NISTIR 7378

A Taxonomy of Definitions for Usability Studies in Biometrics

Ross J. Micheals
Brian Stanton
Mary Theofanos
Shahram Orandi

Information Access Division
Information Technology Lab

November 2006

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NISTIR 7378

A Taxonomy of Definitions for Usability Studies in Biometrics

Ross J. Micheals
Brian Stanton
Mary Theofanos
U.S. Department of Commerce
Technology Administration
National Institute of Standards and Technology
Information Technology Lab
Gaithersburg, MD 20899

Shahram Orandi
MitreTek Systems
Falls Church, VA

November 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

1. Introduction

Historically, usability research strives to focus on user behavior in a manner that is as system independent as possible. Although "ISO/IEC JTC 1/SC 37 Standing Document 2 — Harmonized Biometric Vocabulary, Draft N1779" provides a foundation towards common terminology, it currently lacks definitions specifically for use in usability studies that are also consistent with this practice.

To address this gap, this document describes a taxonomy of definitions for use in usability studies of biometrics. The use of the term taxonomy was deliberately selected since the terms as presented here represent different *classes* of definitions. That is, practitioners are expected to further refine the terminology to best fit their particular needs. The taxonomy is designed to be general enough to incorporate a variety of world views, but specific enough to provide a common ontology for facilitating clear and concise communication.

Whenever possible, the taxonomy was designed to fit within the aforementioned international Harmonized Biometric Vocabulary. However, it is emphasized that these definitions are distinct from existing biometric terminology in that each term is driven by *user behavior* as opposed to a system-oriented viewpoint.

2. Taxonomy

Definitions are presented here in traditional ISO convention; i.e., "the form of a definition shall be such that it can replace the term in context."

2.1 Presentation

The term *presentation* is defined as follows:

> **presentation**
> the display of biometric characteristics to a sensor

Mapping user behavior to the definition of a presentation is straightforward; consider the following:

> EXAMPLE. The positioning of oneself for having a facial photograph taken is a *presentation*; i.e., the display of facial biometric characteristics to a visible light sensor.

The definition of *presentation* refers to *characteristics* (plural) as opposed to a single characteristic because a user may present multiple characteristics simultaneously.

> EXAMPLE. The simultaneous placement of a left index, middle, ring and little finger upon a scanner platen (active sensing area) is the display of fingerprint characteristics to an optical fingerprint sensor; i.e., a left slap presentation.

Simultaneous presentations are not necessarily constrained to any particular specific biometric modality.

> EXAMPLE. The positioning of oneself for having facial and iris photographs taken by a multimodal sensor may be considered to be a single presentation.

Practitioners are expected to describe the relationships among different potential groupings of presentations for their application.

> EXAMPLE. The left slap may be viewed as a single presentation (the presentation of a hand), or as four presentations (the presentation of multiple fingers).

Presentations may be further qualified as *implicit* or *explicit:*

> **explicit presentation**
> a presentation made with the presenter's awareness
>
> **implicit presentation**
> a presentation made without the presenter's awareness

Most presentations are likely to be *explicit.*

> EXAMPLE. A person looking into a camera for a driver's license photo is offering an explicit presentation.

However, sensors may be situated beyond the awareness of a presenter.

> EXAMPLE. If a person was being recorded via a hidden camera, then the presenter would be offering an implicit presentation.

Awareness of the sensor or system itself cannot be equated with awareness of the presentation.

> EXAMPLE. Some airport exit kiosks are capable of taking facial photographs with a fairly wide angle lens. A person may offer an implicit presentation if they are standing in an area in which they perceive that they are not being imaged, but are not far enough out of view to escape the camera's field of view.

Presentations may be further qualified as *cooperative* or *uncooperative:*

> **cooperative presentation**
> a presentation that the presenter provides willingly
>
> **uncooperative presentation**
> a presentation that the presenter provides unwillingly

The definition of cooperative versus uncooperative depends only on the *willingness* to present.

> EXAMPLE. Suppose a person applying for a visa arrives at a consulate and presents their fingerprints to verify their identity. If they present their fingerprints willingly, then a cooperative presentation would occur.

In some extreme cases, a cooperative presentation may be the display of biometric characteristics of someone else.

EXAMPLE. A person entering the country under false documentation may be willing to present false biometric data to a fingerprint sensor (i.e., "spoof" the system). Even though their motivation may be to impersonate someone else, they may offer a cooperative presentation.

