# Quickest Multiple User Active Authentication


**Pramuditha Perera, Julian Fierrez, and Vishal M. Patel**

**Abstract** In this chapter, we investigate how to detect intruders with low latency for Active Authentication (AA) systems with multiple-users. We extend The Quickest Change Detection (QCD) framework is extended to the multiple-user case and the Multiple-user Quickest Intruder Detection (MQID) algorithm is formulated. Furthermore, the algorithm is extended to the data-efficient scenario where intruder detection is carried out with fewer observation samples. The effectiveness of the method is evaluated on two publicly available AA datasets on the face modality.

## 1 Introduction

Balancing the trade-offs between security and usability is one of the major challenges in mobile security [4]. Longer passwords with a combination of digits, letters and special characters are known to be secure but they lack usability in the mobile applications. On the other hand, swipe patterns, face verification and fingerprint verification have emerged as popular mobile authentication methods owing to the ease of use they provide. However, security of these methods are challenged due to different types of attack mechanisms employed by intruders ranging from simple shoulder attacks to specifically engineered spoof attacks. In this context, Active Authentication (AA), where the mobile device user is continuously

P. Perera
Department of Electrical and Computer Engineering, Johns Hopkins University, Baltimore, MD, USA
e-mail: pperera3@jhu.edu

J. Fierrez
School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: julian.fierrez@uam.es

V. M. Patel (✉)
Department of Electrical Engineering, Johns Hopkins University, Baltimore, MD, USA
e-mail: vpatel36@jhu.edu



T. Bourlai et al. (eds.), *Securing Social Identity in Mobile Platforms*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-39489-9_10

monitored and user's identity is continuously verified, has emerged as a promising solution [5, 20, 23].

Authors in [28] identified three characteristics that are vital to a practical AA system; accuracy, latency and efficiency. However, for AA to be deployed in the real-world, it needs to be equipped with another functionality – transferability. Mobile devices are not private devices that people use in isolation. In practice, it is common for mobile devices to be used interchangeably among several individuals. For example, these individuals could be the members of a family or a set of professionals operating in a team (such as physicians in a hospital). Therefore, it is important that the AA systems facilitate smooth transition between multiple enrolled individuals [26].

The presence of multiple enrolled subjects poses additional challenges to an AA system. Detecting intrusions with low latency in this scenario is even more challenging. With this new formulation, the device cannot simply declare an intrusion when there is a change in the device usage pattern. This is because two legitimate users operating on the phone could potentially have different behavior patterns. As a result, the systems is not only expected to identify intrusions, but also to provide smooth functioning when there is a transfer of legitimate users. For example, consider the scenario shown in Fig. 1. There are two legitimate users of the device in this scenario. The first user operates the mobile device between frames (a) and (c). At frame (d), the device is handed over to a second legitimate user. At this point, although there is a change in pattern in device usage, the AA system should not declare an intrusion. On the other hand, when an intruder starts using the device at frame (h), the device is expected to declare an intrusion.

In this chapter, we extend the work proposed in [28] and study the effectiveness of Quickest Change Detection (QCD) algorithm for multiple-user AA. Specifically, we study possible strategies that can be used to extend Mini-max QCD in AA to the case where multiple users are enrolled in the device. Furthermore, we study the effectiveness of data-efficient sampling for this case. In the experimental results section, we show that the QCD algorithm and it's data-efficient extension are effective even in the case of multiple-user AA.

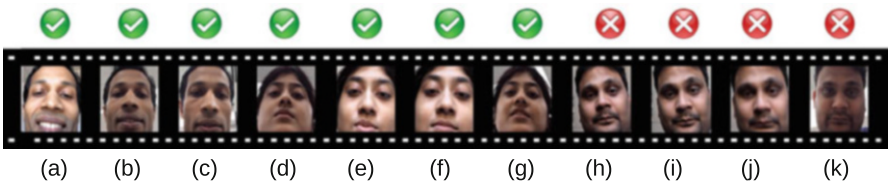



**Fig. 1** Problem of quickest detection of intruders in multiple-user active authentication. In this example, there are two users enrolled in the mobile device. First user uses the device between frames (**a**) to (**c**). At frame (**d**), another legitimate user starts using the device. The second user uses the device between frames (**d**) to (**g**). At frame (**h**), an intruder starts using the device (In this work we assume that intruders do not attempt to hide their identity using a spoofing method). The goal of quickest intrusion detection is to detect the change with the lowest possible latency. However, intruder detector should not declare a false detection prior to frame (**h**)

## 2 Related Work

Initial works of AA predominantly focused on introducing new biometric modalities or increasing the performance of well-known modalities. Gait [15, 34], keystroke [9, 13], voice, swipe patterns [11, 30] and face images [6, 8, 17, 19, 21] are some of the commonly used modalities in mobile AA. In addition, micro movements of the user's touch gestures [3] and behavioral profiling based on stylometry, GPS location and web browsing patterns [12] have also been used for AA in the literature.

More recent works in AA focused on obtaining better authentication performance either by improving the performance in each individual modality or by fusing two or more biometric modalities. In [14], adaboost classifier and LBP features are used for face detection and face authentication in mobile devices. In [29], a facial attribute-based continuous face authentication was proposed for AA. A domain adaptive sparse dictionary-based AA system was proposed in [33], by projecting observations of different domains into a common subspace through an iterative procedure. McCool et al. [19] proposed to fuse face and voice data for obtaining more robust AA. In [6], face modality was fused with gyroscope, accelerometer, and magnetometer modalities for more robust authentication.

