,500 skilled forgery samples and 247,500 random forgery samples drawn from MCYT-100 dataset when 10 training samples were provided.

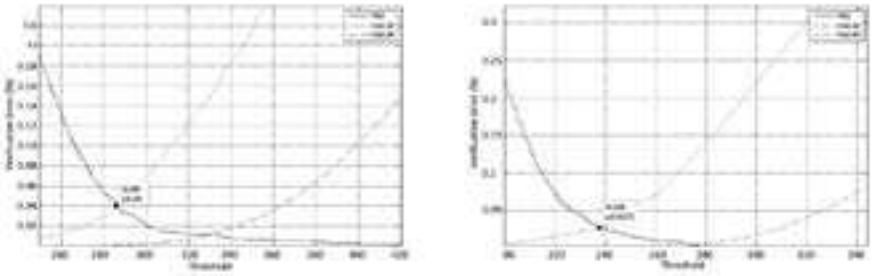
Table 2: EER of the proposed system derived from MCYT-100 dataset when different number of samples are used for training

Number of Training Samples	EER-SF	EER-RF
3	5.74	1.43
5	4.02	1.15
7	3.43	0.87
10	2.72	0.44
20	2.72	0.35

3.3 Comparison with previous work

The online signature verification systems that have been proposed in the literature can be broadly classified into two types based on the signature input that is presented to a matcher: feature based and function based. The first type of systems is generally more preferable due to the computation and space complexity requirement of the system. However, it is claimed that the latter one usually yields better verification performance [FOGRGR07]. In this subsection, a comparison of performance between the systems that are considered as the state of the art for these two approaches and the proposed approach, which is considered as the feature based system, is provided. Results reported on the proposed system as well as the other system are on the same dataset. The function based approach considered here includes Dynamic Time Warping technique (DTW), Hidden Markov Model (HMM), and their template protection approach. The feature based approach compared includes one utilizing Fourier descriptor features, and a 100-feature system in conjunction with three different classifiers.

Table 3 lists the verification performance of these different techniques on MCYT-100 dataset. As seen from the table, the proposed system outperforms other systems especially when a few training samples are supplied. These results emphasize the competitiveness of the proposed system considering that it is a



(a) 5 samples per user

(b) 10 samples per user

Figure 4: Verification rates derived from MCYT-100 dataset when different number of signatures per user are enrolled

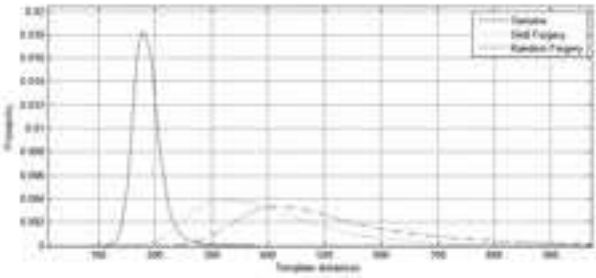


Figure 5: Dissimilarity score distribution of genuine, skill forgery, and random forgery samples, derived from MCYT-100 dataset where 10 samples are used to enroll a user template

computational and space efficient method as compared to the other proposals.

Table 4 reports verification performance for the previous techniques listed above on the SUSIG dataset. As mentioned in [YK09, KY08], they chose to more heavily weigh the signing duration feature as they observed that a skilled forgery signature typically takes twice as long as a genuine one on the average. Hence their FAR-SF is lower than FAR-RF. However, as reported in [YK09, KY08], the EER for the skilled forgery case in this dataset is greatly induced by the significance that a classifier gives to the length disparity between two given signatures. On the other hand, in the proposed system, less weight is given to this length disparity since most of histogram features in the proposed set are attributed by their relative frequency in which the actual length of the signature is ignored. Only 112 histogram features or 25% in the set are attributed by absolute frequency, where the actual length of the signature gets reflected in the feature values. This results in lower FAR-RF but higher FAR-SF than the system in [YK09,KY08]. However, when more weight is given to the histograms with frequency attributes, the EER of skill forgery is reduced from 5.86 to 4.59 whereas that of random forgery remains unchanged. This implies that the verification performance could potentially improve if there are more type of histograms created using absolute frequency and not relative frequency. It also demonstrates that the forger's skill of these two datasets are very different. However, we acknowledge that reported verification rate is not always the best justification for a system's effectiveness, since each system might have been trained and tested differently as well as the difference in employing skilled forgery model. In addition, the system might apply different set of features to employ their classifiers. Nevertheless, the results show that the proposed system, at the very least, comparable to others in terms of the verification performance.