Uncooperative presentations are more common in law enforcement scenarios.

EXAMPLE. A suspect who flees a border patrol is caught and processed. If the suspect is reluctant to present their fingers for matching against a watch list, then an uncooperative presentation would occur.

It is anticipated that most usability studies will be limited to cooperative presentations. Practitioners are therefore encouraged to assume that presentations are cooperative unless otherwise specified.

2.2 Attempt

The term *attempt* is defined as follows:

attempt
the response to an opportunity to make a presentation

NOTE. Presentations may span multiple attempts.

A presentation is typically made to a functioning device.

EXAMPLE. The presentation of a left slap to a ready sensor is an *attempt.*

However, a system needs to be neither online nor operational for an attempt to occur. Simply by the virtue of being available, a sensor implicitly affords an opportunity to present.

EXAMPLE. The presentation of a left slap to a broken sensor is an attempt.

EXAMPLE. The premature presentation of a middle finger to a sensor not yet online is an attempt.

For completeness, we presume that practitioners are likely to consider a lack of response to a non-operational or offline system as *not* an attempt.

EXAMPLE. Making no presentation of an index finger to an offline sensor may be considered as "no attempt."

The following examples illustrate how presentations may span multiple attempts.

EXAMPLE. A fingerprint sensor is configured to automatically capture a left slap followed by a right slap. Suppose the presenter places their left hand on the scanner and that the system successfully captures an image and immediately continues by polling for a right slap. In this case, the presentation of the left slap spanned two separate presentation opportunities. It is assumed that each presentation opportunity corresponded to the sensor polling for a different biometric (left slap, then right slap).

EXAMPLE. A camera takes images in succession. Each image may be considered as separate attempts, but the presenter may be considered as making only a single presentation.

A user may respond to a presentation opportunity with a *lack* of presentation.

> EXAMPLE. An operator triggers a fingerprint scanner to capture, but the intended presenter becomes distracted and no presentation occurs within some specified time (i.e., a system timeout occurs).

Like *presentation*, practitioners are encouraged to further constrain *attempt* according to their needs.

> EXAMPLE. The presentation of a *left slap* may be viewed as a single attempt to present four fingerprints, or, as four attempts each corresponding to a different fingerprint.

An *attempt* may be further qualified as *acceptable* or *unacceptable*:

> **acceptable attempt**
> an attempt that fulfills the minimal capture requirements of a system
>
> NOTE. Acceptable attempts must yield the minimum required biometric data from a working system in a particular configuration.
>
> **unacceptable attempt**
> an attempt that does not fulfill the minimal capture requirements of a system

Notice that capture requirements are associated with a *system*, as opposed to a *sensor*. This allows for more flexible definitions of what constitutes the minimal capture requirements (such as requiring approval from a human in-the-loop).

> EXAMPLE. An attempt occurs where the presenter has their photograph taken, but an operator rejects the image. Since the system has labeled the data as not meeting the minimal capture requirements, the attempt is unacceptable.

> EXAMPLE. An attempt occurs where the presenter has their photograph taken, but the lens cap was not removed from the camera. Since the system did not acquire an image that contains a face, the attempt is unacceptable. This example is only valid if the set of minimum capture requirements includes obtaining an image that contains a non-occluded, visible face.

The biometric data required from a system depends on the system configuration.

> EXAMPLE. A sensor collects a face and iris image simultaneously. The system may be configured to first attempt to collect an iris image, and use the face image as a fallback upon failure to capture an iris image. Such a system has a different set of minimal capture requirements than that same system configured to require both a successful face and a successful iris image.

With the exception of a human in-the-loop, the biometric *system*, and not user behavior is what makes an attempt acceptable or unacceptable.

2.3 Task

The term *task* is defined as follows:

> **task**
> a set of user behavior that defines an attempt

Tasks typically correspond to the desired user behavior.

> EXAMPLE. The presentation of a *left slap* to a sensor may be a task.

This definition of a *task* allows for the further qualification of *attempts*.

> **conformant attempt**
> an attempt that fulfills the requirements set out by a task
>
> **non-conformant attempt**
> an attempt that does not fulfill the requirements set out by a task

A *lack of action* may be the cause of a non-conformant attempt, since a lack of action is a form of response.

> EXAMPLE. A user (presenter) does nothing when instructed to place their left index finger upon a fingerprint scanner platen. Through lack of action, a *non-conformant attempt* occurs.