However, all of these methods focus on the single user authentication problem. Furthermore, the latency of decision making is not quantified in these works. In [26], the problem of single user AA was extended to the multiple user scenario. The authors proposed an SVM-based solution where the scores of each SVM output are fused using a new fusion rule. In speaker recognition, the need to have multiple user systems have been previously discussed [7, 18]. In [24] multiple user authentication is formulated as a conjunction between a classification task and a verification task. Based on the same principle, the authors of [27] introduced sparse representation-based intruder detection scheme for multiple-user AA. In [25], authors proposed to use the principles of QCD for AA. In [28], this formulation was extended with data-efficient QCD with the aim of producing highly accurate predictions with low latency while obtaining low number of sensor observations. In this work, we extend the algorithms presented in [28] and [25] to the multiple-user case and study it's effectiveness in face-based mobile AA.

## 3 Proposed Method

When a user or multiple users start using a mobile device, typically they are required to register with the device. This process is called enrollment of the user(s) to the mobile device. During enrollment, the device gathers sensor observations of the legitimate users and creates user-specific classifiers. Let $m$ be the number of users enrolled in a given device. Technically, $m$ could be any finite number greater or equal to one. However, in practice, it's not common for a mobile device to be shared between more than 5–7 individuals (i.e. normal family size).

For each user $i$, the device gathers enrollment data $Y_i = \{y_{i,1}, y_{i,2}, \ldots, y_{i,k}\}$. Then, the device develops a set of user specific classifiers $c_i$ for each user which produces a classification score for each user. This classifier can be a simple template matching algorithm or a complex neural network. In our experiments, we consider a template matching algorithm due to the easiness in training the classifier. Our template matching classifier $c_i$ generates a user specific score $s_i = c_i(y) = \min(\cos(y, Y_i))$ for a given input $y$ where $\cos(.)$ is the Cosine angle between the two inputs.[1]

In addition, matched and non-match distributions with respect to the learned classifier are obtained and stored during the enrollment phase. Match distribution $f_{0,i}(.)$ of user $i$ can be obtained by considering pairwise score values of $Y_i$ with respect to $c_i$. On the other hand, a known set of negative samples can be used to obtain the non-matched scores $f_{1,i}(.)$ of user $i$. This process is illustrated in Fig. 2. In this work, we approximate the score distribution of intruders with the non-matched distribution. Therefore, we use the terms matched distribution and pre-change distribution interchangeably. Similarly, in the context of this paper, non-matched distribution and post-change distribution will also mean the same.

As the AA system receives observations $\{x_1, x_2, \ldots, x_n\}$, at time $n$, it produces a decision $d_n = f(C_1(x_1), \ldots, C_n(x_n)) \in \{0, 1\}$ based on the set of classifiers $C = \{c_1, \ldots, c_m\}$ where $f(.)$ is a mapping function. If $d_n = 1$, an intrusion is declared. Given this formulation, the goal of an AA system is to detect intrusions

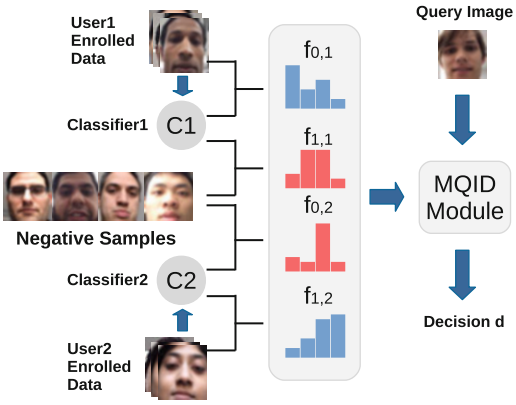



**Fig. 2** Overview of the problem setup for the case of two enrolled users. For each enrolled user, $i$, the enrolled images are obtained during the enrollment phase. These images are used to train a user specific classifier $c_i$. A matched score distribution $f_{0,i}$ and a non-matched distribution $f_{1,i}$ is obtained for each user. A known set of negative users are used to obtain the latter. If more users are present the same structure will be cascaded. During inference, Multi-user Quickest Intruder Detection (MQID) module will produce a decision ($d$) by considering the obtained distributions and past decision scores

[1] Score $s_i$ represents dissimilarity.

with the lowest possible latency when a new observation is received. If an intrusion occurs at time $T$, the following two properties are desired from the AA system.

- **Low detection delay.** The latency between an intrusion occurring and the system detecting the intrusion should be low. If the system detects an intrusion at time $\tau$, detection delay is given by $(\tau - T)^+$ where $[(x)^+]$ denotes the positive part of $x$. For all users, this property is quantified using Average Detection Delay (ADD) defined as $ADD(\tau) = E[(\tau - T)^+]$. Here $T$ denotes the real change point.
- **Low false detections.** In practice, detection delay alone cannot characterize the desired functionality of an AA system. It is also desired that the AA system does not produce false detections prior to the intrusion point. This phenomena can be quantified by considering Probability of False Detections (PFD) as $PFD(\tau) = P[\tau < T]$.

It is desired for an AA system to have low ADD and low PFD.

### *3.1 Quickest Change Detection (QCD)*

Quickest Change Detection is a branch of statistical signal processing that thrives to detect the change point of statistical properties of a random process [1, 2, 31]. The objective of QCD is to produce algorithms that detect the change with a minimal delay (ADD) while adhering to false alarm rate constraints (PFD). Consider a collection of obtained match scores, $s_1, s_2, \cdots, s_n$, from the AA system. Assuming that the individual scores are mutually independent, QCD theory can be used to determine whether a change has occurred before time $n$ or not. In the following subsections we present two main formulations of QCD.

QCD has been studied both in Baysian and a Mini-max frameworks in previous works. In the Baysian setting, it is assumed that the system has prior information about the distribution of intrusions. However, in the case of AA, probability of an intrusion happening cannot be modeled. Therefore, this assumptions does not hold. Therefore, for this work we only consider QCD in a non-Bayesian setting. MiniMax QCD formulation treats the change point $\tau$ as an unknown deterministic quantity [1, 2]. However, as mentioned before, it is assumed that pre-change distribution, $f_0$, and post-change distribution, $f_1$, are known.