Table 3: EER of different verification approaches on MCYT-100 dataset

Matching Types	Approaches	$n = 5$		$n = 10$		Remarks
		EER-SF	EER-RF	EER-SF	EER-RF	
Function-based	DTW [MCN09]	5.53	-	3.93	-	
	DTW [KY05]	9.81	-	-	-	
	DTW-Protected [MCN09]	8.13	-	5.22	-	
	HMM [MMDC+08]	10.29	-	6.33	-	
	HMM-Protected [MMDC+08]	13.30	-	7.95	-	
Feature-based	Fourier Descriptors in [YK09]	14.53	-	-	-	5 training are randomly selected.
	100 global features in [FANLP+05]	6.89	2.2	-	-	
	100 global features in [Nan06]	7.1	1.6	-	-	
	100 global features in [GP09]	6.12	2.05	-	-	5 training are randomly selected.
	UBM-HMM [ARMACC12]	-	-	2.785	-	UBM are trained from 2500 genuine and skill forgery signatures of 50 users. PCA model are trained from 1000 genuie signatures of 100 users.
	The proposed method	**4.02**	**1.15**	**2.72**	0.44	

Table 4: EER of different verification approaches on SUSIG dataset

Matching Types	Approaches	$n = 5$		$n = 10$		Remarks
		EER-SF	EER-RF	EER-SF	EER-RF	
Function-based	DTW [KY05, YK09, KY08]	**3.30**	4.08	-	-	
Feature-based	Fourier Descriptors in [YK09]	6.20	-	-	-	
	The proposed method	6.08	**2.94**	-	-	
	The proposed method*	4.37	**2.91**	-	-	* when the weight of R and $\Phi - \Phi^{d(1,2)}$ histogram attributes is given 3 times of others

4 Conclusion and Future Work

This paper proposes a simple and effective online signature verification system. First, a histogram based feature set that can be efficiently computed is introduced. Second, a model-free Manhattan distance classifier based on a quantized feature vector is used to verify an online signature sample. This implies that a user-specific classifier can be trained using only a few enrollment samples without requiring a training set with a large number of samples. Therefore the technique is suitable for employment in a mobile device application where sensors may differ from one device to another. More importantly, since the feature set employed in the proposed system represents only statistics derived from the original sequence, the transformation is non-invertible where the privacy of the original biometric data is protected. Testing with MCYT dataset, the proposed system achieves competitive performance when compared to other proposed systems.

The limitations of the current work are as follows. First, it is currently possible to match different signature templates generated from the same online signature samples and thereby learn that two leaked biometric templates belong to the same user. Work needs to be done on how one can inject some randomness in the original template generation process so that different templates can be generated from the same set of signatures without compromising system performance. In addition, we plan to further investigate the use of other biometric key binding approaches like fuzzy commitment that could be applied on the proposed feature set in order to strengthen security of the system. Secondly, it is also important to evaluate performance on the dataset that collected in mobile authentication context, i.e., users may sit or stand while signing on the current handset devices that may have non-uniform sampling rate. Then the proposed algorithm can be modified accordingly.

Acknowledgments

The authors were supported by NSF grant 1228842. We also would like to thank the anonymous reviewers for their comments and feedbacks towards this work.

References

[ARMACC12] E. Argones Rua, E. Maiorana, J.L. Alba Castro, and P. Campisi. Biometric Template Protection Using Universal Background Models: An Application to Online Signature. *Information Forensics and Security, IEEE Transactions on*, 7(1):269 –282, feb. 2012.

[CZC] Yao-Jen Chang, Wende Zhang, and Tsuhan Chen. Biometrics-based cryptographic key generation. In *Multimedia and Expo, 2004. ICME '04. 2004 IEEE Int' Conf. on*, pages 2203 – 2206 Vol.3, june.