User (presenter) behavior, as opposed to system behavior, distinguishes between a conformant and a non-conformant attempt.

> EXAMPLE. A user (presenter) that places their right index finger on a fingerprint scanner when instructed to place their *left* index finger makes a *non-conformant attempt* since they do not fulfill the requirements defined by the task of placing their left index finger. Regardless of whether or not the system detects that a fingerprint has been captured, the attempt is non-conformant.

Since the acceptability and conformance qualifiers are orthogonal, they generate four categories of attempts.

1. *acceptable conformant attempt*

   EXAMPLE. The presenter behaves according to task and the system's minimum capture requirements are satisfied.

2. *acceptable non-conformant attempt*

   EXAMPLE. The presenter did not behave according to task, but the system's minimum capture requirements were satisfied anyway.

3. *unacceptable conformant attempt*

   EXAMPLE. The presenter behaves according to task, but the system's minimum capture requirements are not satisfied.

4. *unacceptable non-conformant attempt*

   EXAMPLE. The presenter did not behave according to task, and the system's minimum capture requirements were not satisfied.

An acceptable conformant attempt implies the successful completion of a task because by definition, it is a response that simultaneously satisfies the task requirements while also producing the minimum required biometric data.

The following scenario illustrates how the taxonomy may be used within the context of a simple usability experiment:

> EXAMPLE. Four participants (Participants A through D) are each instructed to perform a *left slap* task.
>
> Assume, with respect to user behavior, that:
>
> - The set of user behavior that defines a left slap task is the placement of the left index, middle, ring, and little fingers onto the fingerprint sensor's platen.
> - User behaviors occur at the appropriate times unless noted otherwise.
>
> Assume, with respect to system behavior, that:
>
> - The system is operational and configured in a manner for collecting left slap images.
> - The system may detect whether or not a hand is on the scanner and approves or rejects that data based on some built-in quality criteria.1
> - The system cannot detect *which* hand (i.e., left versus right) has been placed on the scanner.
> - If the sensor detects that hand has been placed on the scanner and approves the collected data, then the minimum capture requirements are met.
>
> Each participant illustrates a different category of attempt.
>
> Participant A presents a left slap to the fingerprint sensor, which the system detects and approves. The user behavior (the presentation of the left slap) yields an attempt that is *acceptable* (the system detects and approves the data) and *conformant* (the user fulfilled the *left slap* task).
>
> Participant B also presents a left slap to the fingerprint sensor, but the system rejects it. The user behavior yields an attempt that is *unacceptable* (it was rejected) yet *conformant* (the user presented the left slap as they were instructed).

1 Although many sensors may have a high-degree of detection accuracy, it is possible for a system to fail to detect a presentation. The example does not illustrate this case.

Participant C presents a *right* slap to the fingerprint sensor, which the system approves. The user behavior is *acceptable* (it was approved) but *non-conformant*, since the user behavior (the right slap) did not fulfill the task requirements.

Participant D is distracted and makes no presentation to the fingerprint sensor and the system "times out"—i.e., no biometric data was collected within a specified interval. This attempt is *unacceptable* (no hand was detected on the scanner) and *non-conformant* (the response to the presentation opportunity was to do nothing).

The following diagram is an illustration of the participant attempts. Each cell lists the category of attempt, the participant letter, and a summary of the action.

conformance \ acceptability		
	acceptable conformant A left slap presented and approved by system	**unacceptable conformant** B left slap presented but rejected by system
	acceptable non-conformant C right slap presented and approved by system	**unacceptable non-conformant** D no presentation, system timeout

Acceptability changes across the vertical axis—the acceptable attempts are on the left (A and C), and the unacceptable attempts are on the right (B and D). Similarly, conformance changes across the horizontal axis—the conformant attempts are above (A and B) and the non-conformant attempts below (C and D).

3. Conclusion

This document presents a taxonomy of definitions for usability studies in biometrics. Unlike traditional biometric terminology, the terms defined here are primarily driven by *user* (as opposed to *system*) behavior. However, it is likely that the document could provide a foundation for a complimentary *system*-oriented taxonomy. Introducing a taxonomy, rather than a set of strict definitions, allows practitioners to further constrain the terminology presented here to better fit a particular application. The taxonomy's ability to be adapted to a wide variety of edge cases provides evidence of its completeness and robustness.