Due to the absence of prior knowledge on the change point, a reasonable measure of PFD is the reciprocal of mean time to a false detection as follows

$$PFD(\tau) = \frac{1}{E_\infty[\tau]}.$$

Based on this definition of PFD, Lorden proposed a minimax formulation for QCD [2, 16]. Consider the set of stopping times $D_\alpha$ for a given constraint $\alpha$ such that $D_\alpha = \{\tau : PFD(\tau) \leqslant \alpha\}$. Adhering to this constraint, Lorden's formulation optimizes a cost function to solve the minimax QCD problem. In particular, the cost

function is the supremum of the average delay conditioned on the worst possible realizations as follows

$$WADD(\tau) = \sup_{n \geqslant 1} \operatorname{ess\,sup} E_n[(\tau - n)^+ | S^n].$$

Lorden's formulation tries to minimize the worst possible detection delay subjected to a constraint on PFD [16]. It was shown in [1], that the exact optimal solution for Lorden's formulation of QCD can be obtained using the CumSum algorithm [22].

### 3.1.1 CumSum Algorithm

Define the statistic $W(n)$ such that

$$W(n) = \max_{1 \leqslant k \leqslant n+1} \sum_{i=k}^{n} \log(L(s_i)),$$

and $W_0 = 0$, where $L(s_n) = f_1(s_n)/f_0(s_n)$ is the log likelihood ratio. It can be shown that the statistic $W(n)$ has the following recursive form

$$W_{n+1} = (W_n + \log(L(s_{n+1}))^+).$$

Time at which a change occurred ($\tau$) is chosen such that $\tau_c = \inf\{n \geqslant 1 : W_n \geqslant b\}$, where $b$ is a threshold. More details about the CumSum algorithm can be found in [1, 2, 22, 31].

## *3.2 Efficient Quickest Change Detection*

Quickest Change Detection (QCD) is a branch of statistical signal processing that thrives to detect the change point of statistical properties of a random process [1, 2, 31]. The objective of QCD is to produce algorithms that detect the change with a minimal delay (ADD) while adhering to false alarm rate constraints (PFD). Consider a collection of obtained match scores, $s_1, s_2, \cdots, s_n$, from the AA system. Assuming that the individual scores are mutually independent, QCD theory can be used to determine whether a change has occurred before time $n$ or not.

Consider a sequence of time instances $t = 1, 2, \cdots, i$ in which the device operates. At each time $i, i > 0$, a decision is made whether to take or skip an observation at time $i + 1$. Let $M_i$ be the indicator random variable such that $M_i = 1$ if the score $x_i$ is used for decision making, and $M_i = 0$ otherwise. Thus, $M_{i+1}$ is a function of the information available at time $i$, i.e. $M_{i+1} = \phi_i(I_i)$, where $\phi_i$ is the control law at time $i$, and $I_i = [M_1, M_2, \cdots, M_i, s_1^{M_1}, s_2^{M_2}, \cdots, s_i^{M_i}]$ represents the

information at time $i$. Here, $s_i^{M_i}$ represents $s_i$ if $M_i = 1$, otherwise $x_i$ is absent from the information vector $I_i$. Let $S$ be the stopping time on the information sequence $\{I_i\}$. Then, average percentage of observations (APO) obtained prior to the change point can be quantified as $APO = E\left[\frac{1}{S}\sum_{n=1}^{S} M_n\right]$.

In a non-Bayesian setting, due to the absence of a priori distribution on the change point, a different quantity should be used to quantify the number of observations used for decision making. Work in [1, 2], proposes change Duty Cycle (CDC) as $CDC = \lim_n \sup \frac{1}{n} E_n\left[\sum_{k=1}^{n-1} M_k | \tau \geq n\right]$ for this purpose. It should be noted that both CDC and APO are similar quantities. With the definition of CDC, efficient QCD in a minimax setting can be formulated as the following optimization problem

$$\begin{aligned} &\underset{\phi,\tau}{\text{minimize}} \quad ADD(\phi, \tau) \\ &\text{subject to} \quad PFD(\phi, \tau) \leq \alpha, \quad CDC(\phi, \tau) \leq \beta. \end{aligned} \tag{1}$$

In [2], a two threshold algorithm called DE-CumSum algorithm, is presented as a solution to this optimization problem. For suitably selected thresholds chosen to meet constraints $\alpha$ and $\beta$, it is shown to obtain the optimal lower bound asymptotically as $\alpha \to 0$. The DE-CumSum algorithm is presented below.

Start with $W_0 = 0$ and let $\mu > 0$, $A > 0$ and $h \geq 0$. For $n \geq 0$ use the following control rule $M_{n+1} = 0$ if $W_n < 0$ otherwise 1 if $W_n \geq 0$. Statistic $W_n$ is updated as follows

$$W_{n+1} = \begin{cases} \min(W_n + \mu, 0), & \text{if } M_{n+1} = 0 \\ \max(W_n + \log L(s_{n+1}), -h), & \text{if } M_{n+1} = 1, \end{cases}$$

where $L(s) = \frac{f_1(s)}{f_0(s)}$. A change is declared at time $\tau_W$, when the statistic $W_n$ passes the threshold $A$ for the first time as $\tau_W = \inf\{n \geq 1 : W_n > A\}$.

### *3.3 Multi-user Quickest Intruder Detection (MQID)*

Based on the discussion above, we introduce the Multiple-user Quickest Intruder Detection (MQID) algorithm. Whether an intrusion has occurred or not is determined using a score value. When the score value is above a pre-determined threshold, an intrusion is declared. At initialization, it is assumed that the user operating the device is a legitimate user; therefore the score is initialized with zero. The algorithm updates the score value when new observations are observed. During the update step, the algorithm considers matched and non-matched distributions of

all users along with the current score value to produce the updated score. Pseudo code of the algorithm is shown in Algorithm 1.