[FANLP+05] Julian Fierrez-Aguilar, Loris Nanni, Jaime Lopez-Peñalba, Javier Ortega-Garcia, and Davide Maltoni. An On-Line Signature Verification System Based on Fusion of Local and Global Information. In *Audio- and Video-Based Biometric Person Authentication*, volume 3546 of *Lecture Notes in Computer Science*, pages 627–656. Springer Berlin / Heidelberg, 2005.

[FJS11] Asghar Fallah, Mahdi Jamaati, and Ali Soleamani. A new online signature verification system based on combining Mellin transform, MFCC and neural network. *DSP*, 21(2):404 – 416, 2011.

[FOGRGR07] Julian Fierrez, Javier Ortega-Garcia, Daniel Ramos, and Joaquin Gonzalez-Rodriguez. HMM-based on-line signature verification: Feature extraction and signature modeling. *Pattern Recogn. Lett.*, 28:2325–2334, December 2007.

[FW03] Hao Feng and Chan Choong Wah. Online signature verification using a new extreme points warping technique. *Pattern Recognition Letters*, 24(16):2943 – 2951, 2003.

[FWW11] Leah Findlater, Jacob O. Wobbrock, and Daniel Wigdor. Typing on flat glass: examining ten-finger expert typing patterns on touch surfaces. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, CHI '11, pages 2453–2462, New York, NY, USA, 2011. ACM.

[FZ07] Marcos Faundez-Zanuy. On-line signature recognition based on VQ-DTW. *Pattern Recognition*, 40(3):981 – 992, 2007.

[GP09] D.S. Guru and H.N. Prakash. Online Signature Verification and Recognition: An Approach Based on Symbolic Representation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 31(6):1059 –1073, june 2009.

[KY05] Alisher Kholmatov and Berrin Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recogn. Lett.*, 26:2400–2408, November 2005.

[KY08] A. Kholmatov and B. Yanikoglu. SUSIG: an on-line signature database, associated protocols and benchmark results. *Pattern Analysis & Applications*, 2008.

[LTT12] Meng-Hui Lim, Andrew Beng Jin Teoh, and Kar-Ann Toh. An efficient dynamic reliability-dependent bit allocation for biometric discretization. *Pattern Recognition*, 45(5):1960 – 1971, 2012.

[MCN09] E. Maiorana, P. Campisi, and A. Neri. Template protection for Dynamic Time Warping based biometric signature authentication. In *Digital Signal Processing, 2009 16th International Conference on*, pages 1 –6, july 2009.

[MMDC+08] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri. Template protection for HMM-based on-line signature authentication. *CVPR Workshop*, 0:1–6, 2008.

[Nan06] Loris Nanni. An advanced multi-matcher method for on-line signature verification featuring global features and tokenised random numbers. *Neurocomputing*, 69(1618):2402 – 2406, 2006.

[NMLC10] Loris Nanni, Emanuele Maiorana, Alessandra Lumini, and Patrizio Campisi. Combining local, regional and global matchers for a template protected on-line signature verification system. *Expert Syst. Appl.*, 37:3676–3684, May 2010.

[NTH94] Winston Nelson, William Turin, and Trevor Hastie. Statistical Methods for On-Line Signature Verification. *Proceedings of IJPRAI*, pages 749–770, 1994.

[OGFAS+03] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro. MCYT baseline corpus: a bimodal biometric database. *Vision, Image and Signal Processing, IEE Proceedings* -, 150(6):395 – 401, dec. 2003.

[Pla89] Lorette G. Plamondon, R. Automatic signature verification and writer identification - the state of the art. *Pattern Recognition*, 22(2):107–131, 1989. cited By (since 1996) 342.

[QLT07] Yu Qiao, Jianzhuang Liu, and Xiaoou Tang. Offline Signature Verification Using Online Handwriting Registration. In *CVPR '07. IEEE Conference on*, pages 1 –8, june 2007.

[SBAIM12] Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister, and Nasir Memon. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In *CHI '12*, pages 977–986, New York, NY, USA, 2012. ACM.

[URJ04] Umut Uludag, Arun Ross, and Anil Jain. Biometric template selection and update: a case study in fingerprints. *Pattern Recognition*, 37(7):1533 – 1542, 2004.

[YK09] Berrin Yanikoglu and Alisher Kholmatov. Online Signature Verification Using Fourier Descriptors. *EURASIP Journal on Advances in Signal Processing*, 2009.