The algorithm has three arguments. Argument *Efficient* determines whether to use data-efficient version of QCD or not. If data-efficient QCD is used then the parameter $\gamma$ determines the floor threshold. Parameter $D$ governs how fast the score is increased.

During training, enrolled images of each user along with the known negative dataset is used to construct matched and non-matched score distributions. In addition, enrolled images of the user are used to construct a classifier $c_i$. During inference, given an observation $x$, first classification scores from each classifier are obtained. Then, the likelihood of the obtained classifier score is evaluated using the likelihood ratio of each matched and non-matched distribution belonging to each user. The minimum likelihood ratio is considered as the statistic to update the current score of the system.

Updating the score based on the distribution is done as per the Algorithm considering the parameters as well as the magnitude of previous score value.

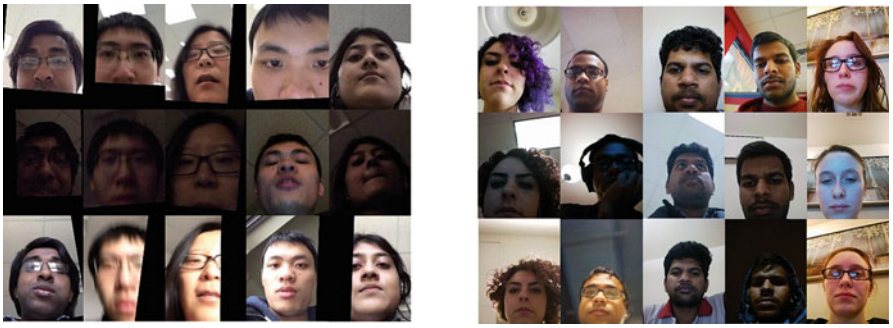
**Algorithm 1:** Algorithm to update the score based on the observations for the proposed method

**input** : $score, x_n, \{f_{0,i}, f_{1,i}, c_i | \forall i\}, \gamma, D$, *Efficient*
**output**: $score$

$L = \min_i \log(\frac{f_{1,i}(c_i(x_n))}{f_{0,i}(c_i(x_n))})$
**if** *Efficient* **then**
  **if** $score < 0$ **then**
    $score = \min(score + D, 0)$;
  **else**
    $score \leftarrow \max(score + L, -\gamma)$ ;
  **end**
**else**
  $score \leftarrow score + L$ ;
**end**
Return $(score)$;

## 4 Experimental Results

We test the proposed method on two publicly available Active Authentication datasets – UMDAA01 [8] and UMDAA02 [17] using the face modality. First, we explain the protocol used for evaluation. Then, we describe the performance metric used. Finally, we introduce the two datasets and present evaluation performance on these datasets (Fig. 3).



(a) (b)

**Fig. 3** Sample face images from the (**a**) UMDAA01 dataset and (**b**) UMDAA02 dataset used for evaluation. Samples from the same subject are shown in each column

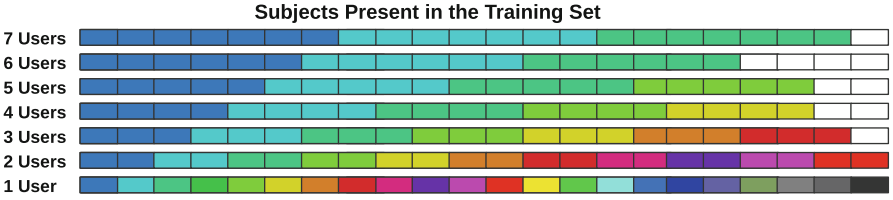



**Fig. 4** Policy used to select the enrolled users for testing. The enrolled users considered together for a trial are denoted in the same color. For the case of 7 enrolled users, there are three trials. For the case of a single user, there are 22 trials

## *4.1 Protocol and Metrics*

In both datasets, the first 22 users were used as possible enrolled users. Users 23–33 were used as the known negative samples. Remaining users were considered as intruders. From the enrolled users 10% of data were randomly chosen to represent the enrolled images. These image frames were removed from the test set. For each dataset, we varied the number of enrolled users from 1 to 7. If the number of enrolled users is $m$, we partitioned the first 22 users into disjoint groups of $m$ and carried out floor$(22/m)$ trials. For example, in the case of 7 users, users 1–7 were considered to be enrolled in the first trial. For the second trial, users 8–14 were considered to be enrolled. Remaining users were not considered for testing. An illustration of the partitions obtained for several trials is shown in Fig. 4. In each trial, the intruder classes were considered one at a time and an intrusion was simulated.

In order to simulate an intrusion, the following process was followed. The entire video clips of the enrolled users were appended in the order of their index to form an augmented video for each trial. Then, each intruder from the intruder set was considered one at a time. Considered intruder's video clip was appended at the end

of the augmented video clip to produce the test video clip. Shown in Fig. 1 is a summary of such a clip for the case of two enrolled users.

During training, we extracted the image frames from the video clip with a sampling rate of 1 image per 3 seconds. We used the Viola-Jones face detector to detect faces in the extracted image frame and performed local histogram normalization. The extracted image was resized to $224 \times 224$ and image features were extracted from the ResNet18 deep architecture which was pre-trained on the ImageNet dataset. For all cases, we considered the distance to the nearest neighbor as the user specific classifier $c_i$.

The performance of a quickest change detection scheme depends on ADD and PFD. Ideally, an AA system should be able to operate with low ADD and PFD. In order to evaluate performance of the system following [28], we used the ADD-PFD graph. We report ADD values required to obtain a PFD of 2% and 5% in Tables 1 and 2, respectively. These tables indicate the latency of detecting an intrusion in average while guaranteeing a false detection rate of 2% and 5%, respectively.

## 4.2 Methods

We evaluated the following methods using the protocol presented. For a fair comparison, in all cases except for in $P_n(FG17)$ we used the statistic $L = \min_i \log(\frac{f_{1,i}(c_i(x_n))}{f_{0,i}(c_i(x_n))})$ as the score value to perform intrusion detection.

**Single score-based authentication (SSA)** Present score value $L$ alone is used to authenticate the user. If the score value is above a predetermined threshold, the user is authenticated otherwise treated as an intrusion.

**Time decay fusion (Sui et al.) [32]** In this method, two score samples fused by a linear function is used along with a decaying function to determine the authenticity of a user as, $s_n = wL_{n-1} + (1-w)L_n \times e^{\tau \delta t}$, where, $w$, $\tau$ are constants and $\delta t$ is the time elapsed since the last observation.

**Confidence functions (Crouse et al.) [6]** A sequential detection score $S_{login}$ is calculated by incorporating time delay since the last observation and a function of the present score $x_n$. The detection score is evaluated as, $S_{login,n} = S_{login,n-1} + f_{map}s_n + \int_{t_{prev}}^{t_{now}} f_{dec}dt$. Functions $f_{map}$ and $f_{dec}$ are empirical functions presented in [6].

**Probability of Negativity ($P_n$(FG17)) [26]** This method is proposed for multi-user AA. Matched and non-matched distributions of each user is used to produce an individual score. These uncertainty scores are then fused to produce the Probability of Negativity ($P_n$). For this baseline, we combined $P_n$ score values sequentially using the method proposed in [32].

**Multi-user Quickest Intruder Detection (MQID)** The method proposed in this paper with the Min-Max formulation.

**Data Deficient Multi-user Quickest Intruder Detection (DEMQID):** The method proposed in this paper using the Min-Max formulation with data-efficient constraints. We selected parameter $D$ by constraining the average number of observations to be 50% of all observations for the case of the single user. In our experiments we found this parameter to be 100.

### *4.3 Results*

We carried experiments on the UMDAA01 and UMDAA02 datasets. The ADD-PFD curves are shown in Figs. 5 and 6 when the number of users are varied from 1 to 7. ADD values obtained for PFD of 2% and 5% are tabulated for UMDAA01 and UMDAA02 in Tables 1 and 2, respectively.

**UMDAA01 Face Dataset** The UMDAA-01 dataset [8] contains images captured using the front-facing camera of an iPhone 5S mobile device of 50 different individuals captured across three sessions with varying illumination conditions. Images of this dataset contain pose variations, occlusions, partial clippings as well as natural facial expressions as evident from the sample images shown in Fig. 3a. For our experiments we concatenated videos from all three sessions to form 50 classes.

In all considered cases MQID method has performed better than the other baseline methods when it was desired to achieve a PFD of 2%. It is also seen that $P_n(FG17)$, which is a method proposed for multi-user AA has also outperformed SSH method which uses log-likelihood ratio in all cases. Furthermore, data-efficient version of the algorithm, DEMQID, has performed on par with MQID, even performing better in certain cases. Average percentage of observations obtained in DEMQID for this dataset was 0.304.

However, it can be observed that when 5% of PFD is allowed, even other baseline methods perform reasonably well. For example, in majority of the cases SSH has performed on par with MQID. We also observe that DEMQID is slightly worse than MQID in this case. This suggests that for the employed deep feature, a PFD rate of 5% can be obtained even when the sequence of data are not considered. DEMQID takes more sparse samples when deciding the score value. As a result, when the score function is noisy, DEMQID is not affected by the noise as much as MQID. Even-though sparser sampling would result in some latency in detection, overall trade-off can be beneficial. This is why, DEMQID outperforms MQID when decision making is more challenging (as was the case when PFD of 2% was considered).

However, when the decision making becomes easier, DEMQID does not contribute towards improving the detection accuracy as score values are less noisy. This is why in the case of 5% of PFD, DEMQID performs worse than MQID.

**UMDAA02 Face Dataset** The UMDAA-02 Dataset [17] is an unconstrained multimodal dataset with 44 subjects where 18 sensor observations were recorded across a two month period using a Nexus 5 mobile device. Authors of [17] have made the face modality and the touch-data modality[10] publicly available. In our

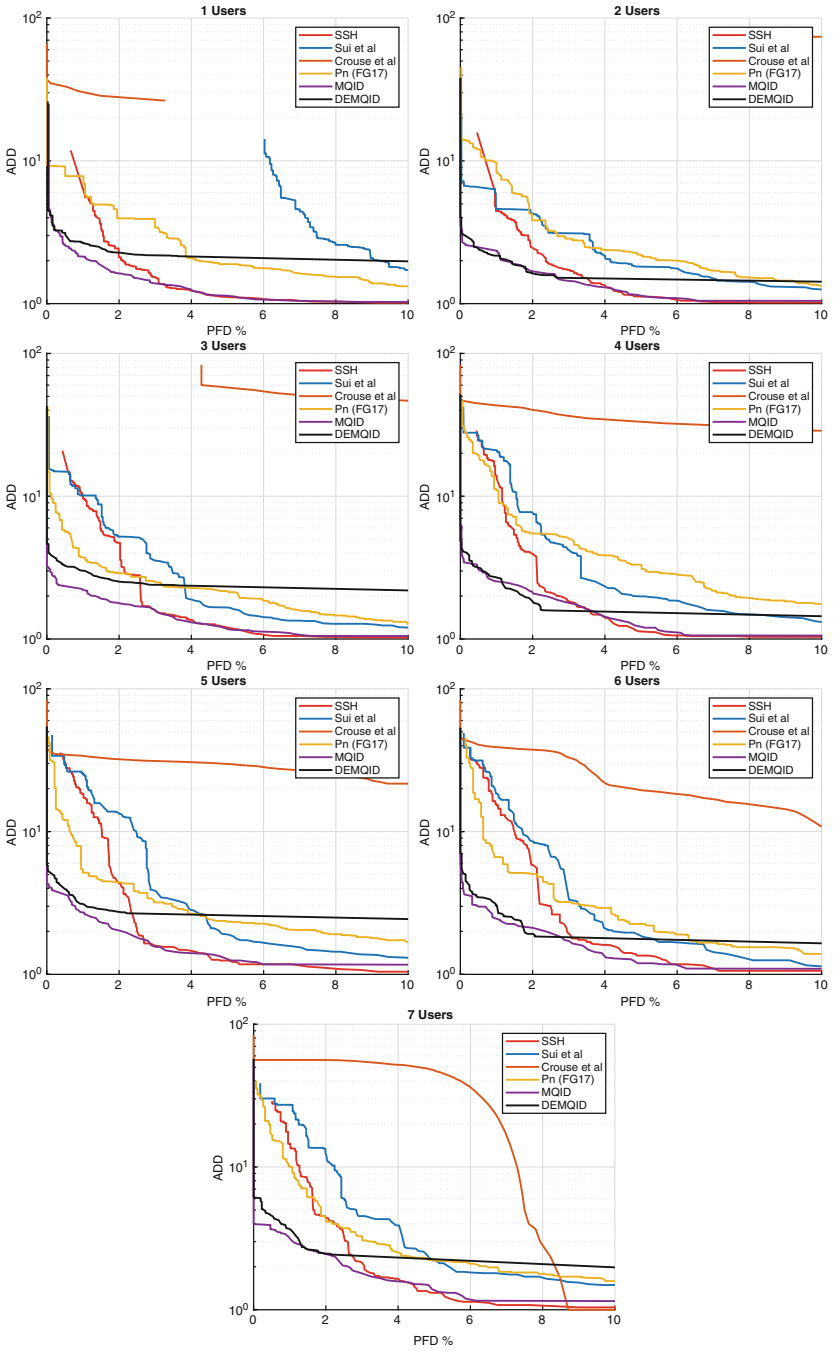



**Fig. 5** The ADD-PFD curves corresponding to the UMDAA01 dataset when the number of users are varied from 1 to 7

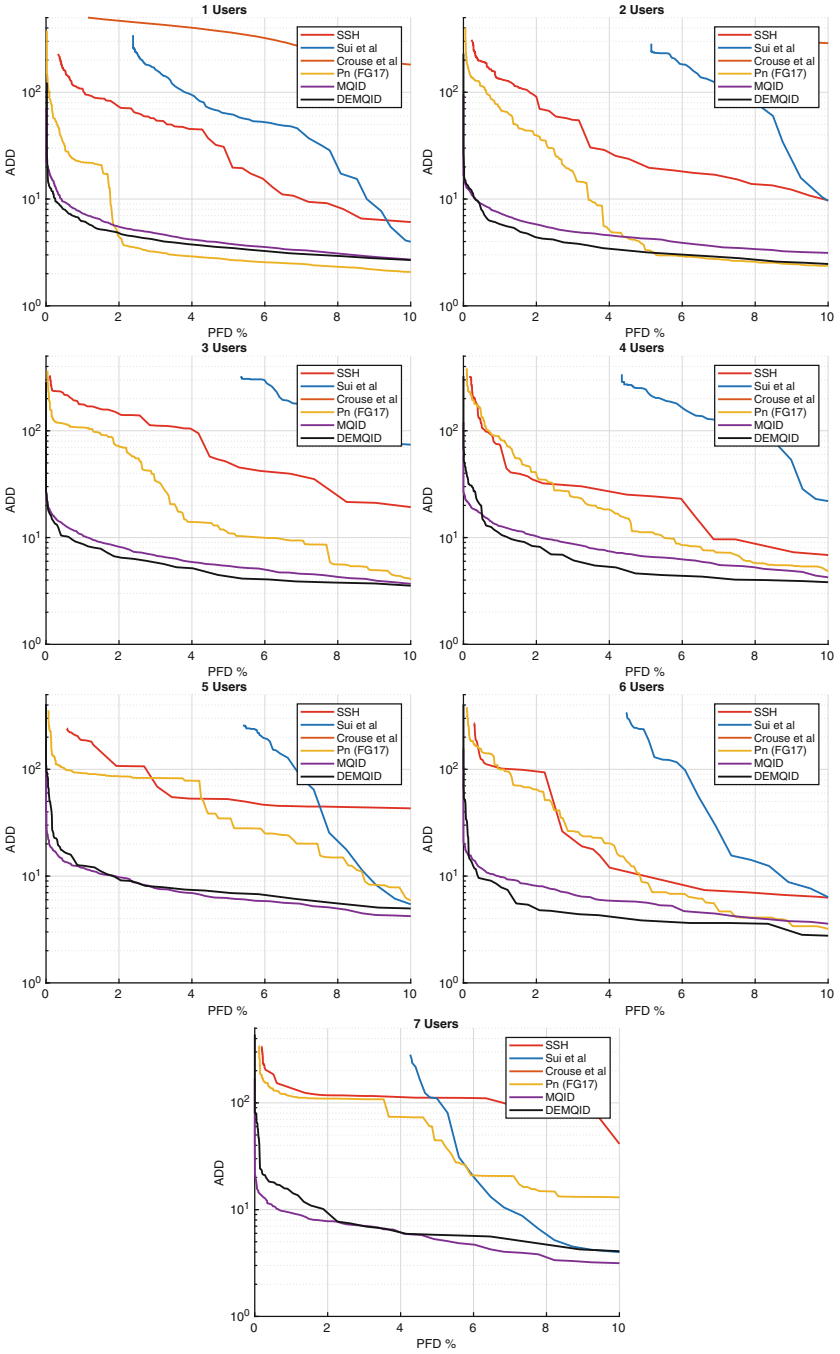



**Fig. 6** The ADD-PFD curves corresponding to the UMDAA02 dataset when the number of users are varied from 1 to 7

**Table 1** Tabulation of ADD for PFD of 2% and 5% when the users are varied from 1 to 7 on the UMDAA01 dataset. When a particular method failed to achieve prescribed PFD it is indicated by N/A

| | 5% | | | | | | | 2% | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # of Users | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| SSH | 1.14 | 1.14 | 1.17 | 1.18 | 1.25 | 1.35 | 1.31 | 2.28 | 2.49 | 4.73 | 3.98 | 4.41 | 5.84 | 4.49 |
| Sui et al. | N/A | 1.82 | 1.66 | 1.98 | 1.89 | 1.86 | 2.51 | N/A | 2.04 | 4.74 | 7.74 | 13.41 | 8.59 | 13.41 |
| Crouse et al. | N/A | N/A | 57.20 | 33.92 | 29.65 | 19.49 | 47.8 | 28.4 | N/A | N/A | 40.44 | 32.25 | 37.04 | 56.2 |
| Pn (FG17) | 2.10 | 2.20 | 2.16 | 3.29 | 2.35 | 2.23 | 2.51 | 3.96 | 3.84 | 2.89 | 5.48 | 4.41 | 5.06 | 4.51 |
| MQID | 1.14 | 1.14 | 1.17 | 1.20 | 1.25 | 1.19 | 1.31 | 1.63 | 1.65 | 1.79 | 2.08 | 2.02 | 2.12 | 2.49 |
| DEMQID | 2.14 | 1.52 | 2.37 | 1.59 | 2.51 | 1.86 | 2.51 | 2.28 | 1.64 | 2.51 | 1.84 | 2.72 | 1.92 | 2.49 |

**Table 2** Tabulation of ADD for PFD of 2% and 5% when the users are varied from 1 to 7 on the UMDAA02 dataset. When a particular method failed to achieve prescribed PFD it is indicated by N/A

| | *5%* | | | | | | | *2%* | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # of Users | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| SSH | 19.7 | 19.6 | 51.82 | 24.33 | 52.64 | 10.01 | 110.2 | 72.92 | 90.71 | 150.0 | 36.23 | 107.6 | 93.6 | 118.1 |
| Sui et al. | 63.1 | 284.9 | N/A | 243.1 | N/A | 237.6 | 109.4 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Crouse et al. | 364.5 | N/A | N/A | N/A | N/A | N/A | N/A | 467.8 | N/A | N/A | N/A | N/A | N/A | N/A |
| Pn (FG17) | 2.71 | 3.31 | 10.91 | 11.22 | 34.64 | 7.06 | 44.55 | 4.30 | 39.56 | 72.52 | 37.44 | 86.3 | 64.0 | 116.0 |
| MQID | 3.83 | 4.28 | 5.42 | 6.67 | 6.11 | 5.61 | 5.30 | 5.58 | 5.77 | 8.14 | 10.38 | 9.10 | 8.03 | 7.78 |
| DEMQID | 3.47 | 3.17 | 4.13 | 4.618 | 6.93 | 3.85 | 5.82 | 4.32 | 4.39 | 6.38 | 8.34 | 9.12 | 4.79 | 10.15 |

work we only consider the face modality to perform tests. A sample set of images obtained from this dataset is shown in Fig. 3b. UMDAA02 is a more challenging dataset compared to UMDAA01 as apparent from the sample images shown in Fig. 3. In particular, we note the existence of a huge intra-class variations in this dataset in terms of poses, partial faces, illumination as well as appearances of the users.

As a result of having higher complexity, detecting intruders become more challenging in UMDAA02 compared to UMDAA01. However, due the challenging behavior of the dataset, the importance of the proposed method is magnified. In all ADD-PFD curves obtained for UMDAA02 in Fig. 6, it is evident that the proposed methods significantly outperform the baseline methods. Furthermore, DEQID has outperformed QID in most of the cases showing the significance of data efficient QCD.

In our evaluations we show that even when the number of users are increased, the performance of the proposed system does not drop drastically. For the UMDAA01 dataset, only 2.35 additional samples were required to maintain a probability of false detection of 2% when the users were increased from 1 o 7. In a more challenging UMDAA02 dataset, 4.33 more samples were required on average to maintain the same false detection rate.

## 5 Concluding Remarks

It has been previously showen that AA yields superior detection performance when the QCD algorithm is used [28]. In this chapter we study the problem of quickest change detection in a multiple-user AA scenario. We proposed MQID algorithm for multiple-user AA with low latency. Furthermore, we extended the initial formulation to a data efficient version by proposing DEMQID algorithm. We evaluated the performance of the proposed methods on the UMDAA01 and UMDAA02 datasets. Our experiments suggest that the proposed method is more effective compared to the baseline methods we considered. It was also shown that, the proposed method allows the number of enrolled users to be increased with a relatively smaller cost in terms of observations. Only 2.35 and 4.33 observations were required on average to maintain a false detection rate of 2% when the users were increased from 1 to 7 in the UMDAA01 and UMDAA02 datasets, respectively.

**Acknowledgements** This work was supported by the NSFgrant 1801435.

## References

1. Banerjee T, Veeravalli VV (2014) Data-efficient quickest change detection. Sri Lankan J Appl Stat Special Issue: Modern Statistical Methodologies in the Cutting Edge of Science 183–208 Nov 2014

2. Banerjee T, Veeravalli VV (2013) Data-efficient quickest change detection in minimax settings. IEEE Trans Inf Theory 59:6917–6931
3. Bo C, Zhang L, Li X-Y, Huang Q, Wang Y (2013) Silentsense: silent user identification via touch and movement behavioral biometrics. In: Proceedings of the 19th annual international conference on mobile computing & networking, MobiCom '13. ACM, New York, pp 187–190
4. Crawford H, Renaud K (2014) Understanding user perceptions of transparent authentication on a mobile device. J Trust Manage 1(7):1–28
5. Crawford H, Renaud K, Storer T (2013) A framework for continuous, transparent mobile device authentication. Comput Secur 39:127–136
6. Crouse D, Han H, Chandra D, Barbello B, Jain AK (2015) Continuous authentication of mobile user: fusion of face image and inertial measurement unit data. In: International conference on biometrics
7. Dunn RB, Reynolds DA, Quatieri TF (2000) Continuous user authentication on mobile devices: recent progress and remaining challenges. IEEE Signal Process Mag 10(1–3):93–112
8. Fathy ME, Patel VM, Chellappa R (2015) Face-based active authentication on mobile devices. In: IEEE international conference on acoustics, speech and signal processing
9. Feng T, Zhao X, Carbunar B, Shi W (2013) Continuous mobile authentication using virtual key typing biometrics. In: Proceedings of the 2013 12th IEEE international conference on trust, security and privacy in computing and communications, TRUSTCOM '13, IEEE Computer Society, Washington, DC, pp 1547–1552
10. Fierrez J, Pozo A, Martinez-Diaz M, Galbally J, Morales A (2018) Benchmarking touchscreen biometrics for mobile authentication. IEEE Trans Inf Forensics Secur 13(11):2720–2733
11. Frank M, Biedert R, Ma E, Martinovic I, Song D (2013) Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf Forensics Secur 8(1):136–148
12. Fridman L, Weber S, Greenstadt R, Kam M (2017) Active authentication on mobile devices via stylometry, Application usage, web browsing, and GPS location. IEEE Syst J 11(2):513–521
13. Gascon H, Uellenbeck S, Wolf C, Rieck K (2014) Continuous authentication on mobile devices by analysis of typing motion behavior. In: Katzenbeisser S, Lotz V, Weippl E (eds) Proceedings of GI conference Sicherheit, Bonn, Gesellschaft für Informatik e.V., pp 1–12
14. Hadid A, Heikkila JY, Silven O, Pietikainen M (2007) Face and eye detection for person authentication in mobile phones. In: ACM/IEEE international conference on distributed smart cameras, Sept 2007, pp 101–108
15. Juefei-Xu F, Bhagavatula C, Jaech A, Prasad U, Savvides M (2012) Gait-ID on the move: pace independent human identification using cell phone accelerometer dynamics. In: IEEE international conference on biometrics: theory, applications and systems, Sept 2012, pp 8–15
16. Lorden G (1971) Procedures for reacting to a change in distribution. Ann Math Stat 42(6):1897–1908
17. Mahbub U, Sakar S, Patel VM, Chellappa R (2016) Active authentication for smartphones: a challenge data set and benchmark results. In: IEEE international conference on biometrics: theory, applications and systems, Sept 2016
18. Martin AF, Przybocki MA (2001) Speaker recognition in a multi-speaker environment. In: INTERSPEECH
19. McCool C, Marcel S, Hadid A, Pietikainen M, Matejka P, Cernocky J, Poh N, Kittler J, Larcher A, Levy C, Matrouf D, Bonastre J-F, Tresadern P, Cootes T (2012) Bi-modal person recognition on a mobile phone: using mobile phone data. In: IEEE international conference on multimedia and expo workshops, July 2012, pp 635–640
20. Meng W, Wong DS, Furnell S, Zhou J (2015) Surveying the development of biometric user authentication on mobile phones. IEEE Commun Surv Tutorials 17(3):1268–1293
21. Narang N, Martin M, Metaxas D, Bourlai T (2017) Learning deep features for hierarchical classification of mobile phone face datasets in heterogeneous environments. In: 2017 12th IEEE international conference on automatic face and gesture recognition (FG 2017). IEEE Computer Society, Los Alamitos, pp 186–193

22. Page ES (1954) Continuous inspection schemes. Biometrika, 41(1/2):100–115
23. Patel VM, Chellappa R, Chandra D, Barbello B (2016) Continuous user authentication on mobile devices: recent progress and remaining challenges. IEEE Signal Process Mag 33(4): 49–61
24. Pelecanos J, Navrátil J, Ramaswamy GN (2008) Conversational biometrics: a probabilistic view. In: Ratha NK, Govindaraju V (eds) Advances in biometrics. Springer, London
25. Perera P, Patel VM (2016) Quickest intrusion detection in mobile active user authentication. In: International conference on biometrics theory, applications and systems
26. Perera P, Patel VM (2017) Towards multiple user active authentication in mobile devices. In: IEEE international conference on automatic face and gesture recognition
27. Perera P, Patel VM (2019) Face-based multiple user active authentication on mobile devices. IEEE Trans Inf Forensics Secur 14(5):1240–1250
28. Perera P, Patel VM (2018) Efficient and low latency detection of intruders in mobile active authentication. IEEE Trans Inf Forensics Secur 13(6):1392–1405
29. Samangouei P, Patel VM, Chellappa R (2015) Attribute-based continuous user authentication on mobile devices. In: IEEE international conference on biometrics: theory, applications and systems
30. Serwadda A, Phoha VV, Wang Z (2013) Which verifiers work? A benchmark evaluation of touch-based authentication algorithms. In: IEEE international conference on biometrics: theory, applications and systems, Sept 2013, pp 1–8
31. Veeravalli VV, Banerjee T (2012) Quickest change detection. ArXiv e-prints, Oct 2012
32. Zou X, Sui Y, Du EY, Li F (2012) Secure and privacy-preserving biometrics based active authentication. In: IEEE international conference on systems, man, and cybernetics (SMC), pp 1291–1296
33. Zhang H, Patel VM, Shekhar S, Chellappa R (2015) Domain adaptive sparse representation-based classification. In: IEEE international conference on automatic face and gesture recognition, vol 1, May 2015, pp 1–8
34. Zhong Y, Deng Y (2014) Sensor orientation invariant mobile gait biometrics. In: IEEE international joint conference on biometrics, Sept (2014), pp 1–8